“Linee Guida analisi rischio trattamenti di dati”

Preliminare conferma e richiamo dei punti fondamentali della “Linee Guida Valutazione d’Impatto Protezione Dati – DPIA” che costituiscono atto preliminare e propedeutico alla predisposizione e approvazione delle “Linee Guida analisi rischio trattamenti di dati”.

1) descrizione dei trattamenti previsti e delle finalità del trattamento:

- la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione;
- vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
- viene fornita una descrizione funzionale del trattamento;
- sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);

2) valutazione della necessità e proporzionalità dei trattamenti. Sono state determinate le misure previste per garantire il rispetto del regolamento:

2.1) misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:

- finalità determinate, esplicite e legittime;
- liceità del trattamento;
- dati personali adeguati, pertinenti e limitati a quanto necessario;
- limitazione della conservazione;

2.2) misure che contribuiscono ai diritti degli interessati:

- informazioni fornite all'interessato;
- diritto di accesso e portabilità dei dati;
- diritto di rettifica e alla cancellazione;
- diritto di opposizione e di limitazione di trattamento;
- rapporti con i responsabili del trattamento;
- garanzie riguardanti trattamenti internazionali;
- consultazione preventiva.

3) misure previste per dimostrare osservanza;

4) valutazione dei rischi per i diritti e le libertà degli interessati:

4.1) l'origine, la natura, la particolarità e la gravità dei rischi o, più in particolare, per ciascun rischio vengono determinate dalla prospettiva degli interessati:

- si considerano le fonti di rischio;
- sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
- sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
- sono stimate la probabilità e la gravità;

4.2) sono determinate le misure previste per gestire tali rischi.

5) misure previste per affrontare i rischi e dimostrare la conformità al presente regolamento:

- a tal fine devono identificarsi
- gli impatti potenziali sui diritti e le libertà degli interessati
- le minacce che potrebbero comportare accessi illegittimi
- le modifiche indesiderate
- l'indisponibilità dei dati

6) documentazione delle decisioni assunte

7) monitoraggio e revisione

Riguardo le “Linee Guida analisi rischio trattamenti di dati” occorre precisare che in base all’art. 32 del GDPR il Titolare del trattamento dei dati personali, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di

varia probabilità e gravità per i diritti e le libertà delle persone fisiche, è chiamato a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Il processo di Analisi & Valutazione del Rischio per la sicurezza dei dati personali e delle informazioni comporta la necessità di avere chiari i concetti di **DATO** e **INFORMAZIONE** che hanno una **SOSTANZIALE COINCIDENZA** secondo le seguenti definizioni

dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
dato	rappresentazione interpretabile delle informazioni in modo formalizzato idoneo per la comunicazione, l'interpretazione o l'elaborazione
informazione	conoscenza di dati che in un determinato contesto ha un significato particolare

La metodologia strutturata di Valutazione del Rischio Privacy tiene conto degli standard internazionale riferiti:

- alla famiglia di norme ISO/IEC 27000 si occupa dei sistemi di gestione per la sicurezza delle informazioni, e quindi anche degli aspetti connessi al risk assessment in ambito information security;
- alla famiglia di norme ISO/IEC 29100 ha ristretto l’ambito di applicazione alla privacy (in un quadro generale più ampio della data protection regolamentata nel GDPR), e alle Personally Identifiable Information (PII) ossia le informazioni riferite a persone.

Più precisamente, gli standard internazionali di riferimento per la Valutazione del Rischio Privacy riguardano le norme:

- *UNI/ISO **31000:2018** – Risk management – Guidelines*
- *UNI CEI EN ISO/IEC **27001:2013** – Information technology – Security techniques – Information security management systems – Requirements*
- ISO/IEC **27701:2019** – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

La sicurezza dei dati personali e delle informazioni sono rivolte alla preservazione della loro RISERVATEZZA, INTEGRITÀ e DISPONIBILITÀ, nonché della AUTENTICITÀ, ACCOUNTABILITY, NON-REPUDIATION e RESILIENZA.

Al riguardo è opportuno precisare cosa si intende per:

1. RISERVATEZZA è il grado in cui l’ACCESSO alle informazioni è limitato a un gruppo preventivamente DEFINITO ed AUTORIZZATO ad avere questo accesso. Questo include anche misure per proteggere la privacy. Le informazioni che si vogliono proteggere non devono essere inaccessibili, ma devono essere accessibili solo dal personale autorizzato.
2. INTEGRITÀ è il grado con cui le informazioni sono aggiornate e sono prive di errori (sia intenzionali che accidentali). L’Integrità è caratterizzata da due aspetti che sono: CORRETTEZZA delle informazioni; COMPLETEZZA delle informazioni. L’integrità delle informazioni equivale a dire che queste siano AGGIORNATE.
3. DISPONIBILITÀ è il grado in cui le INFORMAZIONI sono disponibili all’utente e/o al sistema informativo NEL MOMENTO IN CUI QUESTE VENGONO RICHIESTE in quanto sono NECESSARIE e A CHI LE DEVE RICEVERE. La Disponibilità è caratterizzata da TRE ASPETTI e sono:
    a. TEMPORALE – i sistemi informativi sono disponibili quando necessario;
    b. CONTINUITÀ – il personale può continuare a lavorare in caso di guasto;
    c. ROBUSTEZZA – vi è una capacità sufficiente per consentire a tutto il personale nel sistema di lavorare.

Parole chiave della valutazione del rischio sono:

EVENTO	verificarsi o non verificarsi di un particolare insieme di circostanze
CONSEGUENZA (= IMPATTO)	esito di un evento che influenza gli obiettivi
MINACCIA	modalità operativa comprendente una o più azioni individuali sulle risorse che supportano i dati e può quindi causare un evento pericoloso
VULNERABILITA’	punto debole del sistema / trattamento in corrispondenza del quale le misure di sicurezza sono assenti, ridotte o compromesse
GRAVITA’	rappresenta l'entità del rischio; dipende principalmente dalla natura pregiudizievole del potenziale impatto
PROBABILITA’	plausibilità di un accadimento ipotizzabile – likelyhood / verosimiglianza
CONTROLLO	misura (intervento) che mantiene o modifica il rischio

Un rischio è una combinazione delle conseguenze che potrebbero derivare dal verificarsi di un evento indesiderato e dalla probabilità del verificarsi dell'evento. La valutazione del rischio quantifica o descrive qualitativamente il rischio e consente ai titolari di stabilire le priorità dei rischi in base alla gravità percepita o ad altri criteri stabiliti.
La valutazione del rischio determina il valore delle risorse informative, identifica le minacce e le vulnerabilità applicabili che esistono o possono esistere, identifica i controlli esistenti e i loro effetti sul rischio identificato, determina le potenziali conseguenze e, infine, dà la priorità ai rischi derivati e li classifica rispetto i criteri di valutazione del rischio stabiliti nella costituzione del contesto.

