STUDIO SULLA VALUTAZIONE DEL RISCHIO E D'IMPATTO

A cura di Luigi Zampetti

giugno 2021

MSA
MANAGEMENT SYSTEMS ANALYST

INDICE DEL DOCUMENTO

OBIETTIVO DELLO STUDIO

Premesso che la valutazione dei rischi rappresenta l'approccio su cui si basa il Regolamento UE 2016/679 ed è parte integrante della valutazione d'impatto, questo studio ha i seguenti obiettivi:

I. scomporre un'attività nei suoi elementi costitutivi e nei fattori chi li qualificano (Capitolo 4),

II. dimostrare che il significato degli elementi è comparabile a quello dei termini che qualificano i concetti utilizzati nel Regolamento (Allegati C, E) relativi a:

   a. rischio (origine, natura, particolarità, probabilità, gravità)

   b. trattamento (natura, ambito di applicazione, contesto, oggetto e finalità, fonti di rischio, tipo, estensione, frequenza),

III. illustrare il meccanismo di valutazione dei rischi (Capitoli 5, 6),

IV. dimostrare che il significato degli elementi è comparabile con molti contenuti della valutazione d'impatto (Capitolo 7).

Coerentemente agli obiettivi, questo studio è organizzato in 7 capitoli che riguardano:

- Capitolo 1 - la differenza di approccio tra Direttiva 95/46 e Regolamento UE 2016/679
- Capitolo 2 - l'obiettivo comune alla valutazione del rischio e d'impatto
- Capitolo 3 - il concetto di rischio e la formula di calcolo
- Capitolo 4 - gli elementi costitutivi di un'attività e i fattori qualificanti
- Capitolo 5 - il meccanismo di valutazione del rischio
- Capitolo 6 - esempio di applicazione del meccanismo
- Capitolo 7 - il meccanismo di valutazione

ed è completato da un documento che contiene i seguenti allegati:

- Allegato A - Sui processi aziendali e il re-engineering dei processi.
- Allegato B - Definizioni dei termini-chiave (rischio, trattamento, danno) nel GDPR.
- Allegato C - Analisi semantica dei termini-chiave e comparazione con gli elementi costitutivi di un'attività.
- Allegato D - Metodo ENISA di valutazione del rischio di sicurezza: differenze con il meccanismo di valutazione del rischio basata sull'analisi degli elementi costitutivi di un'attività.
- Allegato E - Valutazione d'impatto: individuazione dei riferimenti e della descrizione presenti:
  - nel testo del GDPR (paragrafo E.1)
  - nell'allegato A delle linee-guida WP 248/01 (paragrafo E.2),
  - nel tool del CNIL (paragrafo E.3), comparandoli con gli elementi e i fattori costitutivi di un'attività e della valutazione del rischio.
  - Comparazione tra gli aspetti presenti nei tre documenti (paragrafo E.4).
- Allegato F - Scale di valori su:
  - Entità (gravità) del Danno, Probabilità, Gravità delle minacce by CNIL, Gravità delle vulnerabilità by CNIL.

TERMINOLOGIA

Di seguito i termini utilizzati nel testo ed il significato attribuito, rintracciabili in tutta la letteratura sul risk management.

- Rischio: eventualità che una minaccia possa trasformarsi realmente in danno, comportando così un determinato impatto.
    - Rischio "potenziale" o "intrinseco" o "inerente": livello di rischio connaturato ad un'attività ed ai singoli fattori, in assenza di misure di contenimento.
    - Rischio "effettivo" o "residuo": livello di rischio che tiene conto delle misure adottate per contrastare il rischio potenziale (o contromisure).
- Vulnerabilità: caratteristica implicita, intrinseca ad una azione, ad un comportamento o ad un mezzo che rappresenta un punto di debolezza che può essere sfruttato da una minaccia per arrecare un danno.
    - Le vulnerabilità possono avere un diverso livello di gravità.
- Minaccia: agente che può causare un danno sfruttando una vulnerabilità e l'assenza o l'insufficienza di misure di contenimento del rischio. Le minacce possono:
    - essere di diverso tipo (naturale, ambientale, accidentale, intenzionale),
    - avere un diverso livello di gravità (assoluta, molto alta, alta, media, bassa, trascurabile)
    - manifestarsi con un diverso grado di frequenza (improbabile, raro, probabile, molto probabile, frequente).
- Incidente: concretizzazione del rischio ([1]).
- Violazione: perdita parziale o totale dei tre requisiti di sicurezza (riservatezza, integrità e disponibilità) dei dati e dei mezzi con cui sono gestiti.
- Danno: conseguenza del verificarsi di un rischio ovvero dell'accadimento di una minaccia.
    - I danni possono essere di diverso tipo (fisico, materiale o tangibile o economico, immateriale o intangibile) ed avere un diverso livello di gravità.
    - La gravità del danno cresce in funzione del valore economico dell'asset, del valore economico dei dati (spesa sostenuta per la raccolta, l'aggiornamento, la conservazione), della criticità dei dati
    - l'azienda e/o per gli utenti).
- Impatto: effetto reale del danno sugli elementi costitutivi dell'attività, sull'attività stessa, sull'organizzazione che gestisce l'attività.
    - Impatto è anche sinonimo di danno oppure sinonimo della misura o entità del danno.
- Misure di sicurezza: comportamenti, azioni, luoghi, apparecchiature, meccanismi, procedure messe in atto, adottate, implementate per colmare le vulnerabilità e contrastare le minacce (contromisure), impedendone l'accadimento, e quindi la produzione di un danno. Le misure possono:
    - essere di diverso tipo (fisico, tecnico, logico, organizzativo)
    - avere un diverso livello di efficacia (assoluta, molto alta, alta, media, bassa, trascurabile).

[1] Per questo che i termini che indicano il rischio e l'incidente sono spesso gli stessi.

1. LA DIFFERENZA DI APPROCCIO DELLE NORME SULLA PRIVACY

Il passaggio dalla Direttiva 95/46 al Regolamento 2016/679 è segnato dalla sostanziale differenza di approccio: mentre il Codice Privacy ([2]) ha un orientamento che guida alla conformità alle norme "unico per tutti" (one size fits all approach) e di tipo "prescrittivo", il Regolamento ha un approccio "caso per caso" (case-by-case approach) di tipo "funzionale", che introduce maggiore flessibilità di risposta, affidando al Titolare la completa responsabilità ex ante ed ex post dei risultati delle azioni intraprese per aderire alla norma.

L'approccio del Regolamento UE è dunque basato sulla valutazione dei rischi (risk based approach), la quale determina che:

1. il valore quantitativo o qualitativo del rischio sia connesso e relativo ad una situazione concreta e ad una minaccia conosciuta;
2. gli obblighi del Titolare (Data controller) e/o del Responsabile del trattamento, in termini di messa in atto delle misure di protezione, variano nel tempo in relazione allo stato della tecnologia e alle pratiche comuni attuate nel settore in cui operano;
3. il grado di responsabilità del Titolare (Data controller) e/o del Responsabile del trattamento è "proporzionale ai rischi stimati tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32". ([3])

La conferma più evidente della centralità della valutazione dei rischi è la ricorrenza nel testo ([4]) di questi termini:

- "rischio/rischi" 132 occorrenze
- "valutazione" 53 occorrenze
- "impatto" 31 occorrenze
- "misure tecniche e organizzative" 142 occorrenze
- "minaccia/minacce" 10 occorrenze.

[2] Adozione della Direttiva dell'Unione Europea 95/46/CE del 24 ottobre 1995.
[3] Art. 83 2.d) il grado.
[4] Fonte: versione della GU UE in lingua italiana del 8 aprile 2016.

2. L'OBIETTIVO COMUNE DELLE VALUTAZIONI DEL RISCHIO E D'IMPATTO

In questo capitolo del documento si dimostra l'obiettivo comune ai due meccanismi di valutazione del rischio e d'impatto di individuare le misure di contrasto.

2.1 Obiettivo

Le valutazioni del rischio e d'impatto di una attività di trattamento hanno per obiettivo la determinazione delle misure di contenimento della probabilità.

La conferma si trova analizzando il testo del GDPR:

- per la valutazione del rischio
    - Art. 24.1 Responsabilità del Titolare del trattamento
    - Art. 32.1 e 32.2 Sicurezza del trattamento
    - Considerando 77 che, nonostante sia dedicato a codici di condotta e certificazioni, afferma come la valutazione del rischio connesso al trattamento in termini di origine, natura, probabilità e gravità orienti la messa in atto di opportune misure per attenuarlo;
- per la valutazione d'impatto
    - Considerando 84 (...determinazione delle opportune misure da adottare...)
    - Considerando 90 (...La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio...)
    - Art. 35.7.d. (...le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali...).

Questo obiettivo è presente anche nel Manuale sulla Sicurezza nel trattamento dei dati personali, emesso da ENISA (European Union Agency for Network and Information Security) a dicembre 2017 ([5]): infatti, al termine della valutazione dei rischi di sicurezza (step 5), è richiesto di verificare le misure già adottate in modo da individuare quelle mancanti ([6]). (vedi Allegato D)

Questo comune obiettivo trova un senso nell'approccio al rischio su cui si basa il GDPR: se conosco il rischio posso individuare le azioni per contenerlo.

2.1.1 Considerazioni

1. La determinazione delle misure è guidata dalla individuazione delle vulnerabilità manifestate dai mezzi impiegati e delle minacce alle quali sono esposti.
2. Le misure che sono già state messe in atto, adottate ed implementate determinano un abbassamento della probabilità di accadimento delle minacce (fattore P della formula di calcolo) e di conseguenza la riduzione del rischio, che da potenziale (o intrinseco o inerente) diventa effettivo (o residuo).
3. Il rischio effettivo o residuo
    - può essere ritenuto accettabile,

[5] dal quale è stato poi realizzato un tool utilizzabile on line
[6] utilizzando le misure previste dall'allegato della ISO/IEC 27001

- oppure ulteriormente abbassato con ulteriori misure,
- oppure trasferito (outsourcing di una o tutte le attività, stipula di una polizza assicurativa).

4. L'insieme delle misure in atto e da adottare è sempre proporzionata alla gravità del rischio potenziale ed effettivo (min 0,1 - max 0,9) tenendo conto del contesto (si vedano gli elementi costitutivi dell'attività e i fattori qualificanti illustrati nel Capitolo 4).

3. IL CONCETTO DI RISCHIO

In questo capitolo del documento si definisce il concetto di rischio, si individuano il metodo di valutazione e le modalità di rappresentazione numerica.

3.1 Definizione

In letteratura il rischio è l'eventualità di subire un danno ([7]) in conseguenza di un'azione, compiuta o subita.

3.2 Formula di calcolo e rappresentazione del valore

Il rischio è espresso con la formula

$$R = P * D$$

nella quale il Rischio (R) è il prodotto

- della Probabilità di accadimento dell'incidente (P)
- per il Danno massimo ([8]) conseguente (D).

Il rischio è quindi tanto più grande quanto più è probabile che accada l'incidente e tanto maggiore è l'entità del danno.

La consistenza del rischio varia nel range di valori tra lo 0,1 e lo 0,9, in quanto:

- il valore 0 (zero) equivarrebbe alla impossibilità di subire un danno (il rischio non esiste perché non sono compiute azioni), mentre
- il valore 1 (uno) esprimerebbe la certezza di subire un danno (non c'è più probabilità, quindi non c'è niente da misurare).

Per aumentare la leggibilità e la capacità di interpretare il rischio, si usano valori in percentuale, nel range tra l'1% ed il 99%.

3.3 Metodi di valutazione del rischio

Il rischio è un concetto probabilistico e sono possibili tre diversi metodi di (analisi e) valutazione:

A. qualitativo, che richiede di esprimere un giudizio sulla situazione che si sta valutando su una scala qualitativa (ad esempio alto, medio, basso; oppure improbabile, poco probabile, probabile, altamente probabile);

B. quantitativo, nel quale la valutazione è espressa in valori numerici riferiti al valore economico sia dei singoli asset che costituiscono l'oggetto dell'analisi che delle perdite (danni) prodotte dal concretizzarsi dei rischi;

C. semi quantitativo, nel quale la valutazione è effettuata in termini qualitativi e poi trasformata in valori numerici (pesi) per poterla sottoporre ad algoritmi di calcolo, come se fosse una valutazione quantitativa, anche se non-economica.

[7] oppure di godere di un vantaggio: ad esempio, l'azione di acquistare un biglietto della lotteria "rischia" di farmi vincere un premio.
[8] Questo criterio è utilizzato nella valutazione del rischio in tutti gli ambiti.

4. LA SCOMPOSIZIONE DI UN'ATTIVITÀ: ELEMENTI COSTITUTIVI E FATTORI QUALIFICANTI

In questo capitolo del documento sono individuati gli ambiti di applicazione della valutazione dei rischi, gli elementi costitutivi di un'attività, i fattori che qualificano gli elementi.

4.1 Individuazione degli elementi

Il rischio può essere valutato in relazione ad azioni da compiere o compiute in qualunque ambito: dalla sicurezza sul lavoro (es. ferimento) alla conduzione di un'azienda (es. fallimento), dallo sfruttamento delle risorse naturali (es. inquinamento dell'ambiente) alla salute personale (es. malattia), dall'esercizio della professione (es. responsabilità professionale) alla concessione di un credito (es. inesigibilità), ecc.

All'interno di qualunque ambito, la valutazione del rischio richiede di prendere in considerazione gli elementi che costituiscono l'attività da analizzare.

4.1.1 Esempio

Analizziamo, ad esempio, l'attività "trasporto e consegna a domicilio di un bene".

TIPO DI ELEMENTO	ELEMENTO	FATTORI CHE DETERMINANO IL RISCHIO	RISCHI (INCIDENTI)	DANNI (POTENZIALI)	TIPI DI DANNI (POTENZIALI)
azione	- trasporto e consegna di un bene	- pianificazione errata - impiego di mezzi inadatti	- ritardo o mancata consegna, - consegna ad un destinatario errato	- penale da pagare - aumento premio polizza - caduta del prestigio	- materiali (economici) - di immagine
modalità, mezzi impiegati, vulnerabilità, minacce	- automezzo - smartphone - lettore di bar code - istruzioni	- obsolescenza - manutenzione insufficiente - incompetenza nell'uso	- malfunzionamento o blocco dei mezzi	- ritardo o mancata consegna - penale da pagare - caduta del prestigio	- materiali (economici) - di immagine
beni e dati	- contenuto del pacco	- Imballaggio insufficiente, - mancato controllo dell'accesso all'automezzo	- danneggiamento o furto del contenuto del pacco	- penale da pagare - aumento premio polizza	- materiali (economici) - di immagine

				- caduta del prestigio	
persone fisiche	- autista, - destinatario	- incompetenza o eccessivo stress dell'autista - coinvolgimento in incidente	- Incidente automobilistico causato o subito	- ferimento o morte dell'autista - aumento premio polizza	- fisici - materiali (economici)
Soggetti	- azienda di trasporti - cliente (o destinatario)	- tutti i precedenti	- tutti i precedenti	- risarcimento - aumento premio polizza - caduta del prestigio	- materiali (economici) - di immagine

4.1.2 Considerazioni

L'esempio mette in evidenza che:

1. il rischio relativo ad una attività è funzione dei diversi fattori che possono determinarlo,
2. i fattori di rischio possono essere:
    A. il modo in cui è svolta l'azione (es. errata o corretta pianificazione)
    B. la qualità dei mezzi impiegati (es. automezzo obsoleto o nuovo),
3. una parte dei fattori di rischio è dunque insita nell'azione e nei mezzi impiegati
4. un'altra parte dei fattori di rischio coincide con fattori esterni all'attività (es. furto e coinvolgimento in un incidente causato da altri),
5. il tipo e la gravità dei danni dipendono:
    - dall'obiettivo dell'attività (es. sarebbero maggiori se il trasporto riguardasse una sacca di sangue in grado di salvare una vita)
    - dal valore del bene (es. trasporto di un'opera d'arte piuttosto di un indumento)
    - dal tipo di minaccia che si concretizza, che ha una sua specifica gravità e probabilità (es. un errore di pianificazione – probabile - produce un ritardo, ma il coinvolgimento in un incidente può produrre il blocco del trasporto ed il ferimento dell'autista, anche se poco probabile).

4.2 Gli elementi costitutivi di un'attività

Da queste considerazioni è ora possibile individuare gli elementi costitutivi di un'attività:

1. l'azione da svolgere/svolta (che può essere l'attività stessa)
2. i beni oggetto dell'azione (tra cui i dati)
3. le persone fisiche impiegate nell'azione o coinvolte dall'azione

4. la modalità utilizzata per agire
5. i mezzi impiegati nell'azione
6. le minacce alle quali sono esposti i mezzi (comprese le vulnerabilità che presentano)
7. le misure di contrasto alle minacce
8. i soggetti che a diverso titolo sono attivi (di cui il Titolare rappresenta l'organizzazione).

4.3 Attività e processi

Nell'esempio abbiamo equiparato il "trasporto e consegna di un bene" ad una attività: tuttavia, un'attività può essere sia suddivisa in sub-attività sia aggregata in processi.

L'attività in esempio potrebbe essere scomposta nelle seguenti sub-attività:

a. pianificazione dell'attività e del percorso
b. scelta dell'automezzo, dei device e dell'autista
c. imballaggio del bene e/o sistemazione nell'automezzo
d. consegna del bene e documentazione della consegna.

Viceversa, assunto che con il termine "processo" si intende la "successione di attività tra loro collegate logicamente e finalizzate a raggiungere un risultato, svolte con determinate modalità e impiegando specifici mezzi", "il trasporto e la consegna di un bene" potrebbe essere assimilata ad un processo costituito da più fasi.

Se ne deduce che prendere in considerazione i 5 elementi individuati (attività, modalità e mezzi, beni, persone, soggetti) rende valida la valutazione del rischio sia in caso di suddivisione (sub-attività) sia in caso di aggregazione (processi).

Da questo momento nel documento si utilizzerà il termine "attività" in luogo anche del termine "processo".

Per approfondire il concetto di "processo aziendale" si veda l'Allegato A.

4.4 Fattori qualificanti gli elementi

Gli elementi che costituiscono un'attività sono a loro volta scomponibili nei fattori che li qualificano, che incidono nella elaborazione della valutazione del rischio.

4.4.1 Caratteristiche dell'attività

Nella tabella 1 sono individuati i fattori che qualificano l'attività.

Tabella 1 - Attività (Elemento I)			
A-settore merceologico dell'organizzazione ([9])	Assume rilevanza quando rientra tra i seguenti. ☐ Energia ☐ Trasporti ☐ Bancario ☐ Infrastrutture mercati finanziari ☐ Sanitario ☐ Acqua potabile ☐ Infrastrutture digitali	E-qualità dell'attività	Determina un diverso livello di danno: ☐ 1-tipo di persone presenti nell'attività (Elemento 3) ☐ 2-tipo di beni oggetto dell'attività (Elemento 2) ☐ 3-tipo di dati utilizzati (Elemento 2) ☐ 4-livello di criticità aziendale dell'attività (vedi B1)
B-obiettivo dell'attività	Determina un diverso livello di danno: ☐ 1-funzionamento della struttura (vedi E4) ☐ 2-realizzazione di un prodotto ☐ 3-erogazione di un servizio a terze parti	F-frequenza dell'attività	Aumenta la probabilità di rischio: ☐ 1-occasionale ☐ 2-poco frequente ☐ 3-frequente ☐ 4-regolare ☐ 5-quotidiana
C-articolazione dell'attività	Introduce più fattori di rischio: ☐ 1-fasi e/o sub-attività ☐ 2-interazioni con altre attività ☐ 3-soggetti esterni coinvolti	G-durata dell'attività	Aumenta la probabilità di rischio: ☐ 1-ore ☐ 2-giorni ☐ 3-settimane ☐ 4-mesi ☐ 5-anni
D-dimensioni dell'attività	Determina un diverso livello di danno:		

[9] Settori che rientrano nella Direttiva 1148/2016 NIS recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (DLGS 65 del 18 maggio 2018).

