GDPR Come valutare i rischi IT e la sicurezza dei dati

Corrado Pomodoro - HSPI

Milano, 22 marzo 2018

HSPI S.p.A.
CONSULENTI DI DIREZIONE: BOLOGNA | MILANO | ROMA
Viale Aldo Moro, 16 - Bologna | 051 509861 | info@hspi.it | www.hspi.it

Rischio

(37) Un gruppo imprenditoriale dovrebbe costituirsi di un'impresa controllante e delle sue controllate, là dove l'impresa controllante dovrebbe essere quella che può esercitare un'influenza dominante sulle controllate in forza, ad esempio, della proprietà, della partecipazione finanziaria o delle norme societarie o del potere di fare applicare le norme in materia di protezione dei dati personali. Un'impresa che controlla il trattamento dei dati personali in imprese a essa collegate dovrebbe essere considerata, unitamente a tali imprese, quale «gruppo imprenditoriale».

(38) I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.

(39) Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

(40) Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato

L 119/8 IT Gazzetta ufficiale dell'Unione europea 4.5.2016

nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

7 di 88

81 ricorrenze della parola **rischio**

Ricerca PDF

Ricerca Adesso | Opzioni | Azzera risultati

Quale parola o frase cercare?

risch

Dove cercare?

<In documento attivo (GDPR_traduzione Italiana Ufficiale)>

Risultati ricerca: 1 documenti, 81 elementi, [00:00]

GDPR_traduzione Italiana Ufficiale.pdf (81)

- rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di
- gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il
- i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili
- il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico
- dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti
- ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati
- rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali
- dei rischi derivanti dal trattamento, e vuole 4.5.2016
- il rischio di errori e al fine di garantire la sicurezza dei dati personali
- potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca
- del rischio per i diritti e le libertà delle persone fisiche. 4.5.2016
- I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e
- interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga
- del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con
- Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si
- un rischio o un rischio elevato. (77) Gli orientamenti per la messa in atto
- un rischio elevato. (77) Gli orientamenti per la messa in atto di opportune misure
- del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità
- il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate
- un rischio elevato per i diritti e le libertà delle persone fisiche e indicare
- tale rischio. (78) La tutela dei diritti e delle libertà delle persone fisiche relativamente
- un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della
- rischio in relazione ai diritti e alle libertà dell'interessato. Il titolare del
- i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la
- tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza
- ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere
- del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi
- i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale
- un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del
- tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle
- un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune
- un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine
- un rischio elevato per i diritti e le libertà della persona fisica, al fine
- un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma

Ricerca PDF

L'analisi dei rischi

conseguenze per i diritti degli interessati *

$$Minaccia \times Vulnerabilità = \textbf{RISCHIO} = Impatto \times Probabilità$$

probabilità della violazione

HSPI

** in caso di violazione di **Riservatezza**, **Integrità** o **Disponibilità** dei dati*

Quando?

Con riferimento alla valutazione d'impatto (PIA), il regolamento ne stabilisce l'obbligo nel caso di "**rischio elevato per i diritti e le libertà* delle persone fisiche**" [art. 35]

- **distruzione** accidentale o illegale [D]
- **perdita** dei dati [D]
- **modifica** non voluta [I]
- **diffusione** non consentita [R]

Secondo il gruppo di lavoro ex articolo 29 (**WP29**):

> *"In pratica, ciò significa che i titolari del trattamento devono **continuamente valutare i rischi** creati **dalle loro attività al fine di stabilire quando** una tipologia di trattamento "**possa presentare un rischio elevato** per i diritti e le libertà delle persone fisiche".*
>
> *"Va sottolineato che al fine di poter gestire i rischi per i diritti e le libertà delle persone fisiche, **detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati**. I titolari del trattamento non possono sottrarsi alla loro responsabilità stipulando polizze assicurative."*

* *diritti alla protezione dei dati e alla vita privata, inclusi la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione [WP29]*

Con quali tecniche o strumenti?

ISO 31000, ISO 27005, NIST SP800-30, linee guida ENISA, altre all'orizzonte…

Non serve necessariamente uno **strumento** (*nelle realtà più complesse aiuta*)

Serve un approccio strutturato in fasi:

Fase 1	Definizione del contesto
Fase 2	Valutazione degli impatti
Fase 3	Identificazione delle possibili minacce e della loro probabilità
Fase 4	Valutazione dei rischi (come combinazione di probabilità ed impatto)

Fase 5	Misure di mitigazione (proporzionate al rischio)

HSPI

Fase 1. Analisi dei rischi – definizione del contesto

Fase 1	**Definizione del contesto**
Fase 2	Valutazione degli impatti
Fase 3	Identificazione minacce e probabilità
Fase 4	Valutazione dei rischi

Considerando le diverse fasi del trattamento:

raccolta, elaborazione, uso, archiviazione, trasferimento, rimozione, etc.