Valutazione del livello di rischio per ogni attività / operazione di trattamento dei dati personali, seguendo il compito n. 3 del Manuale del DPO e il tool dell’ENISA https://www.enisa.europa.eu/risk-level-tool/ che rinviano entrambi alle misure e ai controlli della norma ISO 27001:2013, si articola nelle seguenti fasi:

1. **Definizione e contesto**
2. **Valutazione dell'impatto**
   2a. Confidentiality RISERVATEZZA
   2b. Integrity INTEGRITA’
   2c. Availability DISPONIBILITA’
   2d. Valutazione dell'impatto globale
3. **Analisi delle minacce**
   3.A. Risorse di rete e tecnologiche (hardware e software)
   3.B. Processi/procedure connessi al trattamento
   3.C. Soggetti e persone coinvolti nel trattamento
   3.D. Settore di attività e scala del trattamento
4. **Valutazione del rischio**
5. **misure di sicurezza – ENISA ISO 27001:2013**
   ORGANIZATIONAL SECURITY MEASURES
   - Security management
   - Incident response and business continuity
   - Human resources

   TECHNICAL SECURITY MEASURES
   - Access control and authentication
   - Logging and monitoring
   - Security of data at rest
   - Network/Communication security
   - Back-ups
   - Mobile/Portable devices
   - Application lifecycle security
   - Data deletion/disposal
   - Physical security

6. Documento sintesi analisi e misure proposte

Ai fini della complementarietà tra valutazione del rischio dei trattamenti dei dati personali e procedura di Valutazione di impatto del trattamento dei dati DPIA, fermo restando quanto descritto nel documento proposto con nota **prot. n. 0135203-2019**, ritengo opportuno riportare:

- estratto dalla norma ISO 29134/2017 in merito ai controlli che si pongono in continuità con i controlli della norma ISO 27001:2013;
- tabelle riassuntive degli elementi da tenere in considerazione in merito alla valutazione delle vulnerabilità e delle minacce, nonché della relativa gravità (impatto).

Di seguito la descrizione della procedura di Valutazione del livello di rischio per ogni attività / operazione di trattamento dei dati personali secondo il tool dell’ENISA https://www.enisa.europa.eu/risk-level-tool/

1. Definizione e contesto

a. Processing Operation Description ATTIVITA’ & OPERAZIONI TRATTAMENTO
b. Personal Data Processed TIPOLOGIE DATI PERSONALI
c. Processing Purpose FINALITA’
d. Data Subject(s) INTERESSATI
e. Processing Means MODALITA’ DI CONSERVAZIONE
f. Recipients of Personal Data DESTINATARI External: Internal:
g. Data Processor Used LUOGO DEL TRATTAMENTO DEI DATI - SERVER

2. Valutazione dell'impatto

La valutazione dell'impatto è un processo qualitativo e una serie di fattori devono essere considerati dal responsabile del trattamento dei dati, come I TIPI DI DATI PERSONALI, LA CRITICITÀ DEL TRATTAMENTO, IL VOLUME DEI DATI PERSONALI, LE CARATTERISTICHE SPECIALI DEL RESPONSABILE DEL TRATTAMENTO, NONCHÉ COME CATEGORIE SPECIALI DI INTERESSATI.

LIVELLO DI IMPATTO	DESCRIZIONE
BASSO	Gli individui possono riscontrare alcuni PICCOLI INCONVENIENTI, CHE SUPERERANNO SENZA ALCUN PROBLEMA (tempo impiegato per immettere nuovamente informazioni, fastidi, irritazioni, ecc.)
MEDIO	Gli individui possono incontrare INCONVENIENTI SIGNIFICATIVI, CHE SARANNO IN GRADO DI SUPERARE NONOSTANTE ALCUNE DIFFICOLTÀ (costi aggiuntivi, negazione dell'accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.)
ALTO	Gli individui possono riscontrare CONSEGUENZE SIGNIFICATIVE, CHE DOVREBBERO ESSERE IN GRADO DI SUPERARE ANCHE SE CON GRAVI DIFFICOLTÀ (appropriazione indebita di fondi, lista nera da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, mandato di comparizione, peggioramento della salute, ecc.)
MOLTO ALTO	Individui che possono incontrare CONSEGUENZE SIGNIFICATIVE, O ADDIRITTURA IRREVERSIBILI, CHE NON POSSONO SUPERARE (incapacità al lavoro, disturbi psicologici o fisici a lungo termine, morte, ecc.)

2a. Confidentiality RISERVATEZZA

RIFLETTERE SULL'IMPATTO CHE UNA DIVULGAZIONE NON AUTORIZZATA (PERDITA DI RISERVATEZZA) DEI DATI PERSONALI - NEL CONTESTO IN CUI SI SVOLGE LA PROPRIA ATTIVITÀ COMMERCIALE - POTREBBE AVERE SULL'INDIVIDUO ED ESPRIMERE UNA VALUTAZIONE DI CONSEGUENZA
Esempi / scenari di perdita di riservatezza:

- Un file cartaceo o un laptop contenente dati personali viene perso durante il trasporto.
- L'apparecchiatura è stata smaltita senza distruzione dei dati personali.
- I dati personali vengono inviati per errore a una serie di destinatari non autorizzati.
- Alcuni clienti potrebbero accedere agli account di altri clienti in un servizio online.
- I dati personali sono pubblicati su una bacheca Internet o un sito p2p.
- Un CD-ROM con i dati dei clienti è stato rubato dai locali.
- Un sito Web configurato in modo errato rende pubblicamente accessibili su Internet i dati degli utenti interni.

2b. Integrity INTEGRITA’

RIFLETTERE SULL'IMPATTO CHE UN'ALTERAZIONE NON AUTORIZZATA (PERDITA DI INTEGRITÀ) DEI DATI PERSONALI - NEL CONTESTO IN CUI SI SVOLGE LA PROPRIA ATTIVITÀ COMMERCIALE - POTREBBE AVERE SULL'INDIVIDUO ED ESPRIMERE UNA VALUTAZIONE DI CONSEGUENZA.
Esempi / scenari di perdita di integrità:

- È stato modificato un record necessario per la fornitura di un servizio sociale in linea e l'individuo deve richiedere il servizio in modalità offline.
- È stato modificato un record che è importante per l'accuratezza della cartella di una persona in un servizio medico online.

2c. Availability DISPONIBILITA’

RIFLETTERE SULL'IMPATTO CHE UNA DISTRUZIONE O PERDITA NON AUTORIZZATA (PERDITA DI DISPONIBILITÀ) DI DATI PERSONALI - NEL CONTESTO IN CUI SI SVOLGE LA PROPRIA ATTIVITÀ COMMERCIALE - POTREBBE AVERE SULL'INDIVIDUO ED ESPRIMERE UNA VALUTAZIONE DI CONSEGUENZA.
Esempi / scenari di perdita di disponibilità:

- Un database dei clienti è danneggiato ed è necessaria un'elaborazione Alta per riportare il servizio in linea.
- Una cartella personale viene persa e l'individuo deve fornire nuovamente alcune informazioni all'azienda.
- Un file viene perso / database danneggiato e non è disponibile il backup di queste informazioni.
- Un servizio critico (ad es. Cartella clinica online) non è attivo e non può essere recuperato immediatamente.