	☐ 1-nr. di utenti coinvolti ☐ 2-quantità di dati utilizzati		
D1-quantità di utenti	Determina un diverso livello di danno: ☐ 1-unità ☐ 2-decine ☐ 3-centinaia ☐ 4-migliaia ☐ 5-decine di migliaia ☐ 6-centinaia di migliaia ☐ 7-milioni	D2-quantità di dati	Determina un diverso livello di danno: ☐ 1-esigua ☐ 2-piccola ☐ 3-media ☐ 4-grande ☐ 5-grandissima

4.4.2 Tipi di dati e di persone

Nelle tabelle 2 e 3 sono individuate le variabili dei fattori "tipi di persone e di dati" che caratterizzano l'attività.

([10]) Tabella 2 - tipi di dati (Elemento 2) (vedi fattore E1 qualità dell'attività)			([11]) Tabella 3 - tipi di persone (Elemento 3) (vedi fattore E1 qualità dell'attività)
Dati anagrafici ☐ Nome ☐ Cognome ☐ Sesso ☐ Data di nascita ☐ Luogo di nascita ☐ Codice fiscale	Dati di contatto ☐ Indirizzo postale ☐ Indirizzo mail ☐ Indirizzo PEC Numero di telefono fisso ☐ Numero di cellulare	Categorie particolari di dati ☐ Origini razziali o etniche ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Dati genetici ☐ Dati relativi alla salute ☐ Stato di salute di un familiare ☐ Vita e orientamento sessuale ☐ Biometrici	Tipi di persone ☐ Dipendenti/ Consulenti ☐ Utenti/ Contraenti/ Abbonati/ Clienti (attuali) ☐ Utenti/ Contraenti/ Abbonati/ Clienti (potenziali) ☐ Associati / soci / aderenti / simpatizzanti / sostenitori ☐ Soggetti che ricoprono cariche sociali ☐ Beneficiari o assistiti ☐ Pazienti ☐ Minori ☐ Persone vulnerabili ([12])
Dati relativi alla fornitura di un servizio di comunicazione elettronica ☐ Dati di traffico ☐ Dati relativi alla navigazione Internet	Dati relativi a documenti di identificazione/ riconoscimento ☐ Carta di identità ☐ Passaporto ☐ Patente	Giudiziari ☐ Condanne penali o reati ☐ Misure di sicurezza o di prevenzione	☐ Partecipanti a studi clinici ☐ Candidati ☐ Visitatori / Ospiti / Partecipanti a eventi ☐ Fornitori

[10] Categorie riprese dal Modello di notifica al Garante in caso di data breach, sezione C punto 8.

[11] Categorie riprese dal Modello di notifica al Garante in caso di data breach, sezione C punto 10.

[12] Es. vittime di violenze o abusi, rifugiati, richiedenti asilo minori, anziani, disabili, sieropositivi, affetti da dipendenze, donne per IVG, affette da disagi o con patologia psichiatrica.

	☐ CNS-tessera sanitaria		
Dati di accesso e identificazione ☐ Codice identificativo univoco ☐ Username ☐ Password ☐ Customer ID ☐ Firma grafometrica	Dati di altro tipo 1 ☐ localizzazione ☐ profilazione	Dati di pagamento ☐ nr. conto corrente ☐ nr. carta di credito	
	Dati di altro tipo 2 ☐ lavorativi ☐ professionali ☐ economici ☐ patrimoniali ☐ scolastici		

4.4.3 Sui beni e le persone

Nella tabella 2.1 sono indicate le variabili qualitative dei beni in generale, valide anche per i dati.

Tabella 2.1 - Beni (Elemento 2)
Variabili qualitative ☐ valore economico del bene (vedi fattore E2 qualità dell'attività) ☐ criticità del bene ai fini della continuità aziendale (vedi fattore B1 obiettivo dell'attività e fattore E4 qualità dell'attività) ☐ criticità del bene ai fini della protezione delle persone fisiche (vedi fattori E3 e E1 qualità dell'attività)

Nella tabella 3.1 sono indicate le due classi di persone fisiche i cui fattori qualificanti sono presenti nella tabella 3.

Tabella 3.1 - Persone fisiche (Elemento 3)	
A-impiegate nell'attività	B-coinvolte dall'attività
☐ dipendenti, consulenti, ecc. (vedi fattore A dell'elemento II mezzi impiegati)	☐ utenti, clienti, ecc. (vedi fattore E1 qualità dell'attività)

4.4.4 Modalità e mezzi impiegati per svolgere l'attività

Nelle tabelle 4 e 5 sono individuate i tipi di modalità utilizzati e di mezzi impiegati.

Tabella 4 - Modalità utilizzata (Elemento 4)	Tabella 5 - Mezzi impiegati (Elemento 5)
A-manuale ☐ senza strumenti elettronici Mezzi utilizzati nella modalità manuale: ☐ asset umani (competenza, esperienza, affidabilità del personale) ☐ asset organizzativi (procedure, istruzioni operative, modulistica, linee-guida, ecc.) ☐ asset logistici (uffici, archivi, CED, armadi, ecc.) ☐ servizi di outsourcing documentale.	A-personale ☐ dipendenti ☐ consulenti ☐ volontari, stagisti
B-elettronica ☐ con strumenti elettronici Mezzi utilizzati nella modalità elettronica: ☐ asset umani (competenza, esperienza, affidabilità del personale) ☐ asset organizzativi (procedure, istruzioni operative, outsourcing a terze parti, ecc.) ☐ asset logistici (uffici, CED) ☐ asset hardware (server, computer, device mobili) ☐ asset software (di base e applicativo) ☐ asset e servizi di networking (router e switch, linee voce-dati, accesso a Internet) ☐ servizi di maintenance e assurance degli asset hardware-software ☐ asset e servizi di cloud computing (interscambio file, storage, IaaS, PaaS, SaaS, ecc.).	B-logistica ☐ uffici ☐ archivi ☐ CED ☐ servizi di outsourcing documentale ☐ servizi di outsourcing facility
C-mista ☐ con tutti gli strumenti	C-tecnologie ☐ hardware ☐ software ☐ canali ☐ servizi cloud computing ☐ servizi di manutenzione e assistenza

	D-organizzazione ☐ procedure ☐ istruzioni operative ☐ strutturazione (gerarchie) ☐ controlli

4.4.5 Sulle minacce e le misure

Nelle tabelle 6 e 7 sono individuate le tipologie di minacce e di misure di contrasto.

([13]) Tabella 6 – Minacce (Elemento 6)	Tabella 7 – Misure (Elemento 7)
A-esogene all'attività ☐ 1-accidentali esterne (naturali) ☐ 2-intenzionali esterne	A-Embedded ☐ 1-caratteristiche positive dei mezzi impiegati
B-endogene all'attività ☐ 1-accidentali interne (ambientali, errori involontari, carenze tecniche e organizzative) ☐ 2-intenziomnali interne	B-Add in ☐ 1-azione o strumento applicato ai mezzi impiegati
A-B-Probabilità di manifestazione ☐ 1-improbabile ☐ 2-poco probabile ☐ 3-probabile ☐ 4-molto probabile	A-B Efficacia delle misure ☐ 1-insufficiente ☐ 2-minima ☐ 3-adeguata ☐ 4-ottimale
A-B-Gravità della minaccia ☐ 1-trascurabile ☐ 2-bassa ☐ 3-media ☐ 4-alta ☐ 5-molto alta ☐ 6-assoluta	A-B Tipo di misure ☐ 1-tecniche (strutturali, ambientali, elettroniche) ☐ 2-organizzative (umane)

4.4.6 Sui Soggetti

L'elemento "Soggetti" ricorre nelle attività all'interno delle quali si gestiscono (trattano) dati personali, che per questo la fanno ricadere nel Regolamento UE 2016/679. Da notare che il Titolare rappresenta a tutti gli effetti l'organizzazione che agisce (svolge l'attività).

Questo elemento consente di attribuire i danni prodotti da un'incidente ad uno o più dei Soggetti coinvolti nell'attività.

Tabella 8 – Soggetti (Elemento 8)	
☐ Organizzazione ☐ Titolare	☐ Responsabile ☐ Contitolare

[13] Nel Modello di notifica al Garante in caso di data breach, sezione C punto 7, sono individuate 4 "Cause della violazione" che raggruppano le vulnerabilità presentate dai mezzi e le minacce ai quali sono esposti.

4.4.7 Considerazioni

1. Le attività possono essere svolte utilizzando una modalità manuale, elettronica o mista, che comprende sempre sia mezzi "fisici" (personale, logistica, tecnologie) sia mezzi "organizzativi" (proceduralizzazione dell'attività) ([14]).
2. L'insieme dei mezzi (personale, logistica, tecnologie, organizzazione) abilita e supporta le operazioni previste dalla modalità stessa.
3. Le minacce esogene all'attività sono costituite dai pericoli ai quali sono esposti i mezzi impiegati. Le minacce endogene all'attività sono costituite dalle vulnerabilità che manifestano i mezzi impiegati. Ogni minaccia ha una specifica probabilità di manifestazione e gravita di danno che può procurare.
4. Le misure sono inserite tra le caratteristiche delle attività in quanto:
    a. quelle Embedded sono da intendersi come "qualità" dei mezzi impiegati che ne riduce i punti di debolezza (le vulnerabilità);
    b. quelle Add in, pur essendo "aggiunte" ai mezzi per renderli più sicuri, nella realtà sono sempre presenti facendo parte integrante dell'attività, a meno che non sia ancora stata avviata e quindi la valutazione del rischio (e d'impatto) è proprio finalizzata alla loro individuazione.

4.5 La modalità manuale

Per modalità manuale di svolgimento di tutta o parte di un'attività si intende l'insieme di:

a. asset umani (competenza, esperienza, affidabilità del personale)
b. asset organizzativi (procedure, istruzioni operative, modulistica, linee-guida, ecc.)
c. asset logistici (uffici, archivi, CED, armadi, ecc.)
d. servizi di outsourcing documentale.

4.6 La modalità elettronica

Quando una parte (informatizzazione) o l'intera attività (digitalizzazione) è svolta con strumenti elettronici, la valutazione del rischio riguarda la sicurezza informatica, intesa come la "capacità di evitare un incidente al sistema informatico" e, di conseguenza, ai dati gestiti (trattati) dallo stesso. Per sistema informatico si intende l'insieme di:

a. asset umani (competenza, esperienza, affidabilità del personale)
b. asset organizzativi (procedure, istruzioni operative, outsourcing a terze parti, ecc.)
c. asset logistici (uffici, CED)
d. asset hardware (server, computer, device mobili)
e. asset software (di base e applicativo)
f. asset e servizi di networking (router e switch, linee voce-dati, accesso a Internet)
g. servizi di manutenzione e assistenza degli asset hardware-software
h. asset e servizi di cloud computing (interscambio file, storage, IaaS, PaaS, SaaS, ecc.).

[14] È per questo motivo che la ***sicurezza*** di qualsiasi modalità è sempre basata su ***misure sia organizzative che tecniche***.

4.7 Il fattore umano

In entrambe le modalità le persone hanno un ruolo fondamentale e discriminante, in quanto l'adeguato comportamento e l'utilizzo corretto dei mezzi a disposizione riduce la probabilità di rischio da incidenti accidentali, al netto di azioni dolose (minacce intenzionali), a meno del caso di mezzi che non concedono alternative e obbligano il comportamento (es. porta ad apertura con badge, password policy, ecc.).

Quindi i fattori che qualificano il "mezzo umano", potendo essere intesi come misure di sicurezza o al contrario come vulnerabilità, sono: 1.la proceduralizzazione dell'attività (gerarchia, responsabilità, controlli), 2.il coinvolgimento negli obiettivi aziendali (fidelizzazione), 3.il livello di competenza (nozioni), 4.il livello di capacità (esperienza).

5. IL MECCANISMO DI VALUTAZIONE DEL RISCHIO

In questo capitolo del documento è illustrato il meccanismo di valutazione del rischio ed il ciclo di operazioni di risk management.

5.1 Nuova formula di calcolo del rischio

È ora possibile raffinare la formula di calcolo del rischio in modo che prenda in considerazione i nuovi elementi costitutivi di un'attività:

$$R = f(P, D)$$

nella quale la complessità della funzione f dipende dai parametri che qualificano i due fattori P e D.

I parametri si identificano con gli elementi costitutivi dell'attività e con i loro fattori qualificanti, come individuati nel precedente Capitolo 4:

- il fattore P (probabilità) è funzione:
    1. delle minacce esogene alle quali sono esposti i mezzi impiegati (Elemento 6A)
    2. delle minacce endogene (Elemento 6 B) originate
        - dalle caratteristiche dell'attività (Elemento 1)
        - dalla modalità utilizzata (Elemento 4)
        - dai mezzi impiegati (Elemento 5)
    3. dalla probabilità di manifestazione e dalla gravità delle minacce (Elemento 6 A-B)
- il fattore D (danno) è funzione:
    1. della qualità dell'oggetto danneggiato (persone, beni e dati, mezzi, soggetti, attività) che determina la gravità "oggettiva" del danno
    2. del tipo di danno (fisico, materiale, immateriale) provocato dall'incidente all'oggetto
    3. della gravità del danno provocato all'oggetto (persone, dati, mezzi) dall'incidente.

5.1.1 Considerazioni

1. Come emerso nel precedente Capitolo 4, tra i fattori che qualificano gli elementi che costituiscono un'attività sono presenti:
    - le misure tecniche e organizzative
    - i dati, intesi come "bene" oggetto diretto o indiretto dell'attività.
2. L'introduzione delle misure genera la necessità di valutare il rischio in assenza o in presenza di misure di contrasto, richiedendo di variare la formula di calcolo per valutare:
    a. il rischio potenziale (R^p) quando non si tiene conto delle misure in atto
    b. il rischio effettivo (R^e) quando si tiene conto delle misure in atto.
3. Le misure e la conseguente valutazione di rischi diversi innescano il "ciclo di gestione del rischio".

4. L'identificazione dei beni nei dati, in particolare personali, richiede di prendere in considerazione i requisiti di sicurezza (riservatezza, integrità, disponibilità) ai quali sono soggetti.
5. L'introduzione dei requisiti di sicurezza richiede di stimare i diversi valori di danno (D-r, D-i, D-d).
6. In presenza di tre diversi valori del danno, la formula R = f (P, D) produce tre diversi valori di rischio: Rr = f (P, Dr), Ri = f (P, Di), Rd = f (P, Dd).
7. Il danno con il valore più alto tra i tre è quello che determina il valore del rischio ai diritti e alle libertà delle persone fisiche (criterio già presentato nel precedente Paragrafo 3.2).
8. In ambito privacy la violazione dei dati personali può produrre danni ai diritti e alle libertà delle persone fisiche, proprietarie dei dati stessi, danni generati dalla perdita dei requisiti di sicurezza (riservatezza, integrità, disponibilità) dei mezzi stessi e dei dati personali con essi gestiti.

5.2 Variazioni della formula di calcolo del rischio

Alla luce delle considerazioni 5.1.1, è possibile e necessario ri-scrivere la formula di calcolo del rischio orientandola nel campo della privacy (danni ai dati come perdita dei requisiti di sicurezza) e differenziandola con l'introduzione delle misure di contrasto per valutare il rischio potenziale ed il rischio effettivo.

5.2.1 Formula del rischio potenziale (o intrinseco o inerente)

$$R^p = f\,(P,\ D^m)$$

nella quale il Rischio potenziale (R^p) è il prodotto della Probabilità di accadimento dell'incidente (P) per il Danno massimo (D^m) ad uno dei tre requisiti di sicurezza [(danno alla riservatezza (Di), danno all'integrità (Di), danno alla disponibilità (Dd)].

5.2.2 Formula del rischio effettivo (o residuo)

$$R^e = f\,[(P\text{-}M),\ D^m)]$$

nella quale il Rischio effettivo (R^e) è il prodotto della Probabilità di accadimento dell'incidente (P), abbassata dalle misure in atto (M), per il Danno massimo (D^m) ad uno dei tre requisiti di sicurezza [(danno alla riservatezza (D-), danno all'integrità (Di), danno alla disponibilità (Dd)].

5.2.3 Utilizzo delle scale di valori

Per la applicazione concreta delle formule risultano utili queste scale di valori:

- il rischio potenziale è qualitativamente individuato dai quantitativi della P e del D
- le altre scale sono utilizzate in base alle scelte dell'auditor.

			Gravità della violazione (D)			
			Trascurabile	Bassa	Media	Alta
			1	2	3	4
Probabilità di accadimento (P)	Improbabile	1	1	2	3	4
	Poco Prob.	2	2	4	6	8
	Probabile	3	3	6	9	12
	Molto Prob.	4	4	8	12	16

Rischio potenziale (P)			
Basso	Medio	Alto	Molto alto
1-3	4-6	8-9	12-16

Efficacia delle misure			
Insufficiente	Minima	Adeguata	Ottimale
1	2	3	4

Rischio effettivo			
Basso	Medio	Alto	Molto alto
1	2	3	4

Gravità dell'impatto			
Lieve	Medio	Grave	Gravissimo
1	2	3	4

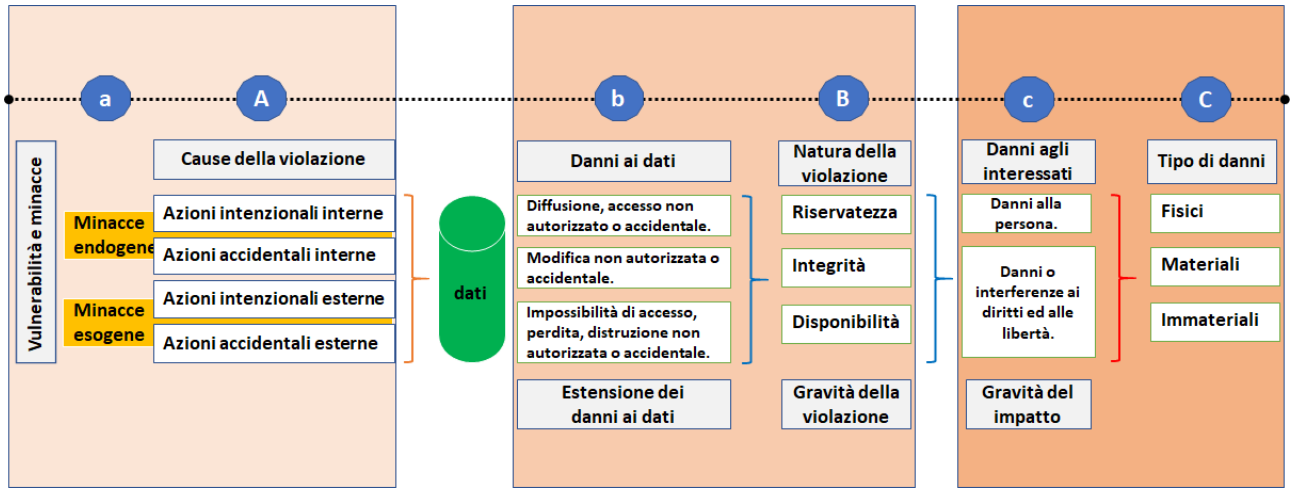
5.3 Sulle cause e gli effetti degli incidenti

L'incidente in cui può incorrere un'attività è sempre il risultato del concretizzarsi di una minaccia che coinvolge con un diverso peso gli elementi costitutivi (mezzi impiegati, beni, persone fisiche), producendo effetti negativi, i danni, sui diversi elementi e sull'attività stessa.

Quando l'incidente riguarda i dati (ed i mezzi con cui sono gestiti) si parla di violazione, e i danni sono valutati in perdita parziale o totale dei tre requisiti di sicurezza (riservatezza, integrità e disponibilità) dei dati (e dei mezzi con cui sono gestiti).

I vari fattori che entrano in gioco in caso di incidente sono legati tra loro da un rapporto causa-effetto del quale si fornisce la rappresentazione grafica.