- ❑ Quali sono i trattamenti sui dati personali?
- ❑ Quali sono le categorie di dati personali trattati?
- ❑ Qual è lo scopo dei trattamenti?
- ❑ Quali sono le categorie di interessati?
- ❑ Chi sono i destinatari dei dati?
- ❑ **Con quali strumenti sono trattati i dati?**
- ❑ **Dove ha luogo il trattamento?**

Registro dei Trattamenti dei Dati personali

Trattamento				Struttura organizzativa (dipartimento, etc)	U.O. o persona di riferimento	Categoria di dati personali	Finalità del trattamento	Categorie di soggetti interessati	Limite di conservazione	Strumenti utilizzati					Modalità di conservazione						Tipo di trattamento effettuato							Categorie di destinatari	Trasferimento verso terzi o organizzazioni internazionali
Nome	Processo (liv 1)	Attività (liv 2)	Operazione (liv 3)							App 1	App 2	App 3	App 4	App 5	Database	File Storage	Email	Personal Pc	Mobile	Cloud	Faldone	Altro 2	Lettura	Copia	Stampa	Trasmissione	Modifica	Elaborazione	Altro		
Nome	T	T.1	T.1.A	Struttura 1	U.O. 1	Categoria dato 1	Fin 1	Cat 1	3 mesi						x	x	x	x				x									
Nome	T	T.1	T.1.B	Struttura 2	U.O. 2	Categoria dato 2	Fin 2	Cat 1	9 mesi						x	x			x			x									
Nome	T	T.2	T.2.A	Struttura 3	U.O. 3	Categoria dato 3	Fin 3	Cat 2	3 mesi						x	x				x		x									
Nome	T	T.2	T.2.B	Struttura 4	U.O. 4	Categoria dato 4	Fin 4	Cat 4	9 mesi						x	x					x	x									

HSPI

Fase 2. Analisi dei rischi – valutazione degli impatti [1 di 2]

Livello di impatto	Descrizione
Molto alto	Inconvenienti significativi con conseguenze anche irreversibili (impossibilità di lavorare, conseguenze psicologiche permanenti, morte, etc.).
Alto	Inconvenienti significativi, superabili solo con serie difficoltà (sottrazione di denaro, limitazioni di credito, danno di proprietà, citazione in giudizio, conseguenze per la salute, perdita impiego, etc.).
Medio	Inconvenienti significativi, superabili con qualche difficoltà (costi extra, impedimento a ricevere servizi, preoccupazione, stress).
Basso	Conseguenze minori, superabili senza particolari problemi (fastidio, perdita di tempo per reintroduzione dei dati, …).

Fase 2. Analisi dei rischi – valutazione degli impatti [2 di 2]

Considerazioni	Valutazione impatto			
	Basso	Medio	Alto	Molto alto
Considerazioni sull'impatto per gli interessati in caso di diffusione non autorizzata (perdita di **riservatezza**) dei dati.	☐	☐	☑	☐
Considerazioni sull'impatto per gli interessati in caso di alterazione non autorizzata (perdita di **integrità**) dei dati.	☐	☑	☐	☐
Considerazioni sull'impatto per gli interessati in caso di distruzione o perdita (perdita di **disponibilità**) dei dati.	☐	☑	☐	☐

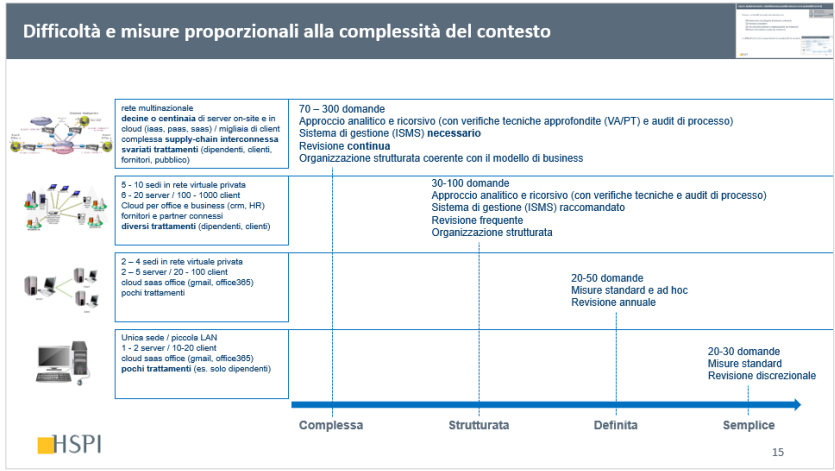
Fase 3. Analisi dei rischi – identificazione possibili minacce e loro probabilità [1 di 3]