2d. Valutazione dell'impatto globale

La valutazione dell'impatto complessivo (attribuito nelle precedenti valutazioni) per

	RISERVATEZZA	INTEGRITA’	DISPONIBILITA’
BASSO			
MEDIO			
ALTO			
MOLTO ALTO			

3. Analisi delle minacce

LE QUATTRO AREE PRINCIPALI DI VALUTAZIONE IN TERMINI DI SICUREZZA DEI DATI:
Per ciascuna area di valutazione, vengono poste cinque domande; una risposta affermativa indica la presenza di un rischio, come indicato nella tabella riassuntiva al termine delle domande.

3.A. Risorse di rete e tecnologiche (hardware e software)

Risorse tecniche e di rete: la probabilità di accadimento della minaccia è BASSA / MEDIA / ALTA, visto che il Sistema è connesso / non è connesso a Internet e permette / non permette accesso da Internet alle risorse interne di altri Sistemi IT. Viene assunto per questo scenario pratico che l’accesso non autorizzato sia gestito come rischio seguendo delle adeguate linee guida di sicurezza interne e buone prassi.

1. Vi sono parti del trattamento svolte attraverso 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.

Esempi:

• Un e-marketplace che offre la possibilità di acquistare beni online
• Un portale di e-news che fornisce informazioni personalizzate per gli utenti registrati
• Un sistema CRM offerto tramite una soluzione cloud as a service.

□ SI □ NO

2. E’ possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per esempio, riguardo a certi 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.

Esempi:

• Una compagnia di assicurazioni consente l'accesso remoto (tramite Internet) ai gestori ai file dei clienti.
• Una società di consulenza consente al personale di accedere al sistema interno per la gestione dei permessi e delle missioni tramite Internet.
• Un'azienda fornisce l'accesso remoto al sistema a fornitori esterni per la manutenzione e il supporto IT.

□ SI □ NO

3. Il Sistema di trattamento dati personali è interconnesso a un altro Sistema o Servizio IT interno o esterno al Vostro ente?

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).

Esempi:

• Un e-bookshop è collegato a un sistema di pagamento online (per supportare gli acquisti elettronici).
• Un piccolo sistema informatico di finanziamento della clinica è collegato al sistema informatico del regime assicurativo nazionale (per convalidare lo stato assicurativo dei pazienti).
• Un sistema CRM interconnesso con il sistema informatico di elaborazione ordini e sistemi a supporto dei pagamenti e dell'emissione delle fatture.

□ SI □ NO

4. E’ facile per soggetti non autorizzati accedere all’ambiente di trattamento dati?

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 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).

Esempi:

• Una PMI non dispone di una sala computer dedicata per l'amministrazione del sistema informatico utilizzato per il trattamento dei dati personali.
• Una PMI ha esternalizzato l'archiviazione dei propri dati a un'azienda che offre l'archiviazione remota dei dati. Non è chiaro quali misure di sicurezza siano state applicate dall'azienda per salvaguardare i locali del data center. Un sistema CRM offerto tramite una soluzione cloud as a service.

□ SI □ NO

5. Il Sistema di trattamento dati personali è progettato, implementato o manutenuto senza seguire le migliori pratiche del settore?

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.
Esempi:
• I diversi componenti di rete e di sistema si basano su tecnologie e protocolli IT standard (contrariamente alle soluzioni ad-hoc).
• Hardware e software sono ottenuti da fornitori affidabili e seguendo procedure contrattuali formali.
• È in atto un piano di manutenzione adeguato, inclusa la manutenzione regolare della rete e dei dispositivi e delle applicazioni di sistema.

□ SI □ NO

3.B. Processi/procedure connessi al trattamento

Processi/Procedure relativi alla operazione di trattamento dei dati personali: la probabilità di accadimento della minaccia è BASSA / MEDIA / ALTA, assumendo che ruoli e responsabilità del responsabile della funzione XXX siano chiaramente definiti ed allineati alle policies interne del Titolare del trattamento e che il trattamento dei dati personali sia ristretto alla sede dell’organizzazione / o sia riferito a e che vengano prodotti files di log per ciascuna attività di trattamento

6. Ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?

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.
Esempi:
• Gli assistenti del dipartimento finanziario non possono solo inserire informazioni, ma anche modificarle ed eliminarle, come i manager.
• Gli infermieri di una clinica medica possono modificare la cartella clinica del paziente, sebbene solo i medici dovrebbero essere in grado di farlo.

□ SI □ NO

7. L’utilizzo accettabile delle risorse di rete, di Sistema e fisiche all’interno dell’ente è definito in modo incerto o insufficiente?

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.
Esempi:
• Non è chiaro se i dipendenti possono utilizzare il proprio indirizzo e-mail professionale per comunicazioni personali.
• Non esiste alcuna politica che imponga il livello di utilizzo della larghezza di banda consentito ai dipendenti su base giornaliera.

□ SI □ NO

8. Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?

I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.

Esempi:
• I dipendenti possono connettersi alla rete aziendale con i loro tablet o altri dispositivi intelligenti.
• I dipendenti possono elaborare i dati utilizzando applicazioni specifiche installate nelle loro tabelle personali / dispositivi intelligenti.
□ SI □ NO

9. Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro dell’ente?

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.
Esempi:
• Un'agenzia di viaggi consente ai dipendenti di utilizzare i propri laptop professionali al di fuori dei locali dell'organizzazione per elaborare i dati dei clienti.
• Una società di consegna consente ai dipendenti di utilizzare tablet dedicati durante la consegna per convalidare i dettagli del destinatario.
□ SI □ NO

10. Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?

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.
Esempi:
• Non esiste un elenco di persone che accedono quotidianamente alla sala computer di un'azienda.
• L'accesso alle cartelle cliniche dei pazienti in una clinica non è registrato.
• Non esiste una politica che imponga come monitorare i registri e quali azioni devono essere intraprese in caso di ripetuti abusi del sistema.
□ SI □ NO

3.C. Soggetti e persone coinvolti nel trattamento

Gruppi/Persone coinvolte nel trattamento di dati personali: la probabilità di accadimento della minaccia è BASSA / MEDIA / ALTA visto che gli addetti XXX hanno / non hanno ricevuto una appropriata formazione sulla sicurezza dei dati e vi è certezza / non vi è certezza che i dati personali vengano sempre trattati e/o distrutti in modalità sicura (a fronte di policy definite / non definite in modo completo/appropriato).

11. Il trattamento di dati personali è svolto da un numero indefinito 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.
Esempi:
• Il sistema di biglietteria delle risorse umane di un'azienda può essere visualizzato da tutti i membri del personale.
• Le cartelle cliniche dei pazienti possono essere elaborate dalle segretarie sebbene solo il personale medico curante dovrebbe avere accesso.
□ SI □ NO

12. Vi sono parti del trattamento svolte da un agente o da un soggetto terzo (responsabile del trattamento)?

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 quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.
Esempi:

• Il sistema informatico di una scuola privata è ospitato in un data center esterno.
• I file dei clienti di una compagnia di assicurazioni vengono elaborati da collaboratori esterni della compagnia
• Viene incaricata una società specializzata per la distruzione di cartelle cliniche dei pazienti in una clinica medica.
• Un'azienda utilizza una soluzione Cloud as a Service per gestire le risorse interne.

□ SI □ NO

13. Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?

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.