Rappresentazione grafica dei rapporti causa-effetto



5.3.1 Tipologie di fattori di cause di incidenti e danni

Nella tabella 9 sono contenute tutte le variabili relative a cause di incidenti, danni ai dati e ai diritti.

Tabella 9.1 Azioni intenzionali interne.

Vulnerabilità e minacce (tab.9-10-11)	Cause della violazione	Natura della violazione	Danni ai dati	Estensione dei danni ai dati	Gravità della violazione dei dai	Conseguenze violazione dei requisiti di sicurezza dei dati	Danni agli interessati	Tipi di danni agli Interessati	Gravità dell'impatto sui diritti
☐ Infedeltà	☐ **Azioni intenzionali interne**	☐ **Perdita riservatezza**	☐ accesso non autorizzato (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ divulgazione al di fuori di quanto previsto (informativa) (*)	☐ pregiudizio alla reputazione (C 75, 85)	☐ Fisico	☐ 1-Lieve
☐ Corruzione			☐ decifratura non autorizzata della pseudonimizzazione (C 75, 85)	☐ parziale (buona parte)	☐ 2-Bassa	☐ correlazione facile ad altre informazioni relative agli interessati (*)	☐ discriminazioni (C 75, 85)	☐ Materiale	☐ 2-Medio
☐ Terrorismo, sabotaggio			☐ rivelazione non autorizzata (C 83)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ utilizzazione per finalità diverse da quelle previste (informativa) (*)	☐ danno sociale significativo (C 75, 85)	☐ Immateriale	☐ 3-Grave
☐ Carenti misure di controllo (es. ispezione log)			☐ diffusione non autorizzata (*)	☐ totale (tutti i dati)	☐ 4-Alta	☐ utilizzazione illecita (*)	☐ perdite finanziarie (C 75, 85)		☐ 4-Gravissimo
☐ Carente protezione accesso fisico ai siti (archivi, CED)			☐ perdita di riservatezza dei dati personali protetti da segreto professionale (C 75, 85)				☐ perdite patrimoniali		
			☐ furto o usurpazione d'identità (C 75, 85, 88)				☐ danno economico significativo (C 75)		
		☐ **Perdita integrità**	☐ modifica non autorizzata (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ dati modificati o inconsistenti (*)	☐ rifiuto o mancato accesso ai servizi	☐ Fisico	☐ 1-Lieve
				☐ parziale (buona parte)	☐ 2-Bassa	☐ dati modificati e consistenti (*)	☐ impedimento o perdita del controllo dei dati personali (limitazione soddisfazione dei diritti) (C 75, 85, 94)	☐ Materiale	☐ 2-Medio
				☐ consistente (larga parte di dati)	☐ 3-Media				☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta			☐ Immateriale	☐ 4-Gravissimo
		☐ **Perdita disponibilità**	☐ distruzione illegale (C 83)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ mancato accesso ai servizi (*)		☐ Fisico	☐ 1-Lieve
			☐ distruzione non autorizzata (*)	☐ parziale (buona parte)	☐ 2-Bassa	☐ malfunzionamento o difficoltà utilizzo (*)		☐ Materiale	☐ 2-Medio
			☐ impossibilità di accesso (*)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ impedimento dell'esercizio (Artt. 15-21) del controllo sui dati personali (C75)		☐ Immateriale	☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta				☐ 4-Gravissimo

Tabella 9.2 Azioni accidentali interne

☐ Insufficiente competenza	**☐ Azioni accidentali interne**	**☐ Perdita riservatezza**	☐ accesso accidentale (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ divulgazione al di fuori di quanto previsto (informativa) (*)	☐ pregiudizio alla reputazione (C 75, 85)	☐ Fisico	☐ 1-Lieve
☐ Mancato rispetto procedure			☐ diffusione accidentale (*)	☐ parziale (buona parte)	☐ 2-Bassa	☐ correlazione facile ad altre informazioni relative agli interessati (*)	☐ discriminazioni (C 75, 85)	☐ Materiale	☐ 2-Medio
☐ Insufficienze esperienza			☐ perdita di riservatezza dei dati personali protetti da segreto professionale (C 75, 85)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ utilizzazione per finalità diverse da quelle previste (informativa) (*)	☐ danno sociale significativo (C 75, 85)	☐ Immateriale	☐ 3-Grave
☐ Errore accidentale (distrazione, stanchezza)				☐ totale (tutti i dati)	☐ 4-Alta	☐ utilizzazione illecita (*)	☐ perdite finanziarie (C 75, 85)		☐ 4-Gravissimo
☐ Carente organizzazione (es. procedure)		**☐ Perdita integrità**	☐ modifica accidentale (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ dati modificati o inconsistenti (*)	☐ perdite patrimoniali	☐ Fisico	☐ 1-Lieve
☐ Carenti misure di controllo (es. audit)				☐ parziale (buona parte)	☐ 2-Bassa	☐ dati modificati e consistenti (*)	☐ danno economico significativo (C 75)	☐ Materiale	☐ 2-Medio
☐ Carenti misure di dissuasione (es. sanzioni, ispezione log)				☐ consistente (larga parte di dati)	☐ 3-Media		☐ rifiuto o mancato accesso ai servizi		☐ 3-Grave
☐ Carente misure antincendio				☐ totale (tutti i dati)	☐ 4-Alta		☐ impedimento o perdita del controllo dei dati personali (limitazione soddisfazione dei diritti) (C 75, 85, 94)	☐ Immateriale	☐ 4-Gravissimo
☐ Carente impianto condizionamento		**☐ Perdita disponibilità**	☐ distruzione accidentale (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ mancato accesso ai servizi (*)		☐ Fisico	☐ 1-Lieve
☐ Carente impianto continuità elettrica			☐ perdita (C 83) (*)	☐ parziale (buona parte)	☐ 2-Bassa	☐ malfunzionamento o difficoltà utilizzo (*)		☐ Materiale	☐ 2-Medio
☐ Carente manutenzione dei sistemi			☐ impossibilità di accesso (*)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ impedimento dell'esercizio (Artt. 15-21) del controllo sui dati personali (C75)		☐ Immateriale	☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta				☐ 4-Gravissimo

Tabella 9.3 Azioni intenzionali esterne

☐ Carente protezione accesso fisico ai siti (archivi, CED)	**☐ Azioni intenzionali esterne**	**☐ Perdita riservatezza**	☐ accesso non autorizzato (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ divulgazione al di fuori di quanto previsto (informativa) (*)	☐ pregiudizio alla reputazione (C 75, 85)	☐ Fisico	☐ 1-Lieve
☐ Carente protezione accesso logico ai sistemi			☐ decifratura non autorizzata della pseudonimizzazione (C 75, 85)	☐ parziale (buona parte)	☐ 2-Bassa	☐ correlazione facile ad altre informazioni relative agli interessati (*)	☐ discriminazioni (C 75, 85)	☐ Materiale	☐ 2-Medio
☐ Carente protezione dei sistemi (es. antivirus)			☐ rivelazione non autorizzata (C 83)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ utilizzazione per finalità diverse da quelle previste (informativa) (*)	☐ danno sociale significativo (C 75, 85)	☐ Immateriale	☐ 3-Grave
☐ Carente protezione delle reti (es. firewall)			☐ diffusione non autorizzata (*)	☐ totale (tutti i dati)	☐ 4-Alta	☐ utilizzazione illecita (*)	☐ perdite finanziarie (C 75, 85)		☐ 4-Gravissimo
☐ Carente monitoraggio delle reti			☐ perdita di riservatezza dei dati personali protetti da segreto professionale (C 75, 85)				☐ perdite patrimoniali		
☐ Carente politica di hardening			☐ furto o usurpazione d'identità (C 75, 85, 88)				☐ danno economico significativo (C 75)		
☐ Carente vulnerability assessment		**☐ Perdita integrità**	☐ modifica non autorizzata (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ dati modificati o inconsistenti (*)	☐ rifiuto o mancato accesso ai servizi	☐ Fisico	☐ 1-Lieve
☐ Carente penetration test				☐ parziale (buona parte)	☐ 2-Bassa	☐ dati modificati e consistenti (*)	☐ impedimento o perdita del controllo dei dati personali (limitazione soddisfazione dei diritti) (C 75, 85, 94)	☐ Materiale	☐ 2-Medio
				☐ consistente (larga parte di dati)	☐ 3-Media				☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta			☐ Immateriale	☐ 4-Gravissimo
		☐ Perdita disponibilità	☐ distruzione illegale (C 83)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ mancato accesso ai servizi (*)		☐ Fisico	☐ 1-Lieve
			☐ distruzione non autorizzata (*)	☐ parziale (buona parte)	☐ 2-Bassa	☐ malfunzionamento o difficoltà utilizzo (*)		☐ Materiale	☐ 2-Medio
			☐ impossibilità di accesso (*)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ impedimento dell'esercizio (Artt. 15-21) del controllo sui dati personali (C75)		☐ Immateriale	☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta				☐ 4-Gravissimo

Tabella 9.4 Azioni accidentali esterne

☐ Carenza strutture edili dei siti	**☐ Azioni accidentali esterne**	**☐ Perdita riservatezza**	☐ accesso accidentale (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ divulgazione al di fuori di quanto previsto (informativa) (*)	☐ pregiudizio alla reputazione (C 75, 85)	☐ Fisico	☐ 1-Lieve
☐ Insufficiente distanza di sicurezza dei siti			☐ diffusione accidentale (*)	☐ parziale (buona parte)	☐ 2-Bassa	☐ correlazione facile ad altre informazioni relative agli interessati (*)	☐ discriminazioni (C 75, 85)	☐ Materiale	☐ 2-Medio
☐ Insufficiente sopraelevazione dei siti			☐ perdita di riservatezza dei dati personali protetti da segreto professionale (C 75, 85)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ utilizzazione per finalità diverse da quelle previste (informativa) (*)	☐ danno sociale significativo (C 75, 85)	☐ Immateriale	☐ 3-Grave
☐ Insufficiente isolamento elettromagnetico				☐ totale (tutti i dati)	☐ 4-Alta	☐ utilizzazione illecita (*)	☐ perdite finanziarie (C 75, 85)		☐ 4-Gravissimo
☐ Inondazione							☐ perdite patrimoniali		
☐ Frana, terremoto, eruzione		**☐ Perdita integrità**	☐ modifica accidentale (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ dati modificati o inconsistenti (*)	☐ danno economico significativo (C 75)	☐ Fisico	☐ 1-Lieve
☐ Balckout elettrico				☐ parziale (buona parte)	☐ 2-Bassa	☐ dati modificati e consistenti (*)	☐ rifiuto o mancato accesso ai servizi	☐ Materiale	☐ 2-Medio
☐ Coinvolgimento in un incidente auto				☐ consistente (larga parte di dati)	☐ 3-Media		☐ impedimento o perdita del controllo dei dati personali (limitazione soddisfazione dei diritti) (C 75, 85, 94)		☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta			☐ Immateriale	☐ 4-Gravissimo
		☐ Perdita disponibilità	☐ distruzione accidentale (C 83) (*)	☐ minima (piccola parte)	☐ 1-Trascurabile	☐ mancato accesso ai servizi (*)		☐ Fisico	☐ 1-Lieve
			☐ perdita (C 83) (*)	☐ parziale (buona parte)	☐ 2-Bassa	☐ malfunzionamento o difficoltà utilizzo (*)		☐ Materiale	☐ 2-Medio
			☐ impossibilità di accesso (*)	☐ consistente (larga parte di dati)	☐ 3-Media	☐ impedimento dell'esercizio (Artt. 15-21) del controllo sui dati personali (C75)		☐ Immateriale	☐ 3-Grave
				☐ totale (tutti i dati)	☐ 4-Alta				☐ 4-Gravissimo

5.3.2 Danni fisici alle persone

L'integrità fisica delle persone - fino al limite della morte -è minacciata:

- direttamente dall'accadimento di minacce naturali e ambientali, sia accidentali che intenzionali esterne e interne che riguardano i siti fisici (uffici, magazzini, archivi, sale CED) come incendi, allagamenti, cortocircuiti, crolli, incidenti di vario tipo, ecc.;
- indirettamente da azioni sia accidentali che intenzionali esterne e interne che generano il mancato accesso ai servizi (es. di assistenza sanitaria) la modifica dell'integrità dei dati che determina l'esecuzione di azioni errate o la mancata esecuzioni di azioni vitali.

Nella tabella 10 esempi di cause, incidenti, danni fisici.

Tabella 10 – danni fisici alle persone		
Cause (vulnerabilità e minacce)	Incidenti	Danni fisici
☐ Carente impianto elettrico ☐ Impianto antincendio inefficace ☐ Armadi e contenitori malfermi ☐ Inesperienza, distrazione ☐ Inondazione ☐ Frana, terremoto, eruzione	☐ Cortocircuito ☐ Incendio ☐ Caduta di armadi o contenitori ☐ Incidente con apparecchiature / auto ☐ Allagamento ☐ Distruzione	☐ folgorazione ☐ ustione ☐ schiacciamento ☐ trauma ☐ affogamento ☐ schiacciamento

5.3.3 Danni all'attività e ai soggetti

L'incidente occorso ad uno o più elementi costitutivi dell'attività produce un danno all'attività stessa intesa come processo di esecuzione delle diverse operazioni.

A sua volta, i danni ad un'attività producono danni ai Soggetti coinvolti, che ai fini privacy possono essere il Titolare, il Responsabile, il Contitolare, constatabili realmente solo ex post l'incidente stesso.

Nella tabella 11 sono individuate le cause in grado di provocare un incidente, i tipi di incidenti, gli effetti secondari sul processo, i diversi tipi di danni all'organizzazione (Titolare).

Tabella 11 – Danni all'attività					
Cause (vulnerabilità e minacce)	Incidenti	Effetti secondari	Danni immateriali	Danni materiali	Danni fisici

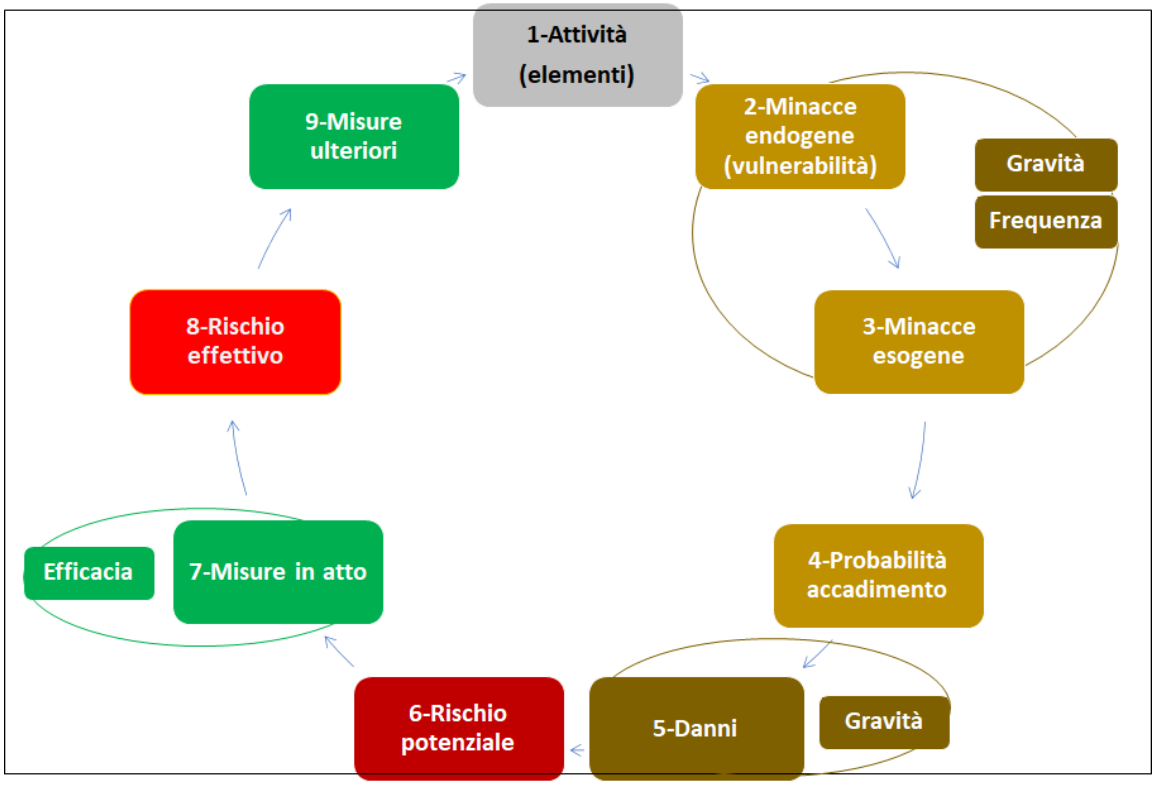
☐ azioni accidentali interne ed esterne ☐ azioni intenzionali interne ed esterne ☐ assenza o inadeguatezza della qualità dei mezzi impiegati ☐ assenza o inadeguatezza delle misure di protezione dei mezzi impiegati	☐ danneggiamento o distruzione di un mezzo fisico o tecnico utilizzato per svolgere l'attività ☐ danneggiamento di una persona che opera all'interno dell'attività	☐ ritardo dell'attività ☐ blocco dell'attività ☐ output dell'attività non conforme ☐ violazione dei requisiti di sicurezza dei dati ☐ violazione dei diritti degli Interessati	☐ perdita del cliente ☐ caduta del prestigio ☐ perdita della reputazione ☐ perdita della competitività	☐ annullamento contratto ☐ penale ☐ risarcimento del danno ☐ aumento polizza assicurativa ☐ causa civile ☐ causa penale ☐ pagamento riscatto ☐ sanzione amministrativa ☐ perdita delle certificazioni	Solo quando il soggetto è anche una persona fisica che svolge o è coinvolta nell'attività

5.4 Ciclo di gestione del rischio

Come emerso nelle considerazioni 5.1.1 è possibile stabilire le fasi che logicamente e cronologicamente compongono il "ciclo di gestione del rischio":

1. Analisi delle caratteristiche dell'attività (caratteristiche, modalità e mezzi)
2. Determinazione delle vulnerabilità
3. Determinazione delle minacce (gravità e frequenza di manifestazione)
4. Determinazione della probabilità di accadimento (fattore P)
5. Stima dei danni (fattore D)
6. Livello di rischio potenziale (in quanto al netto delle contromisure)
7. Misure in atto (o previste nel caso l'attività non sia ancora in corso)
8. Livello di rischio effettivo (in quanto al lordo delle contromisure)
9. Misure ulteriori (da adottare per abbassare il livello di rischio effettivo).