Fase 1	Definizione del contesto
Fase 2	Valutazione degli impatti
Fase 3	**Identificazione minacce e probabilità**
Fase 4	Valutazione dei rischi

Minacce e probabilità di accadimento dipendono da:

- ❑ Infrastrutture tecnologiche (hardware e software)
- ❑ Processi e procedure
- ❑ Parti coinvolte (persone e organizzazioni) nei trattamenti
- ❑ Settore di business e scala dei trattamenti

La **difficoltà** dell'analisi è **proporzionale** alla **complessità** del **contesto**



Fase 3. Analisi dei rischi – identificazione possibili minacce e loro probabilità [2 di 3]

Esempio di ambiti di valutazione

Infrastrutture tecnologiche	
Ci sono parti del trattamento che avvengono via internet?	Quando il trattamento avviene anche parzialmente via internet aumenta la possibilità di attacchi on-line (DOS, SQL injection, Man-in-the-middle) specialmente quando il servizio è accessibile pubblicamente via internet.
Il sistema IT è interconnesso ad altri sistemi interni o esterni?	L'interconnessione con altri sistemi può introdurre minacce addizionali. Soprattutto in caso di configurazioni non adeguatamente controllate.
Utenti non autorizzati possono facilmente ottenere l'accesso agli ambienti IT?	Sebbene il focus dell'analisi sia sui sistemi informatizzati, anche l'ambiente fisico ha un'importanza rilevante per la protezione dei dati e può determinare serie minacce alla salvaguardia dei dati.

Processi e procedure	
Ruoli e responsabilità sono vaghi o non chiaramente definiti?	La mancanza di chiare definizioni di ruoli e responsabilità, può tradursi in accessi non controllati ai dati personali con conseguenti violazioni e compromissione della sicurezza dei sistemi.
Gli impiegati possono utilizzare dispositivi personali per connettersi ai sistemi?	L'utilizzo di dispositivi personali aumenta il rischio di diffusione di dati o accessi non autorizzati. Il mancato controllo centrale dei dispositivi può introdurre più facilmente bachi o virus nei sistemi.
I trattamenti possono essere eseguiti senza che vengano creati e conservati log delle attività?	La mancanza di appropriato monitoraggio e logging delle attività sui sistemi può aumentare la probabilità di violazioni intenzionali o accidentali.

Parti coinvolte	
I trattamenti sono eseguiti da un numero imprecisato di persone (interne e/o esterne all'organizzazione)	Quando i trattamenti dei dati possono essere eseguiti da un grande numero di persone i possibili abusi aumentano a causa del cosiddetto "fattore umano"
Ci sono parti del trattamento condotte da terze parti (responsabili del trattamento)?	Il coinvolgimento di una terza parte può comportare una perdita parziale di controllo sui dati. Inoltre ulteriori minacce possono essere introdotte dalle terze parti.
Il personale coinvolto nei trattamenti è poco consapevole delle implicazioni di sicurezza?	La scarsa sensibilizzazione rispetto alle implicazioni e a i rischi IT aumenta l'esposizione dei dati alle minacce esistenti.

Settore di business e scala dei trattamenti	
Il settore di business è soggetto ad attacchi cyber?	La ricorrenza di incidenti di natura informatica nello stesso settore di business è una indicazione da non sottovalutare per la valutazione di possibili violazioni dei propri dati.
I trattamenti riguardano grandi volumi di dati e/o di interessati?	Il tipo e il volume di dati personali può incrementare l'appetibilità per i potenziali attaccanti.
Ci sono buone prassi di sicurezza applicabili al settore che non sono state adeguatamente applicate?	La mancata applicazioni di misure di sicurezza raccomandate dalle buone prassi può incrementare il livello di esposizione e di vulnerabilità alle minacce.

Fase 3. Analisi dei rischi – identificazione possibili minacce e loro probabilità [3 di 3]

Area di valutazione	Probabilità			
	Bassa [1]	Media [2]	Alta [3]	Molto alta [4]
Infrastrutture tecnologiche	☐	☑	☐	☐
Processi e procedure	☐	☐	☑	☐
Parti coinvolte (persone e organizzazioni) nei trattamenti	☑	☐	☐	☐
Settore di business e scala dei trattamenti	☐	☐	☐	☑

Somma dei risultati	Livello di probabilità
13-16	Molto alta
9-12	**Alta**
6-8	Media
4-5	Bassa

HSPI

Fase 4. Analisi dei rischi – valutazione dei rischi

Fase 1	Definizione del contesto
Fase 2	Valutazione degli impatti
Fase 3	Identificazione minacce e probabilità
Fase 4	**Valutazione dei rischi**