Esempi:

• I dipendenti non sono chiaramente informati del fatto che stanno elaborando informazioni riservate che non possono essere divulgate a parti non autorizzate.
• Ai collaboratori esterni di una società non vengono fornite istruzioni chiare in merito al livello di sicurezza richiesto dei dati personali da loro trattati.

□ SI □ NO

14. Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia 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.

Esempi:

• Non tutte le persone coinvolte nel trattamento dei dati sono informate sulle possibili minacce alla sicurezza e sull'uso corretto delle risorse.
• Il personale che gestisce il centro telefonico di un'azienda non è stato informato di possibili attacchi di phishing e mirati.

□ SI □ NO

15. I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere 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.

Esempi:

• I dati delle risorse umane dei dipendenti non vengono conservati in schedari chiusi a chiave.
• Le copie delle fatture ricevute con carta di credito e dettagli del conto bancario non vengono distrutte con i distruggidocumenti, dopo essere state elaborate.

□ SI □ NO

3.D. Settore di attività e scala del trattamento

Settori di operatività e scala del trattamento: la probabilità di accadimento della minaccia è BASSA / MEDIA / ALTA visto che il settore di operatività della AMMINISTRAZIONE è / non è, in generale, considerato a rischio di cyber attacchi. Viene assunto che nessuna / qualche violazione o furto di dati sia nota o accaduta in passato e che le operazioni di trattamento siano eseguite / non siano eseguite unicamente dal personale della AMMINISTRAZIONE

16. Ritenete che il Vostro settore di attività sia passibile di attacchi cibernetici (cyberattacks)?

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.

Esempi:

• Diverse aziende (dello stesso settore) sono state attaccate nell'ultimo anno.

• È stata data pubblicità a possibili minacce alla sicurezza e vulnerabilità del particolare settore di attività (ad es. Come risultato di uno studio).

□ SI □ NO

17. L’ente ha subito attacchi cibernetici o altre tipologie 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.

Esempi:

• Il reparto IT ha rilevato un numero maggiore di tentativi non riusciti da parte di sistemi esterni di ottenere l'accesso non autorizzato al database.

• Sono stati violati i blocchi nel data center centrale.

□ SI □ NO

18. Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati 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.

Esempi:

• Gli utenti del servizio in linea di un negozio online hanno informato che potrebbero accedere accidentalmente agli account di altri utenti.

• I revisori hanno riscontrato che la politica delle password utilizzata da un servizio in linea è debole.

□ SI □ NO

19. Un trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?

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).

Esempi:

• Un'applicazione online per la cartella clinica di un ospedale che archivia i dati dei pazienti con malattie croniche in tutto il paese.

• Un sito di incontri online che memorizza i profili di centinaia di utenti.

□ SI □ NO

20. Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività dell’ente che non siano state implementate in misura adeguata?

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.

Esempi:

• Una società soggetta a specifiche misure di sicurezza per dispositivi medici, servizi finanziari o servizi di telecomunicazione.

□ SI □ NO

Valutazione della probabilità di occorrenza delle minacce per area

Area di valutazione	n. risposte affermative	Livello	Punteggio
3.A. Risorse di rete e tecnologiche (hardware e software)	0 – 1	Basso	1
	2 – 3	Medio	2
	4 – 5	Alto/Molto Alto	3
3.B. Processi/procedure connessi al trattamento	0 – 1	Basso	1
	2 – 3	Medio	2
	4 – 5	Alto/Molto Alto	3
	0 – 1	Basso	1

3.C. Soggetti e persone coinvolti nel trattamento	2 – 3	Medio	2
	4 – 5	Alto/Molto Alto	3
3.D. Settore di attività e scala del trattamento	0 – 1	Basso	1
	2 – 3	Medio	2
	4 – 5	Alto/Molto Alto	3

4. Valutazione del rischio

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la relativa probabilità di insorgenza della minaccia, è possibile la valutazione finale del rischio come mostrato di seguito.

	IMPACT LEVEL		
PROBABILITÀ DI MINACCIA	Basso	Medio	Alto / Molto Alto
Basso	☐	☐	☐
Medio	☐	☐	☐
Alto/Molto Alto	☐	☐	☐

Legend
Rischio Basso
Rischio Medio
Rischio Alto/Molto Alto

Il livello di rischio per l'operazione di elaborazione è Alto/Molto Alto.

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

Basso: è improbabile che la minaccia si materializzi.
Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
Alto/Molto Alto: la minaccia potrebbe materializzarsi.

Le tabelle 4 e 5 possono quindi essere utilizzate per documentare la probabilità di occorrenza delle minacce
per ciascuna area di valutazione e di conseguenza calcolare il suo valore finale.

T4. Valutazione della probabilità di occorrenza delle minacce per area

AREA DI VALUTAZIONE	PROBABILITA’	
	LIVELLO	PUNTEGGIO
RETE E RISORSE TECNICHE	Basso	1
	Medio	2
	Alto/Molto Alto	3

PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto/Molto Alto	3
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto/Molto Alto	3
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Basso	1
	Medio	2
	Alto/Molto Alto	3

T5. Valutazione della probabilità di occorrenza di una minaccia

Somma globale della probabilità di occorrenza di una minaccia	LIVELLO DI PROBABILITÀ DELLE MINACCE
4 - 5	Basso
6 - 8	Medio
9 -12	Alto/Molto Alto

La probabilità di occorrenza finale della minaccia viene calcolata dopo aver sommato i quattro diversi punteggi ottenuti nella Tabella 4 e associato il risultato complessivo alle somme globali della Tabella 5.

5. misure di sicurezza – ENISA ISO 27001:2013

ORGANIZATIONAL SECURITY MEASURES

- Security management
  - Security policy and procedures for the protection of personal data
  - Roles and responsibilities
  - Access control policy
  - Resource/asset management
  - Change management
  - Data processors
- Incident response and business continuity
  - Incidents handling / Personal data breaches
  - Business continuity
- Human resources
  - Confidentiality of personnel
  - Training

TECHNICAL SECURITY MEASURES

- Access control and authentication
- Logging and monitoring
- Security of data at rest
  - Server/Database security
  - Workstation security
- Network/Communication security
- Back-ups
- Mobile/Portable devices
- Application lifecycle security
- Data deletion/disposal
- Physical security

A seguito della valutazione del livello di rischio, l'organizzazione può procedere alla selezione di adeguate misure di sicurezza per la protezione dei dati personali: organizzative e tecniche. Queste categorie sono state ulteriormente suddivise in sottocategorie con una breve descrizione, che spiega come ciascuna sottocategoria si riferisce a disposizioni specifiche del GDPR e riferite alla norma ISO 27001:2013.
In ciascuna sottocategoria sono presentate le misure per livello di rischio, seguendo lo stesso schema di colorazione utilizzato nella valutazione impatto e minacce (basso: verde, medio: giallo, alto: rosso). Per ottenere la scalabilità, si presume che tutte le misure descritte sotto il livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, le misure presentate sotto il livello medio (giallo) sono applicabili anche a livello di rischio elevato. Le misure presentate sotto il livello alto (rosso) non sono applicabili a nessun altro livello di rischio.
Va notato che l'abbinamento delle misure a specifici livelli di rischio non dovrebbe essere percepito come assoluto. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare l'adozione di misure aggiuntive, anche se assegnate a un livello di rischio più elevato.