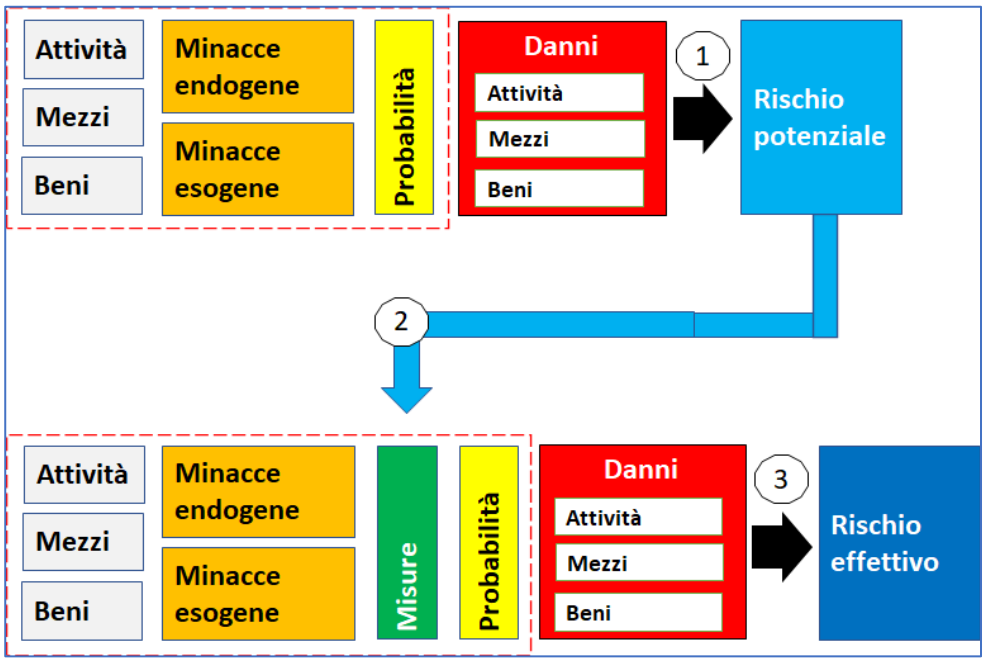
Rappresentazione grafica del ciclo di gestione del rischio



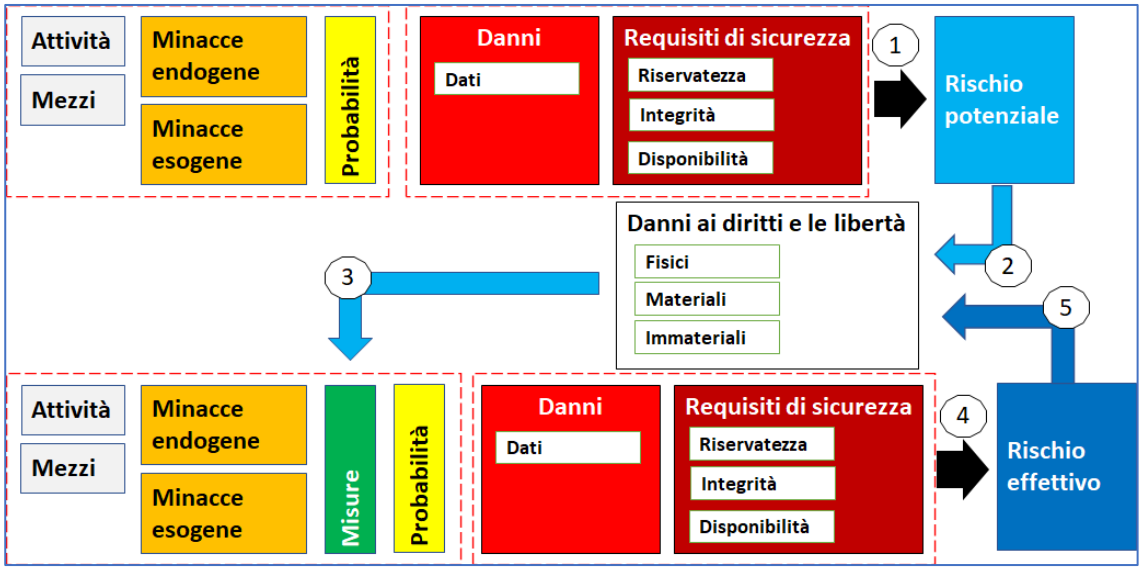
5.5 Rappresentazione grafica dei processi di valutazione

In base alle nuove formule di calcolo illustrate nel paragrafo 5.2, estendendo gli effetti dei rischi sui diritti degli Interessati, si possono rappresentare graficamente i processi di valutazione del rischio e d'impatto.

Rappresentazione grafica della valutazione del rischio



Rappresentazione grafica del ciclo della valutazione d'impatto



6. ESEMPIO DI APPLICAZIONE DEL MECCANISMO DI VALUTAZIONE

In questo capitolo, assunto che la valutazione del rischio è parte integrante della valutazione d'impatto, e premessa l'analisi svolta nel precedente Capitolo 4, con l'esempio che segue si intende dimostrare:

- l'efficacia della suddivisione dell'attività nei suoi elementi costitutivi e fattori qualificanti,
- l'applicabilità della logica descritta nel precedente Capitolo 5
- la possibilità di determinare il rischio per i diritti e le libertà delle persone fisiche.

6.1 Presentazione dell'esempio

L'attività presa in esame è la "produzione e la refertazione di un esame radiologico", attività che è scomponibile in queste sub-attività:

1. prenotazione dell'esame con raccolta e registrazione del nome del Paziente e del tipo di esame
2. raccolta e registrazione dei dati del Paziente e della prescrizione medica, accettazione e fatturazione dell'esame
3. produzione dell'esame
4. refertazione dell'esame
5. consegna del referto al Paziente
6. archiviazione della copia del referto stampato e firmato.

L'analisi è formalizzata in una serie di tabelle di dati così organizzate:

- ❖ prima parte
  - colonna A - sub-attività
  - colonna B - mezzi impiegati per svolgerla
  - cause e possibili incidenti
    - colonna C1 - da vulnerabilità evidenziate dai mezzi
    - colonna C2 - da minacce alle quali sono esposti i mezzi
    - colonna C3 - tipo di causa della violazione ([15])
  - colonna D - probabilità di accadimento delle minacce
  - colonna E1 - danni prodotti ai dati (requisiti di sicurezza) ([16])
  - colonna E2 - gravità della violazione ([17])
  - colonna F - rischio potenziale
- ❖ seconda parte
  - colonna G - misure tecniche e organizzative in atto

[15] Modello di notifica del Data Breach del Garante - Sez. C - Informazioni di sintesi sulla violazione - Punto 7
[16] Modello di notifica del Data Breach del Garante - Sez. C - Informazioni di sintesi sulla violazione - Punto 6
[17] Modello di notifica del Data Breach del Garante - Sezione E - Stima della gravità della violazione – punto 3

- colonna H – rischio effettivo
- colonna L1 - natura della violazione ([18])
- colonna L2 - conseguenze violazione sugli Interessati ([19])
- colonna L3 – impatto sui diritti degli Interessati
- colonna L4 - tipi di danni agli Interessati
- colonna L5 – gravità dell'impatto
- colonna M1 - danni al Titolare o all'organizzazione.

[18] Note al Punto 6 - Sez. C - Informazioni di sintesi sulla violazione del Modello di notifica del Data Breach del Garante

[19] Modello di notifica del Data Breach del Garante - Sezione E - Possibili conseguenze e gravità della violazione - punto 1°, 1b, 1c

Tabella sub-attività 1 prima parte

A	B	C1	C2	C3	D	E1	E2	F
Contesto		Cause			P	Danni		Rp
Attività (sub attività)	Mezzi impiegati	Vulnerabilità	Minacce	Tipo-causa violazione	Probabilità accadimento minacce	Danni ai dati	Gravità violazione	Rischio potenziale
1. prenotazione dell'esame con raccolta e registrazione del nome del Paziente e del tipo di esame	Sistema RIS.PACS	Obsolescenza del RIS.PACS	Malfunzionamento del sistema RIS.PACS	☐ Azione intenzionale interna	☐ 1-improbabile	☐ Riservatezza	☐ 1-trascurabile	☐ 1-basso
	Personale di segreteria	Incompetenza o distrazione dell'addetto	Errata registrazione dei dati	☐ Azione accidentale interna	☐ 2-poco probabile	☐ Integrità	☐ 2-basso	☐ 2-medio
			Errata pianificazione della data	☐ Azione intenzionale esterna	☐ 3-probabile	☐ Disponibilità	☐ 3-medio	☐ 3-alto
				☐ Azione accidentale esterna	☐ 4-molto probabile		☐ 4-alto	☐ 4-altissimo
				☐ Sconosciuta				
				☐ Altro (specificare)				

Tabella sub-attività 1 seconda parte

A	F	G	H	L1	L2	L3	L4	L5	M1
Contesto	Rp	M	Re	Impatti					Danni
Attività (sub attività)	**Rischio potenziale**	**Misure in atto**	**Rischio effettivo**	**Natura della violazione**	**Conseguenze violazione su Interessati**	**Impatto sui diritti Interessati**	**Tipo danni a Interessati**	**Gravità dell'impatto**	**Al Titolare** (organizzazione)
1. prenotazione dell'esame con raccolta e registrazione del nome del Paziente e del tipo di esame	**☐ 1-basso**	Sistema RIS.PACS aggiornato	**☐ 1-basso**	☐ 1-diffusione ☐ 2-accesso non autorizzato o accidentale	Riservatezza ☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro		☐ Fisici	**☐ 1-Lieve**	Perdita economica
	☐ 2-medio	**Personale addestrato**	☐ 2-medio	**☐ 1-modifica non autorizzata o accidentale**	**☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro**	**Contratto non rispettato**	**☐ Materiali**	☐ 2-Medio	Perdita di immagine
	☐ 3-alto	**Istruzioni disponibili**	☐ 3-alto	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro		☐ Immateriali	☐ 3-Grave	Disdetta esame
	☐ 4-altissimo		☐ 4-altissimo					☐ 4-Gravissimo	

Tabella sub-attività 2 prima parte

A	B	C1	C2	C3	D	E1	E2	F
Contesto		Cause			P	Danni		Rp
Attività (sub attività)	**Mezzi impiegati**	**Vulnerabilità**	**Minacce**	**Tipo-causa violazione**	**Probabilità accadimento minacce**	**Danni ai dati**	**Gravità violazione**	**Rischio potenziale**
2. raccolta e registrazione dei dati del Paziente e della prescrizione medica, accettazione e fatturazione dell'esame	Sistema RIS.PACS	Obsolescenza del RIS.PACS	Malfunzionamento del RIS.PACS	☐ Azione intenzionale interna	**☐ 1-improbabile**	☐ Riservatezza	**☐ 1-trascurabile**	**☐ 1-basso**
	Personale di segreteria	**Incompetenza o distrazione dell'addetto**	**Errata fatturazione**	**☐ Azione accidentale interna**	☐ 2-poco probabile	**☐ Integrità**	☐ 2-basso	☐ 2-medio
			Errato esame da produrre	☐ Azione intenzionale esterna	☐ 3-probabile	☐ Disponibilità	☐ 3-medio	☐ 3-alto
				☐ Azione accidentale esterna	☐ 4-molto probabile		☐ 4-alto	☐ 4-altissimo
				☐ Sconosciuta				
				☐ Altro (specificare)				

Tabella sub-attività 2 seconda parte

A	F	G	H	L1	L2	L3	L4	L5	M1
Contesto	Rp	M	Re	Impatti					Danni
Attività (sub attività)	**Rischio potenziale**	**Misure in atto**	**Rischio effettivo**	**Natura della violazione**	**Conseguenze violazione su Interessati**	**Impatto sui diritti Interessati**	**Tipo danni a Interessati**	**Gravità dell'impatto**	**Al Titolare** (organizzazione)
2. raccolta e registrazione dei dati del Paziente e della prescrizione medica, accettazione e fatturazione dell'esame	**☐ 1-basso**	Sistema RIS.PACS aggiornato	**☐ 1-basso**	☐ 1-diffusione ☐ 2-accesso non autorizzato o accidentale	☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro		☐ Fisici	**☐ 1-Lieve**	Perdita economica
	☐ 2-medio	**Personale addestrato**	☐ 2-medio	**☐ 1-modifica non autorizzata o accidentale**	**☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro**	**Contratto non rispettato**	**☐ Materiali**	☐ 2-Medio	Perdita di immagine
	☐ 3-alto	**Istruzioni disponibili**	☐ 3-alto	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro		☐ Immateriali	☐ 3-Grave	Disdetta esame
	☐ 4-altissimo		☐ 4-altissimo					☐ 4-Gravissimo	Invalidità della fattura

Tabella sub-attività 3 prima parte

A	B	C1	C2	C3	D	E1	E2	F
Contesto		Cause			P	Danni		Rp
Attività (sub attività)	**Mezzi impiegati**	**Vulnerabilità**	**Minacce**	**Tipo-causa violazione**	**Probabilità accadimento minacce**	**Danni ai dati**	**Gravità violazione**	**Rischio potenziale**
3. Produzione e registrazione dell'esame	Sistema RIS.PACS	Obsolescenza del RIS.PACS	Malfunzionamento del RIS.PACS	☐ Azione intenzionale interna	**☐ 1-improbabile**	☐ Riservatezza	☐ 1-trascurabile	☐ 1-basso
	Tecnico e Medico radiologo	**Incompetenza o distrazione del Tecnico**	**Errore di utilizzo del RIS.PACS**	**☐ Azione accidentale interna**	☐ 2-poco probabile	**☐ Integrità**	☐ 2-basso	**☐ 2-medio**
		Insufficienti misure di protezione del sistema	Violazione del sistema RIS (accesso non autorizzato, alterazione dei dati registrati, blocco della registrazione)	☐ Azione intenzionale esterna	☐ 3-probabile	☐ Disponibilità	☐ 3-medio	☐ 3-alto
				☐ Azione accidentale esterna	☐ 4-molto probabile		**☐ 4-alto**	☐ 4-altissimo
				☐ Sconosciuta				
				☐ Altro (specificare)				

Tabella sub-attività 3 seconda parte

A	F	G	H	L1	L2	L3	L4	L5	M1
Contesto	Rp	M	Re	Impatti					Danni
Attività (sub attività)	**Rischio potenziale**	**Misure in atto**	**Rischio effettivo**	**Natura della violazione**	**Conseguenze violazione su Interessati**	**Impatto sui diritti Interessati**	**Tipo danni a Interessati**	**Gravità dell'impatto**	**Al Titolare** (organizzazione)
3. Produzione e registrazione dell'esame	☐ 1-basso	Sistema RIS.PACS aggiornato	**☐ 1-basso**	☐ 1-diffusione ☐ 2-accesso non autorizzato o accidentale	☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro	Riservatezza discriminazione (C75,85)	**☐ Fisici**	☐ 1-Lieve	Perdita economica Risarcimenti e sanzioni Aumento premio polizza Causa civile o penale
	☐ 2-medio	**Personale addestrato**	☐ 2-medio	**☐ 1-modifica non autorizzata o accidentale**	**☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro**	Riservatezza pregiudizio alla reputazione (C75,85)	**☐ Materiali**	**☐ 2-Medio**	Perdita di immagine Diffusione dati riservati
	☐ 3-alto	**Istruzioni disponibili**	☐ 3-alto	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro	Riservatezza perdita della riservatezza dei dati personali protetti da segreto professionale (C75,85)	☐ Immateriali	☐ 3-Grave	Disdetta esame Indisponibilità dell'esame Produzione di un referto errato Produzione di un nuovo esame
	☐ 4-altissimo	Sistema PACS.RIS isolato da Internet	☐ 4-altissimo			Disponibilità impedimento dell'esercizio del controllo sui dati personali (C75) (accesso, rettifica, portabilità)		☐ 4-Gravissimo	
		Controllo del traffico di rete Meccanismo di gestione delle password							
		Profilazione degli utenti							
		Controllo dei log.utente							

Tabella sub-attività 4 prima parte

A	B	C1	C2	C3	D	E1	E2	F
Contesto		Cause			P	Danni		Rp
Attività (sub attività)	**Mezzi impiegati**	**Vulnerabilità**	**Minacce**	**Tipo-causa violazione**	**Probabilità accadimento minacce**	**Danni ai dati**	**Gravità violazione**	**Rischio potenziale**
4. refertazione dell'esame	Sistema RIS	Insufficiente chiarezza dell'esame prodotto		☐ Azione intenzionale interna	**☐ 1-improbabile**	☐ Riservatezza	☐ 1-trascurabile	☐ 1-basso
	Medico radiologo	**Incompetenza o distrazione del Medico**	**Errata interpretazione dell'esame (diagnosi)**	**☐ Azione accidentale interna**	☐ 2-poco probabile	**☐ Integrità**	☐ 2-basso	**☐ 2-medio**
		Infedeltà del Medico		☐ Azione intenzionale esterna	☐ 3-probabile	☐ Disponibilità	☐ 3-medio	☐ 3-alto
				☐ Azione accidentale esterna	☐ 4-molto probabile		**☐ 4-alto**	☐ 4-altissimo
				☐ Sconosciuta				
				☐ Altro (specificare)				

Tabella sub-attività 4 seconda parte

A	F	G	H	L1	L2	L3	L4	L5	M1
Contesto	Rp	M	Re	Impatti					Danni
Attività (sub attività)	Rischio potenziale	Misure in atto	Rischio effettivo	Natura della violazione	Conseguenze violazione su Interessati	Impatto sui diritti Interessati	Tipo danni a Interessati	Gravità dell'impatto	Al Titolare (organizzazione)
4. refertazione dell'esame	☐ 1-basso	Personale medico competente	☐ 1-basso	☐ 1-diffusione ☐ 2-accesso non autorizzato o accidentale	☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro		☐ Fisici	☐ 1-Lieve	Prescrizione di cure inadatte
	☐ 2-medio	Procedura obbligata di confronto con altro specialista	☐ 2-medio	☐ 1-modifica non autorizzata o accidentale	☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro	Contratto non rispettato	☐ Materiali	☐ 2-Medio	Perdita economica
	☐ 3-alto		☐ 3-alto	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro		☐ Immateriali	☐ 3-Grave	Perdita di immagine
	☐ 4-altissimo		☐ 4-altissimo					☐ 4-Gravissimo	Causa civile o penale

Tabella sub-attività 5 prima parte

A	B	C1	C2	C3	D	E1	E2	F
Contesto		Cause			P	Danni		Rp
Attività (sub attività)	Mezzi impiegati	Vulnerabilità	Minacce	Tipo-causa violazione	Probabilità accadimento minacce	Danni ai dati	Gravità violazione	Rischio potenziale
5. consegna del referto al Paziente	Personale di segreteria	**Incompetenza o distrazione dell'addetto**	**Consegna ad un terzo diverso dall'Interessato**	☐ Azione intenzionale interna	**☐ 1-improbabile**	**☐ Riservatezza**	**☐ 1-trascurabile**	**☐ 1-basso**
		Insufficienti misure di protezione dei referti		**☐ Azione accidentale interna**	☐ 2-poco probabile	☐ Integrità	☐ 2-basso	☐ 2-medio
		Infedeltà del dipendente		☐ Azione intenzionale esterna	☐ 3-probabile	**☐ Disponibilità**	**☐ 3-medio**	☐ 3-alto
				☐ Azione accidentale esterna	☐ 4-molto probabile		☐ 4-alto	☐ 4-altissimo
				☐ Sconosciuta				
				☐ Altro (specificare)				

Tabella sub-attività 5 seconda parte

A	F	G	H	L1	L2	L3	L4	L5	M1
Contesto	Rp	M	Re	Impatti					Danni
Attività (sub attività)	Rischio potenziale	Misure in atto	Rischio effettivo	Natura della violazione	Conseguenze violazione su Interessati	Impatto sui diritti Interessati	Tipo danni a Interessati	Gravità dell'impatto	Al Titolare (organizzazione)
5. consegna del referto al Paziente	**☐ 1-basso**	**Personale addestrato**	**☐ 1-basso**	**☐ 1-diffusione ☐ 2-accesso non autorizzato o accidentale**	**☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro**	Riservatezza discriminazione (C75,85)	☐ Fisici	**☐ 1-Lieve**	Perdita di immagine
	☐ 2-medio	**Istruzioni disponibili**	☐ 2-medio	☐ 1-modifica non autorizzata o accidentale	☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro	Riservatezza pregiudizio alla reputazione (C75,85)	☐ Materiali	☐ 2-Medio	Causa civile o penale
	☐ 3-alto	Referti conservati in armadio con serratura di sicurezza	☐ 3-alto	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro	**Riservatezza perdita della riservatezza dei dati personali protetti da segreto professionale (C75,85)**	**☐ Immateriali**	☐ 3-Grave	Risarcimenti e sanzioni
	☐ 4-altissimo	Controlli a campione non programmati	☐ 4-altissimo					☐ 4-Gravissimo	Aumento premio polizza

Tabella sub-attività 6 prima parte

A	B	C1	C2	C3	D	E1	E2	F
Contesto		Cause			P	Danni		Rp
Attività (sub attività)	**Mezzi impiegati**	**Vulnerabilità**	**Minacce**	**Tipo-causa violazione**	**Probabilità accadimento minacce**	**Danni ai dati**	**Gravità violazione**	**Rischio potenziale**
6. Conservazione referto	Personale di segreteria	Insufficienti misure di protezione delle copie	Incendio	**☐ Azione intenzionale interna**	☐ 1-improbabile	**☐ Riservatezza**	☐ 1-trascurabile	☐ 1-basso
		Infedeltà del dipendente	Furto	☐ Azione accidentale interna	**☐ 2-poco probabile**	☐ Integrità	☐ 2-basso	☐ 2-medio
			Distruzione	☐ Azione intenzionale esterna	☐ 3-probabile	☐ Disponibilità	☐ 3-medio	**☐ 3-alto**
			Copia non autorizzata	☐ Azione accidentale esterna	☐ 4-molto probabile		**☐ 4-alto**	☐ 4-altissimo
				☐ Sconosciuta				
				☐ Altro (specificare)				

Tabella sub-attività 6 seconda parte

A	F	G	H	L1	L2	L3	L4	L5	M1
Contesto	Rp	M	Re	Impatti					Danni
Attività (sub attività)	**Rischio potenziale**	**Misure in atto**	**Rischio effettivo**	**Natura della violazione**	**Conseguenze violazione su Interessati**	**Impatto sui diritti Interessati**	**Tipo danni a Interessati**	**Gravità dell'impatto**	**Al Titolare** (organizzazione)
6. Conservazione referto	☐ 1-basso	Armadio ignifugo con serratura di sicurezza	**☐ 1-basso**	**☐ 1-diffusione ☐ 2-accesso non autorizzato o accidentale**	**☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro**	Riservatezza pregiudizio alla reputazione (C75,85)	☐ Fisici	**☐ 1-Lieve**	Perdita di immagine
	☐ 2-medio	Nr. limitato di chiavi	☐ 2-medio	☐ 1-modifica non autorizzata o accidentale	☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro	**Riservatezza perdita della riservatezza dei dati personali protetti da segreto professionale (C75,85)**	☐ Materiali	☐ 2-Medio	Causa civile o penale
	☐ 3-alto	**Assegnazione delle chiavi**	☐ 3-alto	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro		**☐ Immateriali**	☐ 3-Grave	Risarcimenti e sanzioni
	☐ 4-altissimo	Controlli a campione non programmati	☐ 4-altissimo					☐ 4-Gravissimo	

6.2 Risultati della valutazione

6.2.1 Molteplicità di valori

L'analisi applicata ad un'attività suddivisa in 6 sub-attività produce differenti livelli di rischio effettivo di violazione dei tre requisiti di sicurezza (riservatezza, integrità, disponibilità) e gravità diverse di impatto sui diritti degli Interessati, per ognuna delle 6 sub-attività in cui è stato suddiviso per analizzarlo compiutamente.