Considerazioni	Valutazione impatto			
	Basso	Medio	Alto	Molto alto
Considerazioni sull'impatto per gli interessati in caso di diffusione non autorizzata (perdita di **confidenzialità**) dei dati.	☐	☐	☑	☐
Considerazioni sull'impatto per gli interessati in caso di alterazione non autorizzata (perdita di **integrità**) dei dati.	☐	☑	☐	☐
Considerazioni sull'impatto per gli interessati in caso di distruzione o perdita (perdita di **disponibilità**) dei dati.	☐	☑	☐	☐

Livello di impatto

Molto alto				
Alto			C	
Medio			I, D	
Basso				
	Basso	Medio	Alto	Molto Alto

Livello di probabilità

Somma dei risultati	Livello di probabilità
13-16	Molto alta
9-12	**Alta**
6-8	Media
4-5	Bassa

HSPI

Fase 5 - Misure di mitigazione (proporzionate al rischio) [1/2]

Devono rispondere alle aree di debolezza risultanti dall'analisi dei rischi (probabilità)

La loro individuazione è facilitata da diversi ***framework* internazionali**:

- ISO/IEC 27001
- CIS (Center for Internet Security) Critical Security Controls (ex SANS 20)
- NIST 800-53 o NIST cybersecurity framework (su cui si basa il framework nazionale per la cybersecurity)
- Linee guida ENISA

NIST CYBERSECURITY FRAMEWORK (CSF)

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

Fase 5 - Misure di mitigazione (proporzionate al rischio) [2/2]

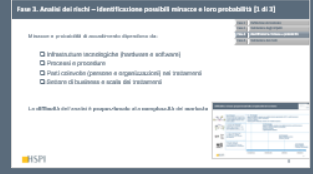
ISO/IEC 27001 – Annex A	
A.5	Information security policies
A.6	Organization of information security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity mgmt
A.18	Compliance

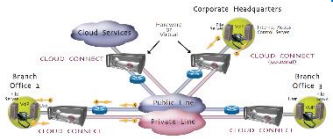
Critical Security Control	
1	**Inventory of Authorized and Unauthorized Devices**
2	**Inventory of Authorized and Unauthorized Software**
3	**Secure Configurations for Hardware and Software**
4	**Continuous Vulnerability Assessment and Remediation**
5	**Controlled Use of Administrative Privileges**
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	**Malware Defenses**
9	Limitation and Control of Network Ports
10	**Data Recovery Capability**
11	Secure Configurations for Network Devices
12	Boundary Defense
13	**Data Protection**
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

Pseudonimizzazione, anonimizzazione, crittografia, cancellazione, trasportabilità, accessi controllati (password sicure), accountability, … non sono necessariamente misure sufficienti né sempre adeguate!

HSPI

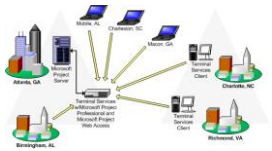
Difficoltà e misure proporzionali alla complessità del contesto





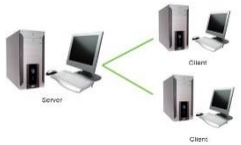
rete multinazionale
decine o centinaia di server on-site e in cloud (iaas, paas, saas) / migliaia di client
complessa **supply-chain interconnessa**
svariati trattamenti (dipendenti, clienti, fornitori, pubblico)

70 – 300 domande
Approccio analitico e ricorsivo (con verifiche tecniche approfondite (VA/PT) e audit di processo)
Sistema di gestione (ISMS) **necessario**
Revisione **continua**
Organizzazione strutturata coerente con il modello di business



5 - 10 sedi in rete virtuale privata
6 - 20 server / 100 - 1000 client
Cloud per office e business (crm, HR)
fornitori e partner connessi
diversi trattamenti (dipendenti, clienti)

30-100 domande
Approccio analitico e ricorsivo (con verifiche tecniche e audit di processo)
Sistema di gestione (ISMS) raccomandato
Revisione frequente
Organizzazione strutturata



2 – 4 sedi in rete virtuale privata
2 – 5 server / 20 - 100 client
cloud saas office (gmail, office365)
pochi trattamenti

20-50 domande
Misure standard e ad hoc
Revisione annuale

Unica sede / piccola LAN
1 - 2 server / 10-20 client
cloud saas office (gmail, office365)
pochi trattamenti (es. solo dipendenti)

20-30 domande
Misure standard
Revisione discrezionale

Complessa — **Strutturata** — **Definita** — **Semplice**

HSPI

Grazie.

corrado.pomodoro@hspi.it