POLITICA DI SICUREZZA E PROCEDURE PER LA PROTEZIONE DEI DATI PERSONALI

Measure identifier	Measure description	Risk level	
A.1	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	A.5	Politica di sicurezza
A.2	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	A.5	Politica di sicurezza
A.3	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate	A.5	Policy di sicurezza
A.4	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	A.5	Policy di sicurezza
A.5	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.	A.5	Policy di sicurezza
A.6	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.	A.5	Security policy

RUOLI E RESPONSABILITÀ

Measure identifier	Measure description	Risk level	
B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	A.6.1.1	Ruoli e responsabilità della sicurezza delle informazioni

B.2	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l’organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	A.6.1.1	Ruoli e responsabilità della sicurezza delle informazioni
B.3	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	A.6.1.1	Ruoli e responsabilità della sicurezza delle informazioni
B.4	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	A.6.1.1	Information security roles and responsibilities
B.5	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.	A.6.1.1	Information security roles and responsibilities

POLITICA DI CONTROLLO DELL'ACCESSO

Measure identifier	Measure description		Risk level
C.1	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	A.9.1.1	Politica di controllo degli accessi
C.2	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell’ambito dei processi e delle procedure relative ai dati personali.	A.9.1.1	Politica di controllo degli accessi
C.3	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).	A.9.1.1	Politica di controllo degli accessi
C.4	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff	A.9.1.1	Access control policy

GESTIONE RISORSE / RISORSE

Measure identifier	Measure description	Risk level	
D.1	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	A.8	Asset management
D.2	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	A.8	Asset management
D.3	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	A.8	Gestione delle risorse
D.4	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	A.8	Asset management

CAMBIO GESTIONE

Measure identifier	Measure description	Risk level	
E.1	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	A. 12.1	Procedure operative e responsabilità
E.2	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	A. 12.1	Procedure operative e responsabilità
E.3	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.	A. 12.1	Procedure operative e responsabilità

RESPONSABILI DEL TRATTAMENTO DEI DATI

Measure identifier	Measure description	Risk level

F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / fornitori outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	A.15 Rapporti con i fornitori	
F.2	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	A.15 Rapporti con i fornitori	
F.3	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	A.15 Rapporti con i fornitori	
F.4	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.	A.15 Rapporti con i fornitori	
F.5	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.	A.15 Rapporti con i fornitori	

GESTIONE DEGLI INCIDENTI / VIOLAZIONE DEI DATI PERSONALI

Measure identifier	Measure description		Risk level
G.1	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni	
G.2	Le violazioni dei dati personali (come definite dall’art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l’organizzazione interna.. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni	
G.3	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un	A.16 Gestione degli incidenti di sicurezza delle informazioni	

	elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	
G.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti	A.16 Gestione degli incidenti di sicurezza personali (data breaches) l'evento e le successive azioni di mitigazione intraprese.

BUSINESS CONTINUITY		
Measure identifier	**Measure description**	**Risk level**
H.1	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
H.2	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
H.3	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.	A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
H.4	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.	A.17 Aspetti di sicurezza nella gestione della business continuity
H.5	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.	A.17 Aspetti di sicurezza nella gestione della business continuity

RISERVATEZZA DEL PERSONALE

Measure identifier	Measure description		Risk level
I.1	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione .	A.7 delle risorse umane	Sicurezza
I.2	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.	A.7 delle risorse umane	Sicurezza
I.3	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).	A7 delle risorse umane	Sicurezza

FORMAZIONE

Measure identifier	Measure description		Risk level
J.1	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione	
J.2	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.	A.7.2.2 Consapevolezza, educazione e formazione alla sicurezza delle informazioni	
J.3	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.	A.7.2.2. Consapevolezza, educazione e formazione alla sicurezza delle informazioni	

CONTROLLO ACCESSI E AUTENTICAZIONE

Measure identifier	Measure description		Risk level
K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	A.9 Controllo degli accessi	

K.2	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	A.9 Controllo degli accessi	
K.3	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	A.9 Controllo degli accessi	
K.4	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	A.9 Controllo degli accessi	
K.5	Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	A.9 Controllo degli accessi	
K.6	Le password degli utenti devono essere memorizzate in una forma "hash".	A.9 Controllo degli accessi	
K.7	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.	A.9 Controllo degli accessi	
K.8	Dovrebbe essere una soggetto ad autenticazione ogni dispositivo (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale	A.9 Controllo degli accessi	

REGISTRAZIONE E MONITORAGGIO

Measure identifier	Measure description	Risk level
L.1	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	A.12.4 Registrazione e monitoraggio
L.2	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero	A.12.4 Registrazione e monitoraggio

	essere sincronizzati con un'unica fonte temporale di riferimento		
L.3	Dovrebbe essere necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.	A.12.4 Registrazione e monitoraggio	
L.4	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.	A.12.4 Registrazione e monitoraggio	
L.5	Un sistema di monitoraggio dovrebbe generare i file log e produrre report sullo stato del sistema e notificare potenziali allarmi.	A.12.4 Registrazione e monitoraggio	
SICUREZZA SERVER / DATABASE			
M.1	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	A. Operations security	12
M.2	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR) .	A. Operations security	12
M.3	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.	A. 12 Sicurezza delle operazioni	
M.4	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.	A. 12 Sicurezza delle operazioni	
M.5	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni	A. 12 Sicurezza delle operazioni	
M.6	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.	A.12 Operazioni di sicurezza	

SICUREZZA DELLA WORKSTATION			
Measure identifier	**Measure description**		**Risk level**
N.1	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione	
N.2	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione	
N.3	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione	
N.4	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione	
N.5	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione	
N.6	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione	
N.7	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	A.14.1 Requisiti di sicurezza nei sistemi	
N.8	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.	A.14.1 Requisiti di sicurezza nei sistemi	
N.9	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.	A.14.1 Requisiti di sicurezza nei sistemi	

SICUREZZA DI RETE / COMUNICAZIONE		
Measure identifier	**Measure description**	**Risk level**

O.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	A.13 Communications Security
O.2	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.	A.13 Sicurezza delle comunicazioni
O.3	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.	A.13 Sicurezza delle comunicazioni
O.4	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	A.13 Sicurezza delle comunicazioni
O.5	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.	A.13 Sicurezza delle comunicazioni
O.6	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.	A.13 Sicurezza delle comunicazioni
O.7	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC)	A.13 Sicurezza delle comunicazioni

BACK-UP

Measure identifier	Measure description	Risk level
P.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	A.12.3 Back-Up
P.2	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	A.12.3 Back-Up
P.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	A.12.3 Back-Up

P.4	I backup completi devono essere eseguiti regolarmente.	A.12.3	Back-Up
P.5	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.	A.12.3	Back-Up
P.6	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.	A.12.3	Back-Up
P.7	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.	A.12.3	Back-Up
P.8	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento.	A.12.3	Back-Up
P.9	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.	A.12.3	Back-Up