Nell'esempio, per le prime cinque sub-attività sono state considerate le "azioni accidentali interne" quali cause di incidenti che possono generare anche rischi di livello medio (errore di utilizzo del software che produce un esame radiologico impreciso e l'errore di interpretazione dell'esame) e, soprattutto, possono comportare un impatto medio o grave e danni fisici; per la sesta sub-attività è stata considerata un'"azione intenzionale interna" (compiute dolosamente dal personale che opera all'interno dell'organizzazione) volta a effettuare una copia non autorizzata di un referto: in questo caso il rischio potenziale è alto (ma l'impatto è basso).

6.2.2 Individuazione del rischio

Il problema di individuare "il" rischio generato dall'intera attività ed il set di danni ai diritti ed alle libertà degli Interessati ad esso collegato si risolve seguendo la logica del "rischio potenziale maggiore" (calcolato sul tipo, gravità e probabilità delle minacce).

Dai valori presenti nella colonna F si evince che la sub-attività 6 di conservazione del referto è quella che, violata, può produrre un rischio potenziale maggiore.

6.2.3 Individuazione dell'impatto

Tuttavia, la gravità dell'impatto non è proporzionale al rischio, anche a quello effettivo, che pure è calcolato al netto delle misure in atto di contrasto alle azioni intenzionali esterne (nell'esempio, accesso fisico o logico non autorizzato) e accidentali interne (nell'esempio, distrazione, incompetenza).

Quella maggiore, infatti, si riscontra nella sub-attività 4 refertazione dell'esame: in questa fase un errore di distrazione può comportare una diagnosi errata con impatto "fisico" sul Paziente che non provvede ad iniziare una terapia.

6.2.4 Conclusioni

Nonostante lo sforzo di sistematizzare le valutazioni del rischio e d'impatto, occorre prendere atto che esse restano attività di tipo "qualitativo", che richiedono l'interpretazione delle informazioni raccolte: quindi i fattori discriminanti sono le competenze e le capacità dell'auditor e dell'avvocato.

7. IL MECCANISMO DI VALUTAZIONE D'IMPATTO

In questo capitolo si intende dimostrare che il significato degli elementi costitutivi di un'attività e dei loro fattori qualificanti individuati nei precedenti Capitoli 4 e 5 è comparabile con i contenuti della valutazione d'impatto relativi alla descrizione del trattamento, del rischio, delle minacce e delle misure, indicati nel Regolamento, nei Criteri WP 248/01, nel formato del CNIL.

Si rammenta che negli Allegati C ed E è stata effettuata la comparazione sistematica tra gli aspetti e le caratteristiche dei termini-chiave (rischio, trattamento, danno, valutazione d'impatto) presenti nelle norme sulla privacy e gli elementi costitutivi di un'attività ed i fattori qualificanti.

1. l'azione da svolgere/svolta (che può essere l'attività stessa)
2. i beni oggetto dell'azione (tra cui i dati)
3. le persone fisiche impiegate nell'azione o coinvolte dall'azione
4. la modalità utilizzata per agire
5. i mezzi impiegati nell'azione
6. le minacce alle quali sono esposti i mezzi (comprese le vulnerabilità che presentano)
7. le misure di contrasto alle minacce
8. i soggetti che a diverso titolo sono attivi (di cui il Titolare rappresenta l'organizzazione).

Tabella A – comparazione elementi costitutivi dell'attività (1di2)

Fase	Elementi	Fattori	Rif. GDPR	Criteri WP 248/01	Domande tool CNIL
Descrizione dell'attività	A-settore merceologico (elemento 1)	([20])	35.7. a)	1 - una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):	Panoramica del trattamento
	B-obiettivo dell'attività (elemento 1)	☐ 1-funzionamento della struttura ☐ 2-realizzazione di un prodotto ☐ 3-erogazione di un servizio a terze parti		1.1 - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);	
	C-articolazione dell'attività (elemento 1)	☐ 1-fasi e/o sub-attività ☐ 2-interazioni con altre attività ☐ 3-soggetti esterni coinvolti		1.2 - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali; 1.3 - viene fornita una descrizione funzionale del trattamento;	Dati, processi e risorse di supporto
	D-dimensioni dell'attività (elemento 1)	☐ 1-nr. di utenti coinvolti ☐ 2-quantità di dati utilizzati			
	E-qualità dell'attività (elemento 1)	☐ 3-tipo di dati utilizzati		1.2 - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;	

[20] Settori che rientrano nella Direttiva 1148/2016 NIS recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (DLGS 65 del 18 maggio 2018).

	F-frequenza dell'attività (elemento 1)				Panoramica del trattamento
	G-durata dell'attività (elemento 1)				

Tabella B – comparazione elementi costitutivi dell'attività (2di2)

Fase	Elementi	Fattori	Rif. GDPR	Criteri WP 248/01	Domande tool CNIL
Descrizione dell'attività	Modalità utilizzata (elemento 4)	1-manuale 2-elettronica 3-mista		1.4 - sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);	Dati, processi e risorse di supporto
	A-manuale ☐ senza strumenti elettronici	☐ asset umani (competenza, esperienza, affidabilità del personale) ☐ asset organizzativi (procedure, istruzioni operative, modulistica, linee-guida, ecc.) ☐ asset logistici (uffici, archivi, CED, armadi, ecc.) ☐ servizi di outsourcing documentale			
	B-elettronica ☐ con strumenti elettronici	☐ asset umani (competenza, esperienza, affidabilità del personale) ☐ asset organizzativi (procedure, istruzioni operative, outsourcing a terze parti, ecc.) ☐ asset logistici (uffici, CED) ☐ asset hardware (server, computer, device mobili) ☐ asset software (di base e applicativo) ☐ asset e servizi di networking (router e switch, linee voce-dati, accesso a Internet)			

		☐ servizi di maintenance e assurance degli asset hardware-software ☐ asset e servizi di cloud computing (interscambio file, storage, IaaS, PaaS, SaaS, ecc.)			
	C-mista	☐ con tutti gli strumenti			
	Mezzi impiegati (elemento 5)	A-personale			
		B-logistica			
		C-tecnologie			
		D-organizzazione			

Tabella C – comparazione minacce e misure

Fase	Elementi	Fattori	Rif. GDPR	Criteri WP 248/01	Domande tool CNIL
Individuazione delle minacce ([21])	☐ A-esogene all'attività (elemento 6)	☐ 1-accidentali esterne (naturali) ☐ 2-intenzionali esterne	35.7. a)	3.1.3 - sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati; 3.1.4 - sono stimate la probabilità e la gravità (considerando 90);	
(e vulnerabilità)	☐ B-endogene all'attività (elemento 6)	☐ 1-accidentali interne (ambientali, errori involontari, carenze tecniche e organizzative) ☐ 2-intenziomnali interne			
	☐ A-B-Probabilità di manifestazione (elemento 6)				
	☐ A-B-Gravità della minaccia (elemento 6)				

[21] Nel Modello di notifica al Garante in caso di data breach, sezione C punto 7, sono individuate 4 "Cause della violazione" che raggruppano le vulnerabilità presentate dai mezzi e le minacce ai quali sono esposti.

Individuazione delle misure in atto	☐ A-Embedded (elemento 7)	☐ 1-caratteristiche positive dei mezzi impiegati	35.7 d)	2.1 sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):	Misure esistenti o pianificate
	☐ B-Add in (elemento 7)	☐ 1-azione o strumento applicato ai mezzi impiegati			
	☐ A-B Tipo di misure (elemento 7)	☐ 1-tecniche (strutturali, ambientali, elettroniche) ☐ 2-organizzative (umane)			

Tabella D – comparazione fattori di rischio (1di2)

Fase	Elementi	Fattori	Rif. GDPR	Criteri WP 248/01	Domande tool CNIL
Danni	☐ Tipi	☐ Fisici ☐ Materiali ☐ Immateriali	35.7 c)	3 - i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c):	Rischi
Entità dei danni	☐ Scala di valori semiquantitativa	☐ 1-lieve ☐ 2-medio ☐ 3-grave ☐ 3-gravissimo			
Tipo di causa della violazione ([22])	☐ Corrispondono a tipologie di minacce o incidenti	☐ Azione accidentale esterna ☐ Azione intenzionale esterna ☐ Azione accidentale interna ☐ Azione intenzionale interna		3.1 - l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:	

[22] Nel Modello di notifica al Garante in caso di data breach, sezione C punto 7, sono individuate 4 "Cause della violazione" che raggruppano le vulnerabilità presentate dai mezzi e le minacce ai quali sono esposti.

Natura della violazione ([23])	☐ R-Perdita di riservatezza	☐ 1-diffusione, ☐ 2-accesso non autorizzato o accidentale			
	☐ I-Perdita di integrità	☐ 1-modifica non autorizzata o accidentale			
	☐ D-Perdita di disponibilità	☐ 1-impossibilità di accesso ☐ 2-perdita ☐ 3-distruzione non autorizzata o accidentale			
Gravità della violazione ([24])	-	☐ 1-Trascurabile ☐ 2-Basso ☐ 3-Medio ☐ 4-alto			

Tabella E – comparazione fattori di rischio (2di2

[23] Note al punto 6 sezione C del Modello di notifica al Garante in caso di data breach.

[24] Nel Modello di notifica al Garante in caso di data breach, sezione E punto 3, la stima della gravità della violazione è indicata su una scala a 4 valori.

Individuazione delle minacce ([25])	☐ A-esogene all'attività (elemento 6)	☐ 1-accidentali esterne (naturali) ☐ 2-intenzionali esterne		3.1.1 - si considerano le fonti di rischio (considerando 90);	
(e vulnerabilità)	☐ B-endogene all'attività (elemento 6)	☐ 1-accidentali interne (ambientali, errori involontari, carenze tecniche e organizzative) ☐ 2-intenziomnali interne			
	☐ A-B-Probabilità di manifestazione (elemento 6)	-			
	☐ A-B-Gravità della minaccia (elemento 6)	-			

[25] Nel Modello di notifica al Garante in caso di data breach, sezione C punto 7, sono individuate 4 "Cause della violazione" che raggruppano le vulnerabilità presentate dai mezzi e le minacce ai quali sono esposti.

Tabella F – comparazione impatti e misure

Fase	Elementi	Fattori	Rif. GDPR	Criteri WP 248/01	Domande tool CNIL
Conseguenze della violazione sugli interessati ([26])	☐ Perdita riservatezza	☐ divulgazione non prevista ☐ possibilità di correlazione ☐ utilizzo per altre finalità ☐ altro		3.1.2 - 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;	
	☐ Perdita integrità	☐ dati modificati o inconsistenti ☐ dati modificati e consistenti ☐ altro			
	☐ Perdita disponibilità	☐ mancato accesso ai servizi ☐ malfunzionamento o difficoltà utilizzo ☐ altro			
Determinazione delle misure	B-Add in (elemento 7)	☐ 1-azione o strumento applicato ai mezzi impiegati	35.7 d)	3.2 sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);	Misure esistenti o pianificate
	A-B Tipo di misure (elemento 7)	☐ 1-tecniche (strutturali, ambientali, elettroniche) ☐ 2-organizzative (umane)			Misure esistenti o pianificate

[26] Nel Modello di notifica al Garante in caso di data breach, sezione E punto 1 a, b, c, sono elencate le conseguenze della violazione.

Tabella G – aspetti specifici sulla privacy

Fase	Elementi	Fattori	Rif. GDPR	Criteri WP 248/01	Domande tool CNIL
Determinazione degli aspetti privacy specifici			35.7 a)	1.1 - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);	Panoramica del trattamento
				1.2 - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;	Dati, processi e risorse di supporto
			35.8.	1.5 - si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);	Panoramica del trattamento
			35.7 b)	2 - la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):	Proporzionalità e necessità
				2.1 - sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):	
				2.1.1 - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:	
				2.1.1.1 - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));	
				2.1.1.2 - liceità del trattamento (articolo 6);	
				2.1.1.3 - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));	
				2.1.1.4 - limitazione della conservazione (articolo 5, paragrafo 1, lettera e));	Proporzionalità e necessità

				2.1.2 - misure che contribuiscono ai diritti degli interessati:	Misure di tutela dei diritti degli interessati
				2.1.2.1 - informazioni fornite all'interessato (articoli 12, 13 e 14);	
				2.1.2.2 - diritto di accesso e portabilità dei dati (articoli 15 e 20);	
				2.1.2.3 - diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);	
				2.1.2.4 -diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);	
				2.1.2.5 - rapporti con i responsabili del trattamento (articolo 28);	Panoramica del trattamento
				2.1.2.6 - garanzie riguardanti trattamenti internazionali (capo V);	
			35.9	2.1.2.7 - consultazione preventiva (articolo 36).	
				4 - le parti interessate sono coinvolte:	
				4.1 - si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);	
				4.2 - si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).	

7.1 Contenuti di una valutazione d'impatto

Dalla analisi effettuata nell'Allegato E sulla valutazione d'impatto sulla protezione dei dati come intesa nel GDPR (C89, 90, 91, 92, 94, 95, art. 35.2, art. 35.3), e come dettagliata nelle linee-guida WP248/01 e nel tool del CNIL, per elaborare la valutazione d'impatto è richiesto di:

I. considerare tutti i (solo i) trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35.1, 35.3, C84, C89, C90);

II. valutare il rischio per il trattamento dei dati in base alla sua origine, natura, particolarità e gravità (C76, C83, C84, C90), individuando i possibili danni fisici, materiali o immateriali (C83);

III. redigere un documento contenente almeno (art. 35.7):

   a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;

   b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

   c) una valutazione dei rischi per i diritti e le libertà degli Interessati di cui al paragrafo 1;

   d) le misure previste per affrontare i rischi (C83, C84, C90);

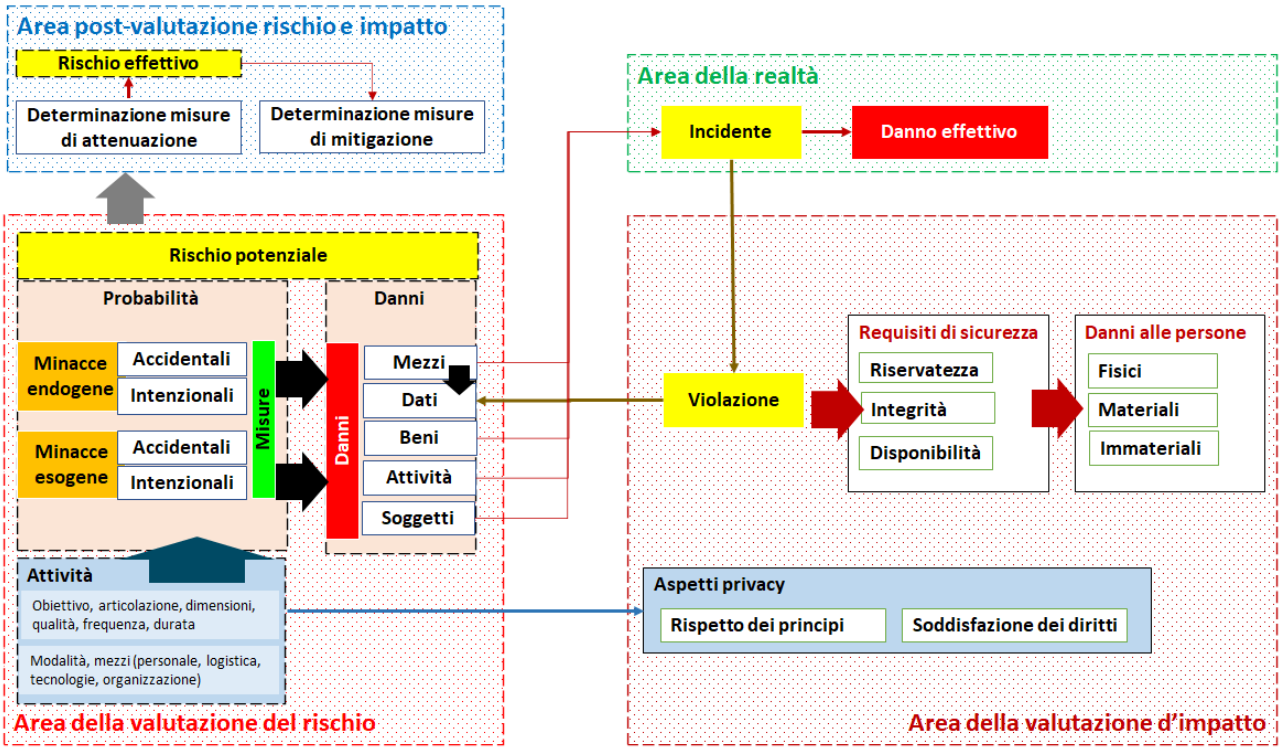
IV. considerare gli aspetti-privacy specifici quali:

   - la necessità e la proporzionalità del trattamento
   - le finalità (determinate, esplicite e legittime) del trattamento
   - la liceità del trattamento
   - i destinatari e il periodo di conservazione dei dati personali
   - le misure che contribuiscono ai diritti degli Interessati
   - le parti interessate coinvolte;

V. determinare le misure aggiuntive a quelle già messe in atto per affrontare i rischi residui.

7.2 Rappresentazione grafica del meccanismo

Utilizzando le informazioni presenti nei Capitoli 4 e 5 è possibile rappresentare graficamente il meccanismo di valutazione del rischio e dell'impatto.