DISPOSITIVI MOBILI / PORTATILI

Measure identifier	Measure description		Risk level
Q.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	A. 6.2	Dispositivi mobili e teleworking
Q.2	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	A. 6.2	Dispositivi mobili e teleworking
Q.3	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	A. 6.2	Dispositivi mobili e teleworking
Q.4	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	A. 6.2	Dispositivi mobili e telelavoro
Q.5	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un	A. 6.2	Dispositivi mobili e telelavoro

	dispositivo mobile che è stato compromesso.	
Q.6	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.	A. 6.2 Dispositivi mobili e telelavoro
Q.7	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.	A. 6.2 Dispositivi mobili e telelavoro
Q.8	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte)	A.6.2 Dispositivi mobile e telelavoro
Q.9	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.	A.6.2 Dispositivi mobile e telelavoro

SICUREZZA DEL CICLO DI VITA DELLE APPLICAZIONI

Measure identifier	Measure description	Risk level
R.1	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.2	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.3	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.4	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.5	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto

R.6	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L’applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.7	Devono essere eseguiti test periodici di penetrazione.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.8	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
R.9	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto

CANCELLAZIONE / DISTRUZIONE DEI DATI

Measure identifier	Measure description	Risk level
S.1	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.	A. 8.3.2 Smaltimento di supporti e 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
S.2	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
S.3	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.	A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
S.4	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.	A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
S.5	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.	A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura

S.6	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all’esterno dei dati personali.	A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura

SICUREZZA FISICA		
Measure identifier	**Measure description**	**Risk level**
T.1	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	A.11 - Sicurezza fisica e ambientale
T.2	Identificazione chiara, tramite mezzi appropriati, ad es. I badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.	A.11 – Sicurezza fisica e ambientale
T.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro	A.11 – Sicurezza fisica e ambientale
T.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.	A.11 – Sicurezza fisica e ambientale
T.5	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	A.11 – Sicurezza fisica e ambientale
T.6	Le aree sicure libere devono essere bloccate fisicamente e riviste periodicamente	A.11 Sicurezza fisica e ambientale
T.7	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.	A.11 Sicurezza fisica e ambientale
T.8	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.	A.11 – Sicurezza fisica e ambientale

6. Esportare l'analisi e le misure proposte

Documento relativo alla sintesi dei passaggi precedenti con reportistica misure individuate come adeguate ai fini della riduzione del rischio e dell’accettazione dello stesso in quanto ritenuto non grave ai fini della tutela dei diritti e delle libertà fondamentali degli individui così come previsto dall’art. 32 del GDPR.

Al quesito: Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Possiamo rispondere, al termine della procedura descritta, che le misure tecniche ed organizzative individuate riguardano quelle riconducibili a quelle riferite al seguente elenco: “Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Sicurezza dei siti web, Backup, Manutenzione, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware,

Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Integrare la protezione della privacy nei progetti, Gestione del personale, Protezione contro fonti di rischio non umane, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati”.

Ai fini della complementarietà tra valutazione del rischio dei trattamenti dei dati personali e procedura di Valutazione di impatto del trattamento dei dati DPIA, fermo restando quanto descritto nel documento proposto con nota **prot. n. 0135203-2019**, ritengo opportuno riportare:

- estratto dalla norma ISO 29134/2017 in merito ai controlli che si pongono in continuità con i controlli della norma ISO 27001:2013;
- tabelle riassuntive degli elementi da tenere in considerazione in merito alla valutazione delle vulnerabilità e delle minacce, nonché della relativa gravità (impatto).

ISO 29134:2017 – Annex B

CATEGORIA	**AZIONE**	RISCHIO PRIVACY	***ESEMPIO DI MINACCE***
Hardware	**Uso anomalo**	Perdita dei dati	*Archiviazione di informazioni, uso personale*
Hardware	**Uso anomalo**	Accesso illegittimo ai dati	*Utilizzo di USB flash drives o dischi che non sono idonei alla sensibilità delle informazioni; uso o trasporto di dispositivi sensibili per fini personali etc.*
Hardware	**Danni fisici/materiali**	Perdita dei dati	*Allagamenti, incendi, atti vandalici; danni fisici/materiali da eventi naturali o malfunzionamenti di dispositivi di memorizzazione, etc.*
Hardware	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Sbirciare lo schermo/passwords di persone, origliare, scattare foto di uno schermo, geolocalizzare dispositive, rilevamento di segnali elettromagnetici, etc.*
Hardware	**Perdita**	Perdita dei dati	*Furto di laptop o smartphones, smaltimento non controllato di hardware o dispositive, etc.*
Hardware	**Perdita**	Accesso illegittimo ai dati	*Furto di un pc portatile in una stanza d’albero, furto di smartphone aziendale da parte di un borseggiatore, recupero di dispositive di memorizzazione o di hardware; smarrimento di un dispositivo elettronico, etc.*
Hardware	**Modifica**	Perdita dei dati	*Aggiunta di hardware in compatibile che comporta malfunzionamenti; rimozione di component essenziali per l’operatività dei sistemi, etc.*
Hardware	**Modifica**	Accesso illegittimo ai dati	*Tracciamento da parte di un keylogger basato su hardware; rimozione di component; connessione di dispositive (es.*

CATEGORIA	**AZIONE**	RISCHIO PRIVACY	***ESEMPIO DI MINACCE***
			USB) che lanciano sistemi operativi o acquisiscono o modificano dati, etc.
Hardware	**Modifica**	Modifiche indesiderate ai dati personali	*Aggiunta di hardware incompatibile che provoca malfunzionamenti; rimozione di component essenziali per il corretto funzionamento di applicazioni, etc..*
Hardware	**Sovraccarico**	Perdita dei dati	*Dispositivi di memorizzazione (es. Dischi) pieni; sbalzi di corrente, sovraccarico delle capacità dei processori; surriscaldamento, temperature eccessive, etc.*
Hardware	**Perdita di dischi rigidi**	Accesso illegittimo ai dati	*Procedure di smaltimento o contratti di manutenzione superficiali o inidonei possono configurare accesso non autorizzato a dati personali.*
Software	**Uso anomalo**	Perdita dei dati	*Cancellazione di dati; uso di software copiato o contraffatto; errore di cancellazione dati da parte degli operatori*
Software	**Uso anomalo**	Accesso illegittimo ai dati	*Scansioni di contenuti; riferimenti incrociati illeciti; abuso di privilegi sui dati; cancellazione delle trace di utilizzo; invio di spam mediante un software e-mail; uso non corretto di funzioni di rete, etc.*
Software	**Uso anomalo**	Modifiche indesiderate ai dati personali	*Modifiche indesiderate alle informazioni nei database; cancellazione di files necessary per il corretto funzionamento di software; operatori che modificano dati, etc.*
Software	**Danni fisici/materiali**	Perdita dei dati	*Cancellazione di programmi eseguibili o di codice sorgente; bombe logiche, etc.*
Software	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Scanning di indirizzi e porte di rete; raccolta di dati di configurazione; analisi di codice sorgente per individuare vulnerabilità e falle nei sistemi; test di come I database rispondano a queries di attacco deliberato, etc.*
Software	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Scanning di indirizzi e porte di rete; vulnerabilità di attacco nell’ascolto, analisi e reporting delle porte e dei servizi.*
Software	**Perdita**	Perdita dei dati	*Licenze del software usato per l’accesso ai dati non rinnovate, etc.*
Software	**Modifica**	Perdita dei dati	*Errori durante aggiornamenti, configurazione o manutenzione; infezioni da malware; sostituzione di componenti, etc.*

CATEGORIA	**AZIONE**	RISCHIO PRIVACY	***ESEMPIO DI MINACCE***
Software	**Modifica**	Accesso illegittimo ai dati	*Tracciamento da keylogger software-based; infezioni da malware; installazione di tools di Amministrazione remota; sostituzione di componenti o parti del software, etc.*
Software	**Modifica**	Modifiche indesiderate ai dati personali	*Errori durante aggiornamenti, configurazione o manutenzione; infezioni da malware; sostituzione di componenti, etc.*
Software	**Sovraccarico**	Perdita dei dati	*Eccedenze nelle dimensioni del database; iniezioni di dati fuori dall’intervallo normale dei valori, etc.*
Mezzi di comunicazione informatica	**Danni fisici/materiali**	Perdita dei dati	*Taglio dei cavi di rete; segnale Wi.-Fi non sufficiente, etc.*
Mezzi di comunicazione informatica	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Intercettazione di traffic Ethernet; acquisizione di dati trasmessi in una rete Wi-Fi, etc.*
Mezzi di comunicazione informatica	**Perdita**	Perdita dei dati	*Furto di cavi di rame, etc.*
Mezzi di comunicazione informatica	**Modifica**	Modifiche indesiderate ai dati personali	*Attacchi “Man-in-the-middle” o “Man in the browser” per modificare o aggiungere dati al traffic di rete; attacchi replay (reinvio di dati intercettati), etc.*
Mezzi di comunicazione informatica	**Sovraccarico**	Perdita dei dati	*Uso improprio di banda; download non autorizzati; perdita di connettività Internet, etc.*
Persone	**Uso anomalo**	Accesso illegittimo ai dati	*Influenze (phishing, social engineering, corruzione, etc.); pressioni (ricatti, molestie psicologiche, etc.), etc.*
Persone	**Uso anomalo**	Modifiche indesiderate ai dati personali	*Influenze (pettegolezzi, disinformazione, etc.), etc.*
Persone	**Danni fisici/materiali**	Perdita dei dati	*Infortunio sul lavoro; malattia professionale; oltri infortuni o malattie; morte; indisposizione neurologica, psicologica o psichiatrica, etc.*
Persone	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Divulgazione non intenzionale di informazioni nei colloqui; uso di dispositive di ascolto per origliare o registrare di nascosto negli incontri, etc.*

CATEGORIA	**AZIONE**	RISCHIO PRIVACY	***ESEMPIO DI MINACCE***
Persone	**Perdita**	Perdita dei dati	*Riassegnazione ruoli; termine o cessazione per interruzione di contratti; subentro di tutta o parte dell’organizzazione, etc.*
Persone	**Perdita**	Accesso illegittimo ai dati	*Soffiare il personale ad un’altra organizzazione; cambi di mansione; subentro di tutta o parte dell’organizzazione, etc.*
Persone	**Sovraccarico**	Perdita dei dati	*Carichi di lavoro eccessivi, stress o cambiamenti negative nelle condizioni lavorative; assegnazione di compiti al personale oltre le loro capacità; uso insufficiente di competenze, etc.*
Persone	**Sovraccarico**	Modifiche indesiderate ai dati personali	*Carichi di lavoro eccessivi, stress o cambiamenti negative nelle condizioni lavorative; assegnazione di compiti al personale oltre le loro capacità; uso insufficiente di competenze, etc.*
Documenti cartacei	**Danni fisici/materiali**	Perdita dei dati	*Invecchiamento o deterioramento dei documenti archiviati; documenti bruciati durante un incendio, etc.*
Documenti cartacei	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Leggere, fotocopiare, fotografare, etc.;*
Documenti cartacei	**Perdita**	Perdita dei dati	*Furto di documenti; perdita di documentazione durante spostamenti; smaltimento, etc.*
Documenti cartacei	**Perdita**	Accesso illegittimo ai dati	*Furto di documenti dagli uffici; furto dalle cassette postali; recupero dati da documenti gettati via, etc.*
Documenti cartacei	**Modifica**	Modifiche indesiderate ai dati personali	*Cambio di ciifre in un document, sostituzione di un document originale con una copia falsificata, etc.*
Documenti cartacei	**Sovraccarico**	Perdita dei dati	*Cancellazione graduale nel tempo; cancellazione volontaria di porzioni di documenti, etc.*
Canali di trasmissione documentazione cartacea	**Danni fisici/materiali**	Perdita dei dati	*Interruzione di un flusso autorizzativo dovuto ad una riorganizzazione; consegna di posta interrotta da sciopero, etc.*
Canali di trasmissione documentazione cartacea	**Intercettazione (umana/tecnologica)**	Accesso illegittimo ai dati	*Lettura di libri firma in circolazione; riproduzione documenti in transito, etc.*

CATEGORIA	**AZIONE**	RISCHIO PRIVACY	***ESEMPIO DI MINACCE***
Canali di trasmissione documentazione cartacea	**Perdita**	Perdita dei dati	*Eliminazione di un processo a seguito di una riorganizzazione; perdita di un fornitore di consegna documenti, etc.*
Canali di trasmissione documentazione cartacea	**Modifica**	Perdita dei dati	*Modifiche a come la posta viene smistata. Riorganizzazione dei sistemi di trasmissione documentazione cartacea; cambio di lingua ufficiale o lavorativa, etc.*
Canali di trasmissione documentazione cartacea	**Modifica**	Modifiche indesiderate ai dati personali	*Modifiche a una nota senza che l’autore ne sia a conoscenza; cambio da un libro firma ad un altro; invio di più documenti in conflitto tra loro, etc.*
Canali di trasmissione documentazione cartacea	**Sovraccarico**	Perdita dei dati	*Quantità di posta eccessiva; processo di validazione sovraccarico, etc.*

Tabelle riassuntive:

Criteri di valutazione delle informazioni

Liv.	R- Riservatezza	I - Integrità	D- Disponibilità
1 - Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio e tempo necessario per correggere le informazioni).	**Organizzazione** L’indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio e tempo necessario per correggere le informazioni).

2 - Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all’immagine), ma un’eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici e che creano piccole difficoltà (p.e. costi, paura, incomprensioni, stress, malanni minori) a causa degli effetti sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un’impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici e che creano piccole difficoltà (p.e. costi, mancato accesso a servizi, incomprensioni, stress, malanni minori), a causa degli effetti vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L’indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici e che creano piccole difficoltà (p.e. costi, mancato accesso a servizi, incomprensioni, stress, malanni minori), a causa degli effetti vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
3 - Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all’immagine) e un’eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha elevato impatto (esempi: fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute) che può essere superato con difficoltà sulla vita sociale o personale degli interessati.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un’impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto (esempi: fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute) sulla vita sociale o personale degli interessati.	**Organizzazione** L’indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di **disponibilità** ha elevato impatto (esempi: fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute) sulla vita sociale o personale degli interessati.