Allegati allo studio sulla valutazione del rischio e d'impatto

8. ALLEGATO A – SUI PROCESSI AZIENDALI

In ambito aziendale, i processi sono intesi come "aggregazioni di attività finalizzate al raggiungimento di uno stesso obiettivo". ([27])

I processi aziendali sono suddivisibili in ***fasi*** nelle quali sono contenute le ***attività*** omogenee all'obiettivo della fase, e si connotano per:

I. l'utilizzo di input, e cioè di risorse di partenza o in entrata,
II. l'interazione con altri processi svolti all'interno o all'esterno della struttura organizzativa owner del processo, e
III. la produzione di output come risultato delle attività di processo.

La maggior parte delle attività si basano sull'utilizzo di dati, che sono importati, generati, scambiati, elaborati, trasmessi, conservati durante il processo aziendale.

I processi aziendali "***primari***" o processi "core" sono quelli il cui output genera valore per gli stakeholders (ad esempio: clienti, utenti, dipendenti, pazienti, azionisti, ecc); i processi "***di supporto***" sono invece quelli che forniscono input e informazioni cosiddette "di servizio" necessarie ai processi primari.

Le risorse impiegate nei processi sono di varie tipologie; l'elenco delle principali:

- Umane (Personale interno ed esterno)
- Organizzative e procedurali (livello di strutturazione, certificazioni, organi e procedure di controllo)
- Tecniche (apparecchiature, impianti, tecnologie)
- Logistiche (uffici, magazzini, fabbriche, depositi)
- Economico-finanziarie (fondi disponibili, linee di credito, quotazione di borsa)
- Know-how (brevetti, partnership, competenze specialistiche del personale)
- Reputazionali (immagine presso gli organi di stampa e nei social network, fidelizzazione dei clienti, capacità di rastrellare credito, partnership)
- Informative (conservazione e utilizzo dei dati prodotti dai processi, raffronto con informazioni esogene).

[27] Fonte: "La gestione dei processi nell'ottica del valore", David Pierantozzi, 1998 EGEA editore. (Pag. 14)

A.1 Re-engineering dei processi

Va sottolineato che, *quando* un processo oggetto della valutazione del rischio *evidenzia una forte criticità* in termini di *inefficienza* (sono usate più risorse di quante ne occorrono, l'andamento non è lineare ma involuto e/o ripetitivo) o di *inefficacia* (l'output del processo non è quello atteso per quantità e/o qualità), l'owner è chiamato ad effettuare interventi di tipo:

A. **incrementale** e cioè volti al continuo e graduale miglioramento dei processi, interventi noti anche col termine di **Business Process Improvement** (BPI),

oppure

B. **radicale** e cioè volti al completo ridisegno del processo, interventi noti col termine di **Business Process Reengineering** (BPR).

9. ALLEGATO B - DEFINIZIONI DEI TERMINI-CHIAVE NEL GDPR

In questa parte del documento sono riportate le definizioni relative ai tre termini-chiave – rischi, trattamenti e danni - presenti nel GDPR.

Considerando 49

(49) ...compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali **conservati o trasmessi**...

Considerando 75

(75) I **rischi** per i diritti e le libertà delle persone fisiche, aventi **probabilità e gravità diverse**, possono **derivare da** trattamenti di dati personali suscettibili di cagionare un **danno fisico, materiale o immateriale**, in particolare:

- **se** il trattamento può comportare **discriminazioni**, **furto o usurpazione d'identità**, **perdite finanziarie**, **pregiudizio alla reputazione**, **perdita di riservatezza dei dati personali protetti da segreto professionale**, **decifratura non autorizzata della pseudonimizzazione**, o qualsiasi altro **danno economico o sociale significativo**;
- **se** gli interessati rischiano di essere **privati dei loro diritti e delle loro libertà** o venga loro **impedito l'esercizio del controllo sui dati personali** che li riguardano;
- **se** sono trattati dati personali che rivelano l'**origine razziale o etnica**, le **opinioni politiche**, le **convinzioni religiose o filosofiche**, l'**appartenenza sindacale**, nonché **dati genetici**, dati **relativi alla salute** o i dati relativi **alla vita sessuale** o a **condanne penali** e a **reati** o alle relative **misure di sicurezza**;
- **in caso di** valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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**, al fine di creare o utilizzare **profili personali**;
- **se** sono trattati dati personali di **persone fisiche vulnerabili**, in particolare **minori**;
- **se** il trattamento riguarda una **notevole quantità di dati personali** e un **vasto numero di interessati**.

Considerando 76

(76) La **probabilità e la gravità del rischio** per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla **natura**, all'**ambito di applicazione**, al **contesto** e alle **finalità** del **trattamento**. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Considerando 77

(77) ...l'individuazione del **rischio** connesso al trattamento, la sua valutazione in termini di **origine, natura, probabilità e gravità**, ...

Considerando 80

(80) ... rischio per i diritti e le libertà delle persone fisiche, tenuto conto della **natura**, del **contesto**, dell'**ambito di applicazione** e delle **finalità del trattamento**...

Considerando 83

(83) ...valutare i **rischi** inerenti al trattamento...Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la **distruzione accidentale o illegale**, la **perdita**, la **modifica**, la **rivelazione** o l'**accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati**, che potrebbero cagionare in particolare un **danno fisico, materiale o immateriale**.

Considerando 84

(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 titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto 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 valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento 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 85

(85) ...**perdita del controllo dei dati personali** che li riguardano o **limitazione dei loro diritti**, **discriminazione**, **furto o usurpazione d'identità**, **perdite finanziarie**, **decifratura non autorizzata della pseudonimizzazione**, **pregiudizio alla reputazione**, **perdita di riservatezza dei dati personali protetti da segreto professionale** o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata...

Considerando 88

(88) ... **furto d'identità o altre forme di abuso**...

Considerando 89

(89) ... tipi di **trattamenti** che potenzialmente **presentano** un **rischio** elevato per i diritti e le libertà delle persone fisiche, per loro **natura**, **ambito di applicazione**, **contesto** e **finalità**...

Considerando 90

(90) ... valutare la particolare **probabilità e gravità del rischio**, tenuto conto della **natura**, dell'**ambito di applicazione**, del **contesto** e delle **finalità** del **trattamento** e delle **fonti di rischio**....

Considerando 91

(91) ... (trattamenti **ad elevato rischio** da assoggettare a valutazione d'impatto ex art. 35)

Considerando 94

(94) ...**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...

Articolo 83

... a) la natura, la gravità e la durata della violazione tenendo in considerazione la **natura**, l'**oggetto** o la **finalità** del **trattamento** in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito...

10. ALLEGATO C - ANALISI SEMANTICA DEI TERMINI-CHIAVE E COMPARAZIONE CON GLI ELEMENTI COSTITUTIVI DI UN'ATTIVITÀ

In questa parte del documento i significati dei tre termini-chiave - trattamenti, rischi e danni - presenti nel GDPR sono analizzati e comparati con i termini utilizzati nel ***Capitolo 4 dello Studio****.*

Nella tabella sono rammentati sinteticamente.

Elemento	Termini utilizzati nello Studio	Termini presenti nel GDPR
1	l'**azione** da svolgere/svolta (che può essere l'attività stessa)	Trattamento
2	i **beni** oggetto dell'azione (tra cui i **dati**)	Dati personali
3	le **persone fisiche** impiegate nell'azione o coinvolte dall'azione	Interessati
4	la **modalità** utilizzata per agire	
5	i **mezzi impiegati** nell'azione	*tipici della modalità utilizzata*
6	le **minacce** alle quali sono esposti i mezzi (comprese le ***vulnerabilità*** che presentano)	
7	le **misure** di contrasto alle minacce	
8	i **soggetti** che a diverso titolo sono attivi (di cui il titolare rappresenta l'organizzazione).	Titolare, Responsabile, Contitolare

C.1 Rischio

C.1.1 Analisi semantica

Il termine "**rischio**" nel GDPR è sempre **([28])** associato a "**i diritti e le libertà delle persone fisiche**".

Tale rischio:

1. **esiste** *ma in potenza* per la stessa natura del trattamento (Considerando 75, 89, 91, 94), oppure è *accertato* a seguito della valutazione d'impatto (art. 35);
2. **è individuabile e valutabile** conoscendone questi elementi di qualificazione:
    a. origine (C77)

[28] Nel Considerando 83 si parla di "rischio per la sicurezza dei dati" ma comunque tenendo "in considerazione i rischi presentati dal trattamento dei dati personali… che potrebbero cagionare in particolare un danno fisico, materiale o immateriale."

b. natura (C77) o particolarità (C84)

c. probabilità (C75, 76, 77, 90)

d. gravità (C75, 76, 77, 90).

I diritti e le libertà delle persone fisiche sono soggetti a questi **tipi di rischio**:

- (C75) privazione dei diritti e delle libertà
- (C85) limitazione dei diritti
- (C75) impedimento dell'esercizio del controllo sui dati personali (come negli Artt. 15-21)
- (C85) perdita del controllo dei dati personali.

Le persone fisiche, che sono state private o limitate nei loro diritti e libertà, sono esposte a questi tipi di **danni**:

- (C85) fisici (*es. cure errate o tardate*)
- (C75, C85) materiali (finanziari, economici)
- (C75, C85) immateriali (discriminazione, pregiudizio alla reputazione).

C.1.2 Aspetti che qualificano il rischio per i diritti e le libertà

Nella tabella che segue sono riportati:

- Il riferimento al testo del GDPR (C = considerando)
- i termini (origine, natura o particolarità, probabilità e gravità) utilizzati nei Considerando 75, 76, 77 per qualificare il rischio (aspetti) per i diritti e le libertà delle persone fisiche
- la declinazione di tali aspetti nel GDPR
- la corrispondenza con gli elementi costitutivi un'attività (vedi Capitolo 4 dello studio) e con i fattori presenti nella nuova formula di calcolo del rischio (vedi Capitolo 4 dello studio).

Rif. GDPR	Aspetti del rischio	Rif. GDPR	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
C77	**Origine**	**Il rischio *origina* dal trattamento** (Considerando 75,76, 77, 80, 83, 89, 90, 91, 94, art. 83) - (C75) derivare da trattamenti di dati personali suscettibili di	**Il rischio è funzione di:** - caratteristiche dell'attività **(elemento 1)** - modalità utilizzata **(elemento 4)**

		cagionare un danno fisico, materiale o immateriale - (C76) con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento - (C77) connesso al trattamento - (C80) tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento - (C83) inerenti al trattamento - (C89) per loro natura, ambito di applicazione, contesto e finalità - (C90) tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento - (C91) trattamenti ad elevato rischio - (C94) certi tipi di trattamento - (art. 83) in considerazione la natura, l'oggetto o la finalità del trattamento	- mezzi impiegati **(elemento 3)** - minacce **(elemento 6)** - misure **(elemento 5).**

Rif. GDPR	Aspetti del rischio	Rif. GDPR	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
C77 (C84)	Natura (particolarità)	La natura del *rischio* deriva dalla violazione dei requisiti di sicurezza: - (C49) ...compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi...	*La natura del rischio deriva da:* - i beni oggetto dell'attività che sono rappresentati da "dati personali" (**elemento 2 e 1-E3**) - dalla modalità utilizzata (**elemento 4**) - i mezzi impiegati per gestire i dati (**elemento 5**)

			- dai requisiti di sicurezza (riservatezza, integrità, disponibilità) violati relativi ai mezzi e quindi ai dati.

Rif. GDPR	Aspetti del rischio	Rif. GDPR	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo

C75, 76, 77, 90	Probabilità	La *probabilità* del rischio è **determinata da:** la natura, l'ambito di applicazione, il contesto e le finalità del trattamento (C76, 80).	*La probabilità del rischio è determinata da:*
			- le **minacce esogene** alle quali sono esposti i mezzi impiegati (**elemento 6-A**)
			- le **minacce endogene** (elemento 4-B) originate
			  o dalle caratteristiche dell'attività (**elemento 6-B**)
			  o dalla modalità utilizzata (**elemento 4**)
			  o dai mezzi impiegati (**elemento 5**)
			- il tipo di minacce che ne determinala probabilità (**elemento 6 A-B**)
			- le misure in grado di ridurre o annullare le vulnerabilità e contrastare le minacce (**elemento 7**).

Rif. GDPR	Aspetti del rischio	Rif. GDPR	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo

C75, 76, 77, 90	**Gravità**	**La *gravità* del rischio è determinata da:** la natura, l'ambito di applicazione, il contesto e le finalità del trattamento (C76, 80). **Altri *fattori* che determinano la gravità del rischio** (C75): - trattamento di dati di categorie particolari (artt.9 ,10) - valutazione aspetti personali - previsioni di aspetti personali - creazione profili personali - persone fisiche vulnerabili - minori - quantità dati personali - vastità numero interessati	**La gravità del rischio è determinata da**: - il tipo di minacce che ne determinala probabilità e la gravità (**elemento 6**) - la quantità e qualità dei dati e delle persone fisiche (**elemento 1 D, 1 E**).

C.1.3 Considerazioni

1. La comparazione evidenzia che

- gli aspetti del rischio presenti nel GDPR sono coerenti e corrispondono agli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
- quindi i fattori presenti nella nuova formula di calcolo del rischio R = *f*(P * D) sono validi anche per valutare i rischi per i diritti e le libertà delle persone fisiche.

C.2 Trattamento

C.2.1 Analisi semantica

L'articolo 4.2 del GDPR definisce 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".

Se lo svolgimento di un'attività prevede l'utilizzo [29] di dati personali, si può affermare che attività e trattamento abbiano lo stesso significato: la conferma è il titolo dell'articolo 30 del GDPR "Registri delle *attività di trattamento*" svolte sotto la responsabilità del titolare o per suo conto.

Da sottolineare che, come un'attività è la fonte del suo rischio, così il trattamento determina il proprio rischio, anche in termini di probabilità e gravità.

C.2.2 Aspetti che qualificano il trattamento

Nel GDPR non ci sono le descrizioni degli aspetti che qualificano i trattamenti [30] utilizzati nei Considerando 76, 80, 89, 90, 93, art. 83, ma, essendo i termini attività e trattamento semanticamente assimilabili, nella tabella che segue sono riportati:

- Il riferimento al testo del GDPR (C = considerando)
- i nomi degli aspetti che qualificano i trattamenti
- i termini (natura, ambito di applicazione, contesto, oggetto o finalità, fonti di rischio, tipo, estensione, frequenza) utilizzati nei Considerando 76, 80, 89, 90, 93, art. 83 per qualificare il trattamento (aspetti)
- la corrispondenza con gli elementi costitutivi un'attività (vedi Capitolo 4 dello studio) e con i fattori presenti nella nuova formula di calcolo del rischio (vedi Capitolo 5 dello studio).

Rif. GDPR	Aspetti del trattamento	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
C76, 80, 89, 90 Art.83	Natura	La natura del trattamento è identificabile nel: - obiettivo dell'attività **(elemento 1-B)** - articolazione dell'attività **(elemento 1-C)** - modalità utilizzata **(elemento 2)**

[29] L'utilizzazione dei dati trova nelle operazioni di trattamento (art.4.2) la migliore declinazione: 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.

[30] Natura, Ambito di applicazione, Contesto, Oggetto o finalità, Fonti di rischio, Tipo, Estensione, Frequenza

		- mezzi impiegati **(elemento 2).**
C76, 80, 89, 90	**Ambito di applicazione**	**L'ambito di applicazione del trattamento è individuabile nel**: - D-dimensioni dell'attività **(elemento 1-D)** - E-qualità dell'attività **(elemento 1-E)** - F-frequenza dell'attività **(elemento 1-F)** - G-durata dell'attività **(elemento 1-G).**
C76, 90, 89, 90	**Contesto**	**Il contesto del trattamento è assimilabile a**: - settore merceologico **(elemento 1-A)** - obiettivo dell'attività **(elemento 1-B)** - articolazione dell'attività **(elemento 1-C)** - modalità utilizzata **(elemento 4)** - mezzi impiegati **(elemento 5).**
C76, 80, 89, 90 Art. 83	**Oggetto o finalità**	**L'oggetto o finalità del trattamento è comparabile a**: - obiettivo dell'attività **(elemento 1-B)** - articolazione dell'attività **(elemento 1-C)**.
Rif. GDPR	**Aspetti del trattamento**	**Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo**
C90	**Fonti di rischio**	**Le fonti di rischio del trattamento sono vulnerabilità intrinseche all'attività, alla modalità, ai mezzi, alle misure in atto. Vedi**: - caratteristiche dell'attività **(elemento 1)** - modalità utilizzata **(elemento 4)** - mezzi impiegati **(elemento 5)** - minacce **(elemento 6)** - misure **(elemento 7).**
C93	**Tipo**	**Il tipo di trattamento è determinata da:** - settore merceologico **(elemento 1-A)** - obiettivo dell'attività **(elemento 1-B)** - articolazione dell'attività **(elemento 1-C)**.
C93	**Estensione**	**L'estensione del trattamento è determinata da:**

		- articolazione dell'attività **(elemento 1-C)** - dimensioni dell'attività **(elemento 1-D)** - durata **(elemento 1-G).** *Se riferita ai dati trattati, l'estensione del trattamento può riguardare un campione, una minima parte, una gran parte, a totalità dei dati.* **L'estensione del trattamento funge da** fattore di aumento della probabilità e della gravità del rischio e del danno.
C93	**Frequenza**	**La frequenza del trattamento può essere**: occasionale, poco frequente, molto frequente, regolare, quotidiana. **(elemento 1-F)** **La frequenza del trattamento funge da** fattore di aumento della probabilità e della gravità del rischio e del danno.

C.2.3 Considerazioni

1. La comparazione evidenzia che

- gli aspetti del rischio presenti nel GDPR sono coerenti e corrispondono agli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo.

C.3 Danno

C.3.1 Analisi semantica del termine "danno"

Nella valutazione del rischio il danno è una stima degli effetti di un possibile incidente (ovvero un rischio concretizzato). **([31])**

Quando l'incidente coinvolge mezzi che gestiscono dati personali si parla di *violazione* dei requisiti di sicurezza (riservatezza, integrità, disponibilità): la violazione dei dati *può* produrre danni ai diritti ed alle libertà delle persone fisiche alle quali appartengono i dati gestiti.

Nel GDPR il termine "danni" è utilizzato associato a:

- (C49) danni ai sistemi informatici e di comunicazione elettronica
- (C85) danni fisici, materiali o immateriali alle persone fisiche
- (146) danni cagionati a una persona da un trattamento non conforme.

Mentre il termine "danno" è utilizzato associato a:

- (75) danno fisico, materiale o immateriale derivato da trattamenti di dati personali
- (83) danno fisico, materiale o immateriale cagionato dal trattamento di dati personali
- (94) danno o un'interferenza con i diritti e le libertà della persona fisica scaturito da certi tipi di trattamento e dall'estensione e frequenza del trattamento.

Il GDPR mette a disposizione una serie di termini per definire e descrivere i danni: nella tabella che segue sono forniti:

- Colonna 1 - il riferimento al testo del GDPR
- Colonna 2 - il termine utilizzato
- Colonna 3 - il significato del termine che "**può**" intendersi come
    - danno,
    - **(*)** incidente o violazione,
    - **(**)** fattore di crescita del danno quale caratteristica dell'attività (trattamento).
- Colonna 4 - l'oggetto dell'incidente (dati o persone)
- Colonna 5 - il requisito di sicurezza violato (RID) da cui origina il danno
- Colonna 6 - il tipo di danno alle persone (F = fisico, M = materiale, I = immateriale), come da Considerando 75 e 83.

[31] Ovviamente il danno è anche il risultato della rilevazione delle perdite economiche e di altra natura effettuata a valle di un incidente avvenuto.

1	2	3	4	5	6
Rif. GDPR	**Termine utilizzato**	**Significato**	**Oggetto dell'incidente**	**Requisito violato**	**Tipo di danno**
C75, 85 C75, 85, 88 C75, 85 C75, 85 C75, 85 C75, 85 C75, 85	- discriminazioni - furto o usurpazione d'identità - perdite finanziarie - pregiudizio alla reputazione - perdita di riservatezza dei dati personali protetti da segreto professionale - decifratura non autorizzata della pseudonimizzazione - danno economico o sociale significativo	- Danno o interferenza ai diritti - Danno o interferenza ai diritti - Danno o interferenza ai diritti - Danno o interferenza ai diritti - Incidente o violazione **(*)** - Incidente o violazione **(*)** - Danno o interferenza ai diritti	- Persone - Dati - Persone - Persone - Dati - Dati - Persone	- R, I - R - R - R (diff.one) - R - R - R, I, D	- M, I - M, I - M - I - M, I - M, I - M, I
C75	- privazione diritti e libertà	- Danno o interferenza ai diritti	- Persone	- R, I, D	- M, I
C85	- limitazione dei diritti	- Danno o interferenza ai diritti	- Persone	- n.a.	- n.a.
C75	- impedimento dell'esercizio del controllo sui dati personali (Artt. 15-21)	- Danno o interferenza ai diritti	- Persone	- n.a.	- n.a.

C94	- danno o un'interferenza con i diritti e le libertà	- Danno o interferenza ai diritti	- Persone	- R, I, D	- M, I
C83	- distruzione accidentale o illegale, la perdita	- Incidente o violazione **(*)**	- Dati	- D	- M, I
C83	- modifica	- Incidente o violazione **(*)**	- Dati	- I	- F, M, I
C83	- rivelazione o accesso non autorizzati	- Incidente o violazione **(*)**	- Dati	- R (diff.one)	- M, I
C85	- perdita del controllo dei dati personali	- Incidente o violazione **(*)**	- Dati	- R, I, D	- M, I
C75	- trattamento di dati di categorie particolari (artt. 9 e 10)	- **(**)** (caratteristica 1.B dell'attività)	- Dati	- n.a.	- n.a.
C75	- valutazione aspetti personali	- **(**)** (caratteristica dell'attività)	- Dati	- n.a.	- n.a.
C75	- previsioni di aspetti personali	- **(**)** (caratteristica dell'attività)	- Dati	- n.a.	- n.a.
C75	- creazione profili personali	- **(**)** (caratteristica dell'attività)	- Dati	- n.a.	- n.a.
C75	- persone fisiche vulnerabili	- **(**)** (caratteristica dell'attività)	- Dati	- n.a.	- n.a.
	- minori	- **(**)** (caratteristica dell'attività)	- Dati	- n.a.	- n.a.
C75	- quantità dati personali	- **(**)** (caratteristica dell'attività)	- Dati	- n.a.	- n.a.
	- vastità numero interessati	- **(**)** (caratteristica dell'attività)	- Persone	- n.a.	- n.a.

C.3.2 Caratteristiche dei danni ai dati

I danni subiti dai dati a seguito di una violazione si caratterizzano per:

- **estensione**
    - minima (piccola parte)
    - parziale (buona parte)
    - consistente (larga parte di dati)
    - totale (tutti i dati);
- **persistenza**
    - minima (possibilità di recupero alta, tempi minimi, costi bassi)
    - media (recupero fattibile, tempi e costi medi)
    - duratura (recupero possibile, tempi e costi alti)
    - definitiva (recupero impossibile);
- **tempi di manifestazione**
    - a breve termine
    - a medio termine
    - a lungo termine;
- **gravità**
    - minimo o trascurabile
    - non trascurabile con impatto possibile sull'attività
    - serio con impatto possibile sull'attività
    - molto serio con sciuro impatto negativo sull'attività
    - di elevato valore, rilevante per l'intera organizzazione.

11. ALLEGATO D - IL METODO ENISA

D.1 Obiettivo

Il Manuale sulla Sicurezza nel trattamento dei dati personali di ENISA ha l'obiettivo di valutare il rischio concreto (per i diritti e le libertà degli interessati) nell'ottica di adottare le misure tecniche e organizzative adeguate al rischio presentato.

D.2 Struttura del metodo

Il metodo di valutazione del rischio ENISA prevede 5 fasi o step:

FASE / STEP	ATTIVITA' DI ANALISI
1	Definizione dell'operazione di trattamento e del suo contesto.
2	Comprensione e valutazione dell'impatto.
3	Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia).
4	Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto).

In base ai risultati della valutazione è richiesto di verificare le misure tecniche e organizzative di sicurezza adottate per proteggere I dati trattati nel processo.

5	Verifica delle misure tecniche e organizzative adottate e implementate

Le misure sono elencate in tre liste diverse da utilizzare a seconda che il rischio emerso dalla valutazione abbia un valore basso, medio o alto, con la seguenti scalabilità:

	Misure A.1	Misure A.2	Misure A.3
Valore del rischio BASSO	obbligatorie		
Valore del rischio MEDIO	*applicabili*	obbligatorie	
Valore del rischio ALTO/ MOLTO ALTO	*applicabili*	*applicabili*	obbligatorie

D.3 Step 1: definizione dell'operazione di trattamento e del suo contesto

La "definizione dei confini del sistema di trattamento dei dati oggetto di valutazione e assessment, e del relativo contesto" è effettuata considerando 7 elementi; nella Tabella che segue sono comparati agli elementi che qualificano un'attività (trattamento):

Elementi del Manuale	Elementi del trattamento (attività)
1. Cos'è l'operazione di trattamento dei dati personali?	***La descrizione dell'operazione di trattamento è presente negli elementi:*** - *(1) settore merceologico della struttura organizzativa dove si svolge il processo/attività* - *(1) obiettivo del processo/attività (funzionamento della struttura, realizzazione di un prodotto, erogazione di un servizio a terze parti)* - *(1) articolazione del processo/attività (fasi e attività/sub-attività)*
2. Quali sono le tipologie di dati personali trattati?	***Le tipologie di dati sono presenti negli elementi:*** - *(1) dimensioni dell'attività (nr. di utenti coinvolti, quantità di dati utilizzati)* - *(1) qualità dell'attività (tipo di utenti, tipo di dati, livello di criticità aziendale del processo)*
3. Qual è la finalità del trattamento?	***La finalità del trattamento è comparabile a:*** - *(1) l'obiettivo dell'attività (funzionamento della struttura, erogazione di un servizio a terze parti)* - *(1) l'articolazione dell'attività.*
4. Quali sono gli strumenti utilizzati per il trattamento dei dati personali?	***Gli strumenti utilizzati sono presenti negli elementi:*** - *(2) la modalità utilizzata (manuale, elettronica, mista) ed i relativi mezzi impiegati: a. personale, b. logistica, c. tecnologie, d. organizzazione.*
5. Dove avviene il trattamento dei dati personali?	***Paese*** *di stabilimento del Titolare e degli eventuali Responsabili.*
6. Quali sono le categorie di soggetti interessate?	***Le categorie di soggetti sono presenti negli elementi:*** - *(1) dimensioni dell'attività (nr. di utenti coinvolti, quantità di dati utilizzati)*

	- *(1) qualità dell'attività (tipo di utenti, tipo di dati, livello di criticità aziendale del processo)*
7. Chi sono i destinatari dei dati?	***Individuazione** dei Destinatari e del loro Paese di stabilimento e della liceità del trasferimento dei dati.*

D.3.1 Considerazioni

Gli elementi che qualificano la valutazione del rischio di un'attività (trattamento) e la valutazione del rischio per i diritti e le libertà sono utilizzabili per declinare i 7 elementi indicati nello step 1 del Manuale ENISA.

D.4 Step 2: comprensione e valutazione dell'impatto

Sulla base dell'analisi dello Step 1, si valuta separatamente l'impatto sui diritti e sulle libertà delle persone fisiche derivanti dalla possibile perdita di riservatezza, integrità e disponibilità dei dati, assegnando ad ogni requisito il livello reputato adatto a descrivere la situazione, su una scala a 4 valori (basso, medio, alto, molto alto): *il più alto* dei 3 livelli è considerato come *il risultato finale* della valutazione dell'impatto, relativo al trattamento *complessivo* dei dati personali.

La valutazione dell'impatto è un processo qualitativo.

		LIVELLO DI IMPATTO (o DANNO)			
AZIONE	REQUISITO DI SICUREZZA	Basso	Medio	Alto	Molto alto
Valutare il livello di impatto (**rating**) che la divulgazione non autorizzata (**perdita di riservatezza**) dei dati personali trattati potrebbe avere sull'individuo.	**Riservatezza**				
Valutare il livello di impatto (**rating**) che l'alterazione non autorizzata (**perdita di integrità**) dei dati personali trattati potrebbe avere sull'individuo.	**Integrità**				
Valutare il livello di impatto (**rating**) che la distruzione (**perdita di disponibilità**) dei dati personali trattati potrebbe avere sull'individuo.	**Disponibilità**				

Nella Tabella che segue sono descritti i 4 livelli di impatto ed I relativi effetti.

Livello di impatto	Descrizione del livello di impatto	Descrizione degli effetti
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	Conseguenze minori, superabili senza particolari problemi (fastidio, perdita di tempo per reintroduzione dei dati, ...).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali,	Inconvenienti significativi, superabili con qualche difficoltà (costi extra, impedimento a ricevere servizi, preoccupazione, stress).

	paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).	
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	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.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).	Inconvenienti significativi con conseguenze anche irreversibili (impossibilità di lavorare, conseguenze psicologiche permanenti, morte, etc.).

D.5 Step 3: definizione di possibili minacce e valutazione della loro probabilità

Il manuale fornisce 20 domande afferenti a 4 diverse aree.

All'auditor è richiesto di:

I. assegnare un valore su una scala da 0 a 1 ad ogni domanda la probabilità di occorrenza delle minacce

II. effettuare la somma dei valori per ogni area, che varierà tra minimo 0 (tutte le cinque domande hanno peso zero) e massimo 5 (tutte le cinque domande hanno peso uno)

III. sommare I valori di tutte le 4 aree per individuare il livello di probabilità nei tre range

- da 0 a 1 = basso livello di probabilità
- da 2 a 3 = medio livello di probabilità
- da 4 a 5 = alto livello di probabilità

IV. trasformare il livello di probabilità (qualitativo) in un punteggio numerico

- basso livello di probabilità = 1
- medio livello di probabilità = 2
- alto livello di probabilità = 3

V. sommare i punteggi ottenuti per ogni area

VI. la somma varierà nel range tra 4 (punteggio minimo 1 per tutte e quattro le aree) e 12 (punteggio massimo di 3 per tutte e quattro le aree)

VII. il valore della somma globale della probabilità di occorrenza di una minaccia intercetta il livello di probabilità finale

- da 4 a 5 = basso livello finale di probabilità
- da 6 a 8 = medio livello finale di probabilità
- da 9 a 12 = alto livello finale di probabilità.

Si rammenta che, una volta effettuata l'individuazione, la valutazione della probabilità di accadimento delle minacce è un processo semi-quantitativo.

Seguono le tabelle fornite nel Manuale con l'unica variazione di comparare il contenuto delle domande con gli elementi costitutivi di un'attività (trattamento).

AREA DI VALUTAZIONE	Somma delle risposte	PROBABILITA'	
		LIVELLO	PUNTEGGIO
A. RISORSE DI RETE E TECNICHE	0 o 1	Basso	1
	2 o 3	Medio	2
	4 o 5	Alto	3
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	0 o 1	Basso	1
	2 o 3	Medio	2
	4 o 5	Alto	3
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	0 o 1	Basso	1
	2 o 3	Medio	2
	4 o 5	Alto	3
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	0 o 1	Basso	1
	2 o 3	Medio	2
	4 o 5	Alto	3

Probabilità di occorrenza della minaccia	
LIVELLO DI PROBABILITA' DELLE MINACCE	Somma globale della probabilità di occorrenza di una minaccia
Basso	4
	5
Medio	6
	7
	8
Alto	9
	10
	11
	12

AREA		DOMANDA	DESCRIZIONE	Elementi del trattamento (attività)
A. RISORSE DI RETE E TECNICHE	1	Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.	- *(1) l'articolazione dell'attività* - *(2) il tipo di mezzi impiegati che comprendono le misure di sicurezza*
	2	È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.	
	3	Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).	
	4	Le persone non autorizzate possono accedere facilmente	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la	

		all'ambiente di trattamento dei dati?	sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).	
	5	Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.	La risposta presuppone l'analisi privacy by design

AREA		DOMANDA	DESCRIZIONE	Elementi del trattamento (attività)
B-PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	1	I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.	Le risposte richiedono di conoscere i risultati delle azioni compiute sul personale, le procedure adottate, la profilazione applicativa.
	2	L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	
	3	I dipendenti sono autorizzati a portare e utilizzare i propri	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso	

		dispositivi per connettersi al sistema di trattamento dei dati personali?	non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.	La risposta richiede di conoscere le procedure adottate.
	4	I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.	La risposta richiede di conoscere le procedure adottate.
	5	Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali.	La risposta richiede di conoscere il funzionamento degli applicativi software.

AREA		DOMANDA	DESCRIZIONE	Elementi del trattamento (attività)
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	1	Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	La risposta richiede di conoscere i risultati delle azioni compiute sul personale, le procedure adottate, la profilazione applicativa.
	2	Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente	La risposta richiede di conoscere i risultati della tenuta del registro delle attività di trattamento.

		/ terza parte (responsabile del trattamento)?	quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	
	3	Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.	La risposta richiede di conoscere i contenuti dei contratti tra le parti.
	4	Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	La risposta richiede di conoscere i risultati delle azioni compiute sul personale.
	5	Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.	

AREA		DOMANDA	DESCRIZIONE	Elementi del trattamento (attività)
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	1	Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.	Le risposte richiedono l'esistenza dei registri degli incidenti e delle violazioni.
	2	La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	
	3	Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.	
	4	Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	- *(1) le dimensioni dell'attività (nr. di utenti coinvolti, quantità di dati utilizzati)*
	5	Esistono best practices di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.	La risposta richiede di conoscere gli eventuali standard di riferimento del settore merceologico in cui si opera.

D.5.1 Considerazioni

Dalla comparazione del contenuto delle domande con gli elementi costitutivi di un'attività (trattamento) emerge che la probabilità delle minacce è funzione del *dettaglio* dei mezzi impiegati:

- modalità manuale
  a. asset hardware (locali, magazzini, armadi, ecc.)
  b. asset organizzativi (procedure, istruzioni operative, modulistica, linee-guida, ecc.).
- modalità elettronica.
  c. asset hardware (server, computer, device mobili)
  d. asset software (di base e applicativo)
  e. servizi di maintenance e assurance degli asset hardware-software
  f. asset e i servizi di networking (router e switch, linee voce-dati, accesso a Internet)
  g. asset ed i servizi di cloud computing (storage, IaaS, PaaS, ecc.)
  h. asset organizzativi (procedure, istruzioni operative, ecc.).

D.6 Step 4: valutazione del rischio

All'auditor è richiesto di individuare sulla mappa di valutazione del rischio:

I. il livello (basso, medio alto, molto alto) di impatto risultato degli step 1 e 2,
II. la probabilità (bassa, media alta) di occorrenza della minaccia risultato dello step 3.

Il valore del rischio risulterà dall'incrocio dei valori I e II su una scala tra 1 e 12.

Valutazione del rischio (step 4)		**Livello di impatto** (step 1-2)			
		Basso	Medio	Alto	Molto alto
Probabilità di occorrenza della minaccia (step 3)	Bassa	1	2	3	4
	Media	2	4	6	8
	Alta	3	6	9	12

D.6.1 Considerazioni.

Alla luce di quanto precede è possibile affermare che:

1) il rischio valutato con il metodo ENISA risulta essere il risultato di un processo semi-quantitativo;

2) *per la definizione dell'operazione di trattamento e del suo contesto (**step 1**) è possibile utilizzare gli elementi costitutivi di un'attività;*

3) la comprensione e la valutazione dell'impatto (**step 2**) si sostanzia nello stabilire il possibile livello di danno ai (perdita dei) requisiti di sicurezza (riservatezza, integrità, disponibilità) in base alle minacce intrinseche agli elementi (vulnerabilità) che caratterizzano il trattamento; [**fattore D della formula**]

4) la definizione delle possibili minacce e la valutazione della loro probabilità di accadimento (**step 3**) sono determinate dalla modalità di svolgimento (manuale, elettronica, mista), dai mezzi, dalla articolazione del trattamento che i mezzi devono abilitare e supportare; [**fattore P della formula**] (**[32]**)

5) la valutazione del rischio (**step 4**) è la combinazione del livello di impatto (scala a quattro livelli) con la probabilità di accadimento (scala a tre livelli) su una matrice a 12 valori; [**fattore R della formula**];

6) la verifica delle misure tecniche e organizzative adottate e implementate [**step 5**] è effettuata in base al livello di rischio individuato. (**[33]**)

D.7 La formula di calcolo del rischio di sicurezza ENISA

Ricapitolando quanto previsto nel Manuale ENISA, l'auditor per valutare il rischio di sicurezza:

1. analizza alcune caratteristiche dell'attività
    a. definizione dell'operazione di trattamento
    b. tipologie di dati personali trattati
    c. finalità del trattamento
    d. strumenti utilizzati per il trattamento
    e. luogo del trattamento
    f. categorie di soggetti interessate
    g. destinatari dei dati
2. decide discrezionalmente quale impatto (danno) possono avere su ogni singolo requisito di sicurezza
3. analizza altre caratteristiche dell'attività

[32] Il limite del metodo ENISA è che gli elementi delle aree rappresentano un ambito ristretto anche se significativo della realtà. Inoltre non sono prese in considerazione misure idonee alla modalità manuale.

[33] Le misure di sicurezza NON fanno parte dei mezzi impiegati ma la loro adozione è esaminata in relazione ad elenchi ripresi dallo standard ISO/IEC 27001.

h. a. risorse di rete e tecniche

i. b. processi / procedure relativi all'operazione di trattamento dei dati

j. c. parti / persone coinvolte nel trattamento dei dati personali

k. d. settore di operatività' e scala di trattamento

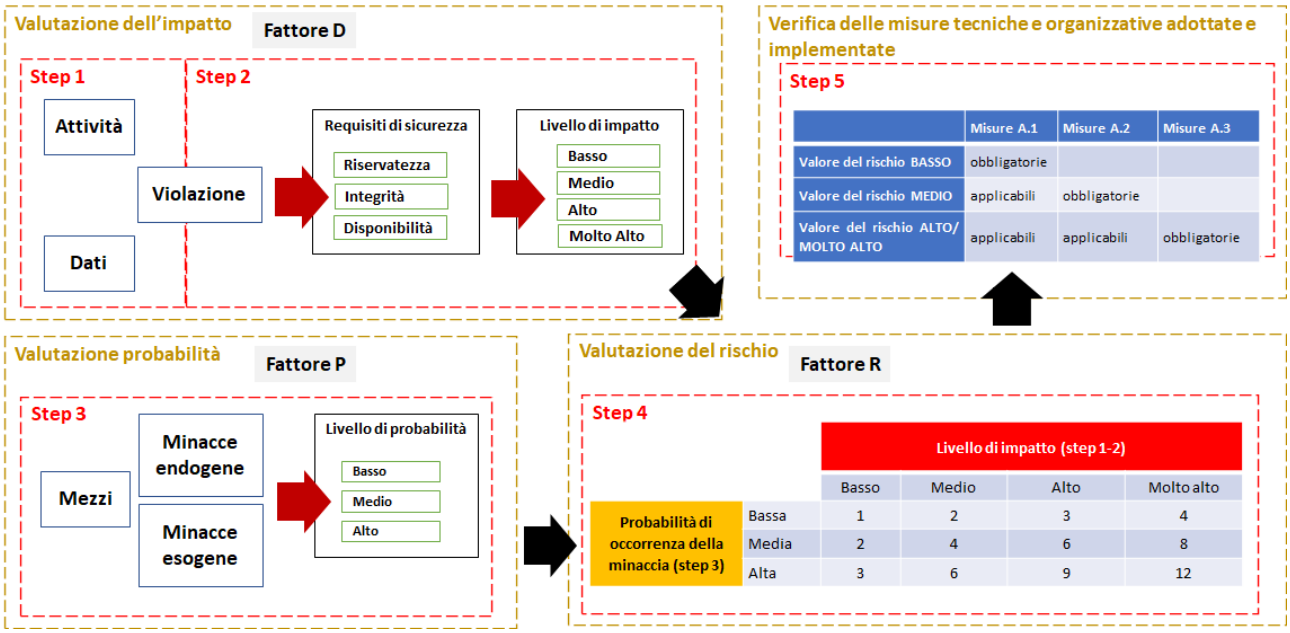
4. decide la probabilità di accadimento delle minacce
5. incrocia i valori 2 e 4 su una mappa di valori.

La formula di calcolo che se ne può ricavare diventa:

R = P (*f*mezzi-minacce) * D (*f*attività) dove D è quello più alto tra I valori D-ris, D-int, D-disp

D.8 La rappresentazione grafica del meccanismo ENISA

Gli elementi e le fasi del meccanismo sono rappresentati nel seguente diagramma di flusso.



12. ALLEGATO E - LA VALUTAZIONE D'IMPATTO

In questa parte del documento sono riportate la definizione ed i contenuti della valutazione d'impatto nel GDPR, nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 dal Gruppo di lavoro articolo 29 per la protezione dei dati (17/IT WP 248 rev.01), nel tool del CNIL [34].

Le modalità ed i contenuti di una valutazione d'impatto indicati nel GDPR, dal WP29 e dal CNIL sono comparate con gli elementi costitutivi di un'attività e con i fattori presenti nella nuova formula di calcolo.

Considerando 76

(76) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una *valutazione oggettiva* mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un *rischio elevato*.

Considerando 83

(83) Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i *rischi* presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un *danno fisico, materiale o immateriale*.

Considerando 84

(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 titolare del trattamento dovrebbe essere responsabile dello svolgimento di una *valutazione d'impatto 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 valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento 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 89

[34] L'autorità garante francese o Commission nationale de l'informatique et des libertés.

(89) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una *valutazione d'impatto sulla protezione dei dati*, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Considerando 90

(90) In tali casi, è opportuno che il titolare del trattamento effettui una *valutazione d'impatto sulla protezione dei dati* prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.

Considerando 91

(91) ...effettuare una valutazione d'impatto sulla protezione dei dati...

Considerando 92

(92) ...effettuare una valutazione d'impatto sulla protezione dei dati...

Considerando 94

(94) ...effettuare una valutazione d'impatto sulla protezione dei dati...

Considerando 95

(95) ...effettuare una valutazione d'impatto sulla protezione dei dati...

Articolo 35 "Valutazione d'impatto sulla protezione dei dati"

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, 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 titolare del trattamento *effettua*, prima di procedere al trattamento, *una valutazione dell'impatto dei trattamenti* previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

3. La *valutazione d'impatto sulla protezione dei dati* di cui al paragrafo 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 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'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

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

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

E.1 Comparazione con i contenuti dell'Art. 35.7

	Contenuti DPIA ex Art. 35.7	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
a)	una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;	- **Caratteristiche dell'attività (elemento 1)**
b)	una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;	n.a.
c)	una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e	**I rischi per i diritti sono determinati dai rischi che corrono i dati personali gestiti dai mezzi impiegati per gestirli.** **Vedi la valutazione del rischio effettuata sugli elementi che costituiscono l'attività di trattamento:** - caratteristiche dell'attività **(elemento 1)** - modalità utilizzata **(elemento 4)** - mezzi impiegati **(elemento 5)** - minacce **(elemento 6)** - misure **(elemento 7).**
d)	le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.	- ***è un'attività eseguibile solo dopo la valutazione del rischio/impatto (vedi successivo punto 3.2)*** - ***è possibile includere anche le misure in atto*** **(elemento 7)**

E.2 Comparazione con i criteri dell'Allegato 2 WP248 rev.01

Nell'allegato sono indicati i criteri da seguire per elaborare una valutazione d'impatto sulla protezione dei dati: nella tabella che segue sono comparati agli elementi costitutivi di un'attività ed ai fattori presenti nella nuova formula di calcolo del rischio.

	Criterio DPIA ex WP248/01	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
1	una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):	- **Caratteristiche dell'attività (elemento 1)**
1.1	la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);	- **Caratteristiche dell'attività (elemento 1)**
1.2	vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;	n.a.
1.3	viene fornita una descrizione funzionale del trattamento;	- **Caratteristiche dell'attività (elemento 1)**
1.4	sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);	- **Modalità (elemento 4)** - **Mezzi (elemento 5)**
1.5	si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);	n.a.

	Criterio DPIA ex WP248/01	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
2	la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):	
2.1	sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):	- *è un'attività eseguibile solo dopo la valutazione del rischio/impatto (vedi successivo punto 3.2)* - *è possibile includere anche le misure in atto* (elemento 7)
2.1.1	misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:	n.a.
	finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));	n.a.
	liceità del trattamento (articolo 6);	n.a.
	dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));	n.a.
	limitazione della conservazione (articolo 5, paragrafo 1, lettera e));	n.a.
2.1.2	misure che contribuiscono ai diritti degli interessati:	n.a.
	informazioni fornite all'interessato (articoli 12, 13 e 14);	n.a.
	diritto di accesso e portabilità dei dati (articoli 15 e 20);	n.a.
	diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);	n.a.
	diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);	n.a.
	rapporti con i responsabili del trattamento (articolo 28);	n.a.
	garanzie riguardanti trattamenti internazionali (capo V);	n.a.
	consultazione preventiva (articolo 36).	n.a.

	Criterio DPIA ex WP248/01	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
3	i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c):	n.a.
3.1	l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:	- *vedi i seguenti punti 3.1.1 e 3.1.2*
3.1.1	si considerano le fonti di rischio (considerando 90);	**Le fonti di rischio del trattamento sono vulnerabilità intrinseche all'attività, alla modalità, ai mezzi, alle misure in atto.** **Vedi**: - caratteristiche dell'attività **(elemento 1)** - modalità utilizzata **(elemento 4)** - mezzi impiegati **(elemento 5)** - minacce **(elemento 6)** - misure **(elemento 7).**
3.1.2	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;	- ***è un'attività a carattere consulenziale eseguibile dopo avere individuato i requisiti di sicurezza violati.*** - ***vedi anche i risultati dell'analisi semantica del termine "danno" (Allegato D).***
3.1.3	sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;	**Le minacce che possono determinare la violazione dei requisiti di sicurezza sono sia le vulnerabilità intrinseche all'attività, alla modalità, ai mezzi, alle misure in atto, che le minacce presenti nel contesto. Vedi**: - caratteristiche dell'attività **(elemento 1)** - modalità utilizzata **(elemento 4)** - mezzi impiegati **(elemento 5)** - minacce **(elemento 6)** - misure **(elemento 7).**

	Criterio DPIA ex WP248/01	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
3.1.4	sono stimate la probabilità e la gravità (considerando 90);	**La probabilità delle minacce è determinata da**: - il tipo di **minacce esogene** alle quali sono esposti i mezzi impiegati **(elemento 4-A)** - il tipo di **minacce endogene** (**elemento 4-B**) originate o dalle caratteristiche dell'attività (**elemento 1**) o dalla modalità utilizzata (**elemento 4**) o dai mezzi impiegati (**elemento 5**) - le misure in grado di ridurre o annullare le vulnerabilità e contrastare le minacce **(elemento 7)**.
		La gravità delle minacce è determinata da: - il tipo di minacce (**(elemento 4-A-B)** - la quantità e qualità dei dati e delle persone fisiche (**elementi 1-D1 1-E1, E3**).
3.2	sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);	- ***è un'attività eseguibile solo dopo la valutazione del rischio/impatto*** - ***è possibile includere anche le misure in atto*** **(elemento 7)**
4	le parti interessate sono coinvolte:	n.a.
4.1	si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);	n.a.
4.2	si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).	n.a.

E.3 Comparazione con le domande del tool del CNIL

Nel tool sono indicate le informazioni da reperire e utilizzare per elaborare una valutazione d'impatto sulla protezione dei dati: nella tabella che segue sono comparati agli elementi costitutivi di un'attività ed ai fattori presenti nella nuova formula di calcolo del rischio.

Domande presenti nel tool del CNIL	Corrispondenza con gli elementi costitutivi un'attività e con i fattori della nuova formula di calcolo
Panoramica del trattamento	
Qual è il trattamento in considerazione?	- **Obiettivo dell'attività (elemento 1-B)**
Quali sono le responsabilità connesse al trattamento? (individuazione responsabili esterni)	- **Articolazione dell'attività (elementi 1-C)**
Ci sono standard applicabili al trattamento?	n.a.
Dati, processi e risorse di supporto	
Quali sono i dati trattati?	- **Articolazione dell'attività (elementi 1-E3)**
Quale è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	- **Articolazione dell'attività (elemento 1-C)**
Quali sono le risorse di supporto ai dati?	- **Modalità (Elemento 4)** - **Mezzi (Elemento 5)**
Principi fondamentali	n.a.
Proporzionalità e necessità	n.a.
Gli scopi del trattamento sono specifici, espliciti e legittimi?	n.a.
Quali sono le basi giuridiche che rendono lecito il trattamento?	n.a.
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	n.a.
I dati sono esatti e aggiornati?	n.a.
Quale è il periodo di conservazione dei dati?	n.a.

Misure di tutela dei diritti degli interessati	
Come sono informati del trattamento gli interessati?	n.a.
Ove applicabile: come si ottiene il consenso degli interessati?	n.a.
Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	n.a.
Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	n.a.
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	n.a.
In caso di trasferimento dei dati al di fuori dell'Unione Europea, i dati godono di una protezione equivalente?	n.a.
Rischi	**I rischi che corre il trattamento sono le vulnerabilità intrinseche all'attività, alla modalità, ai mezzi, alle misure in atto e alle minacce presenti nel contesto. Vedi:** - caratteristiche dell'attività **(elemento 1)** - modalità utilizzata **(elemento 4)** - mezzi impiegati **(elemento 5)** - minacce **(elemento 6)** - misure **(elemento 7).**
Misure esistenti o pianificate	- **Misure in atto (elemento 7)**

E.4 Comparazione dei contenuti dell'art. 35.7 del GDPR, dei criteri del WP248/01, delle domande del tool del CNIL

Rif.	Contenuti DPIA ex Art. 35.7.	Rif.	Criterio DPIA ex WP248/01.	Domande ex tool CNIL.
a)	*una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*	*1*	*una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):*	***Panoramica del trattamento*** *- Qual è il trattamento in considerazione?*
		1.1	*la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);*	
		1.2	*vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;*	***Dati, processi e risorse di supporto*** *- Quali sono i dati trattati?*
		1.3	*viene fornita una descrizione funzionale del trattamento;*	***Dati, processi e risorse di supporto*** *- Quale è il ciclo di vita del trattamento dei dati (descrizione funzionale)?*
		1.4	*sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);*	***Dati, processi e risorse di supporto*** *- Quali sono le risorse di supporto ai dati?*
		1.5	*si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);*	***Panoramica del trattamento*** *- Ci sono standard applicabili al trattamento?*

Rif.	Contenuti DPIA ex Art. 35.7.	Rif.	Criterio DPIA ex WP248/01.	Domande ex tool CNIL.
b)	*una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*	*2*	*la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):*	
		2.1	*sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):*	
		2.1.1	*misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:*	
		2.1.1.1	*finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));*	***Proporzionalità e necessità** - Gli scopi del trattamento sono specifici, espliciti e legittimi?*
		2.1.1.2	*liceità del trattamento (articolo 6);*	***Proporzionalità e necessità** - Quali sono le basi giuridiche che rendono lecito il trattamento?* ***Misure di tutela dei diritti degli interessati** - Ove applicabile: come si ottiene il consenso degli interessati?*
		2.1.1.3	*dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));*	***Proporzionalità e necessità** - I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?*

				Proporzionalità e necessità *- I dati sono esatti e aggiornati?*
		2.1.1.4	*limitazione della conservazione (articolo 5, paragrafo 1, lettera e));*	***Proporzionalità e necessità*** *- Quale è il periodo di conservazione dei dati?*

Rif.	Contenuti DPIA ex Art. 35.7.	Rif.	Criterio DPIA ex WP248/01.	Domande ex tool CNIL.
		2.1.2	*misure che contribuiscono ai diritti degli interessati:*	
		2.1.2.1	*informazioni fornite all'interessato (articoli 12, 13 e 14);*	***Misure di tutela dei diritti degli interessati*** *- Come sono informati del trattamento gli interessati?*
		2.1.2.2	*diritto di accesso e portabilità dei dati (articoli 15 e 20);*	
		2.1.2.3	*diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);*	***Misure di tutela dei diritti degli interessati*** *- Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?*
		2.1.2.4	*diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);*	***Misure di tutela dei diritti degli interessati*** *-Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?*
		2.1.2.5	*rapporti con i responsabili del trattamento (articolo 28);*	***Panoramica del trattamento*** *- Quali sono le responsabilità connesse al trattamento? (individuazione responsabili esterni)*

				Misure di tutela dei diritti degli interessati *- Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?*
		2.1.2.6	*garanzie riguardanti trattamenti internazionali (capo V);*	***Misure di tutela dei diritti degli interessati*** *- In caso di trasferimento dei dati al di fuori dell'Unione Europea, i dati godono di una protezione equivalente?*
		2.1.2.7	*consultazione preventiva (articolo 36).*	

Rif.	Contenuti DPIA ex Art. 35.7.	Rif.	Criterio DPIA ex WP248/01.	Domande ex tool CNIL.
c)	*una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e*	*3*	*i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c):*	***Rischi***
		3.1	*l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:*	
		3.1.1	*si considerano le fonti di rischio (considerando 90);*	
		3.1.2	*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;*	

		3.1.3	*sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;*	
		3.1.4	*sono stimate la probabilità e la gravità (considerando 90);*	
		3.2	*sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);*	***Misure esistenti o pianificate***
		4	*le parti interessate sono coinvolte:*	
		4.1	*si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);*	
		4.2	*si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).*	

Rif.	Contenuti DPIA ex Art. 35.7.	Rif.	Criterio DPIA ex WP248/01.	Domande ex tool CNIL.
d)	*le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*			***Misure esistenti o pianificate***

E.5 Standard di riferimento

L'auditor che intende elaborare la valutazione del rischio e d'impatto, oltre a quanto offerto dal GDPR e il WP29, può avvalersi di due specifici standard:

- ISO/IEC 31000:2018 Risk Management
- ISO/IEC 29134:2017 Guidelines for privacy impact assessment.

13. ALLEGATO F – SCALE DI VALORI

F.1 - Scala dell'entità (gravità) del Danno

criterio	livello	valore
- Episodio con effetti rapidamente reversibili per i diritti e le liberà degli interessati - Dati che potranno essere rapidamente ripristinati	Lieve	1
- Episodio con effetti reversibili per i diritti e le liberà degli interessati - Dati che potranno essere certamente ripristinati entro 7 giorni	Medio	2
- Episodio con effetti difficilmente reversibili per i diritti e le liberà degli interessati - Dati che potranno difficilmente e/o solo in parte essere ripristinati entro 7 giorni	Grave	3
- Episodio con effetti irreparabili per i diritti e le liberà degli interessati - Dati che non potranno essere ripristinati	Gravissimo	4

F.2 - Scala delle Probabilità

criterio	livello	valore
- La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti - L'evento non si è mai verificato negli ultimi 5 anni - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe incredulità in azienda	Improbabile	1
- La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi - L'evento si è verificato negli ultimi 5 anni e/o ci si aspetta una frequenza fra 1 e 3 anni - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una grande sorpresa in azienda	Poco probabile	2

- La mancanza rilevata può provocare un danno, anche se non in modo automatico o diretto - L'evento si è verificato negli ultimi 3 anni e/o ci si aspetta una frequenza fra 1 mese ed 1 anno - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una moderata sorpresa in azienda	Probabile	3
- Esiste una correlazione diretta tra la mancanza rilevata e il verificarsi del danno ipotizzato - L'evento si è verificato nell'ultimo mese e/o ci si aspetta una frequenza inferiore a 1 mese - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe alcuno stupore in azienda	Molto probabile	4

F.3 - Scala della gravità delle minacce by CNIL

criterio	livello	valore
le fonti di rischio non sembrano avere capacità speciali per eseguire una minaccia (ad esempio, la funzione software si insinua da un individuo che agisce senza intenti dannosi e che ha privilegi di accesso limitati).	TRASCURABILE	1
le capacità delle fonti di rischio di mettere in atto una minaccia sono limitate (ad esempio: la funzione del software si insinua da un individuo malintenzionato con privilegi di accesso limitati).	LIMITATO	2
le capacità delle fonti di rischio di mettere in atto una minaccia sono reali e significative (ad esempio, la funzione software si insinua da un individuo che agisce senza intenti dannosi e che ha privilegi di amministrazione illimitati).	SIGNIFICATIVO	3
le capacità delle fonti di rischio di mettere in atto una minaccia sono definite e illimitate (ad esempio, la funzione del software si insinua da un utente malintenzionato con privilegi di amministrazione illimitati).	MASSIMO	4

F.4 - Scala della gravità delle vulnerabilità by CNIL

criterio	livello	valore
non sembra possibile mettere in atto una minaccia sfruttando le proprietà dei beni di supporto (ad esempio furto di documenti cartacei conservati in una stanza protetta da un lettore di badge e codice di accesso).	TRASCURABILE	1
mettere in atto una minaccia sfruttando le proprietà delle risorse di supporto sembra essere difficile (ad esempio il furto di documenti cartacei conservati in una stanza protetta da un lettore di badge).	LIMITATO	2
sembra possibile mettere in atto una minaccia sfruttando le proprietà dei beni di supporto (ad esempio il furto di documenti cartacei conservati in uffici a cui non è possibile accedere senza aver prima effettuato il check-in alla reception).	SIGNIFICATIVO	3
eseguire una minaccia sfruttando le proprietà delle risorse di supporto sembra essere estremamente facile (ad esempio il furto di documenti cartacei conservati in una lobby).	MASSIMO	4

LUIGI ZAMPETTI

Nel settore ICT dal 1979, oggi è consulente per i sistemi di gestione.

In ambito privacy, si è occupato in Telecom Italia di servizi di supporto alla compliance, con l'entrata in vigore del D.lgs. 196/2003.

Dal 2016 ha sviluppato una originale metodologia (ASG679©) di raccolta e sistematizzazione delle informazioni aziendali, e progettato e sviluppato checklist on line per l'audit del sistema di gestione privacy, la valutazione dei profili di rischio legati ai processi aziendali e all'IT.

È stato specialista di Sanità Digitale nella funzione Marketing della Direzione Business di Telecom Italia, dal 2003 al 2016, partecipando all'elaborazione di studi specifici e business model dei seguenti servizi e-Health: Domicilio Sanitario, Identità Digitale, FSE, Mobile Health, Patient Empowerment, Telemedicina, Interoperabilità, Cloud Computing, in collaborazione con Federsanità-ANCI, Assinform, AISIS, SIT, CNR-LAVSE-ITB-ICAR, Netics e le Università di Genova, Milano-Politecnico, Napoli-Federico II, Milano-Bocconi (CERMES e CERGAS), Roma-Tor Vergata (CEIS), Politecnica delle Marche.

È stato Project Manager di progetti di telemedicina in Italia, Brasile, Cuba. PM del progetto di Telecom Italia «sito Web Giubileo 2000» per il Vaticano.

Ha conseguito le seguenti certificazioni e abilitazioni: Digital Product Management (DigComp 2016); Lead Auditor BS 7799 per i sistemi di gestione della sicurezza delle informazioni (DNV Knowledge Institute 2004); abilitazione in Economia delle Imprese Cooperative e delle Organizzazioni non-profit (EINCOP 1994).