4 - Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti non reversibili sulla vita degli interessati in termini di: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di integrità ha impatti non reversibili sulla vita degli interessati in termini di: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L’indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. **Interessati** La mancanza di disponibilità ha impatti non reversibili sulla vita degli interessati in termini di: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

Categoria	**Minaccia**
Danni fisici	Incendio
	Allagamento
	Polvere, corrosione, congelamento.
	Distruzione di strumentazione da parte di malintenzionati o per errore (disattenzione)
	Attacchi (bombe, terroristi)
Eventi naturali	Fenomeni climatici (uragani, nevicate)
	Terremoti, eruzioni vulcaniche
	Fulmini e scariche atmosferiche
Perdita di servizi essenziali	Guasto aria condizionata o sistemi di raffreddamento
	Perdita di energia (o sbalzi di tensione)
	Malfunzionamento nei componenti di rete
	Errori di trasmissione (incluso il misrouting)
	Interruzione nei collegamenti di rete (inclusi danni alle linee di TLC)
	Eccesso di traffico sulla rete
	Interruzione di servizi erogati riconducibili ai fornitori esterni (inclusi ISP, CSP, DR site, supporto tecnico specialistico, esternalizzazione attività). Per esempio a causa di fallimento, chiusura, incidenti.
	Indisponibilità di personale (malattie, sciopero, eccetera)
Disturbi	Disturbi elettromagnetici
Compromissione di informazioni	Intercettazione (inclusa analisi del traffico)
	Furto di documenti o supporti di memorizzazione
	Furto di apparati o componenti
	Recupero di informazioni da media (principalmente memorie di massa) dismessi.
	Rivelazione di informazioni (da parte del personale o fornitori)
	Ricezione dati da origini non affidabili
	Infiltrazione nelle comunicazioni
	Ripudio dei messaggi
Problemi tecnici	Fault o malfunzionamento della strumentazione IT
	Saturazione dei sistemi IT
	Malfunzionamenti software applicativi sviluppati per i clienti
	Malfunzionamenti pacchetti software usati internamente
	Malfunzionamenti software applicativi sviluppati per uso interno
	Errori di manutenzione hardware e software di base
Azioni non autorizzate	Uso non autorizzato o negligente della strumentazione
	Importazione o esportazione illegale di software (copia illegale di software o uso di software illegale)
	Alterazione volontaria e non autorizzata di dati di business
	Virus (malware, anche per mobile)
	Accesso non autorizzato alla rete (anche tramite AP wireless non autorizzati)
	Uso non autorizzato della rete da parte degli utenti o abuso delle autorizzazioni

	Trattamento (volontario o inconsapevole) non consentito di dati (personali)
Compromissione di funzioni	Errori degli utenti
	Uso dei servizi da parte di persone non autorizzate o elevamento di privilegi.
	Degrado dei media (memorie di massa)
	Uso di servizi in modo non autorizzato
	Furto identità

Criteri di valutazione delle minacce

Livello	Linee guida per la verosimiglianza
1 - Bassa	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare con frequenza inferiore rispetto a quanto riportato dalle ricerche più note; - in caso di **attacco deliberato**, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico e con scarse risorse a disposizione. - in caso di attacco **non deliberato**, l’ambito è poco complesso e quindi è difficile commettere errori; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 - Media	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare secondo quanto riportato dalle ricerche più note; - in caso di **attacco deliberato**, i dati sono poco appetibili e l'immagine aziendale non è compromessa e quindi può essere condotto da malintenzionati non particolarmente motivati, mediamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque rari; - in caso di **attacco non deliberato**, l’ambito è mediamente complesso e quindi possono essere commessi errori; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.
3 - Alta	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; - in caso di **attacco deliberato**, i dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente; - in caso di attacco **non deliberato**, l’ambito è di elevata complessità (per esempio per molteplicità di sedi, tipologie di sistemi informatici, utenti interni e/o esterni) e quindi è facile siano commessi errori; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia si verifica quasi certamente.

Asset	**vulnerabilità**	**minacce**
Hardware	manutenzione insufficiente / installazione errata del supporto di memorizzazione	violazione della manutenibilità del sistema informativo
	mancanza di schemi periodici di sostituzione	distruzione di attrezzature o media
	suscettibilità a umidità, polvere, sporco	polvere, corrosione, congelamento
	sensibilità alle radiazioni elettromagnetiche	radiazioni elettromagnetiche
	mancanza di un controllo efficiente delle modifiche alla configurazione	errore in uso
	suscettibilità alle variazioni di tensione	perdita di alimentazione
	suscettibilità alle variazioni di temperatura	fenomeno meteorologico
	memoria non protetta	furto di media o documenti
	mancanza di cure a disposizione	furto di media o documenti
	copia incontrollata	furto di media o documenti
Software	test del software assente o insufficiente	abuso dei diritti
	difetti noti nel software	abuso dei diritti
	nessun "logout" quando si lascia la workstation	abuso dei diritti
	smaltimento o riutilizzo dei supporti di memorizzazione senza la corretta cancellazione	abuso dei diritti
	mancanza di piste di controllo	abuso dei diritti
	assegnazione errata dei diritti di accesso	abuso dei diritti
	software distribuito su larga scala	corruzione dati
	applicare i programmi applicativi ai dati errati in termini di tempo	corruzione dati
	interfaccia utente complicata	errore in uso
	mancanza di documentazione	errore in uso
	impostazione errata dei parametri	errore in uso
	date errate	errore in uso
	mancanza di meccanismi di identificazione e autenticazione come l'autenticazione dell'utente	falsificazione dei diritti
	tabelle password non protette	falsificazione dei diritti
	cattiva gestione delle password	falsificazione dei diritti
	servizi non necessari abilitati	trattamento illecito di dati
	software immaturo o nuovo	malfunzionamento del software
	specifiche non chiare o incomplete per gli sviluppatori	malfunzionamento del software
	mancanza di un efficace controllo delle modifiche	malfunzionamento del software
	download e utilizzo incontrollati del software	manomissione del software
	mancanza di copie di backup	manomissione del software
	mancanza di protezione fisica dell'edificio, porte e finestre	furto di media o documenti
	mancata produzione di rapporti di gestione	uso non autorizzato dell'attrezzatura

Network	mancanza di prova dell'invio o della ricezione di un messaggio	diniego di azioni
	linee di comunicazione non protette	intercettazioni
	traffico sensibile non protetto	intercettazioni
	scarso cablaggio comune	guasto delle apparecchiature di telecomunicazione
	unico punto di errore	guasto delle apparecchiature di telecomunicazione
	mancanza di identificazione e autenticazione del mittente e del destinatario	falsificazione dei diritti
	architettura di rete non sicura	spionaggio remoto
	trasferimento delle password in chiaro	spionaggio remoto
	inadeguata gestione della rete (resilienza del routing)	saturazione del sistema informativo
	connessioni di rete pubblica non protette	uso non autorizzato dell'attrezzatura
Presonnel	assenza di personale	violazione della disponibilità del personale
	procedure di assunzione inadeguate	distruzione di attrezzature o media
	formazione di sicurezza insufficiente	errore in uso
	uso errato di software e hardware	errore in uso
	mancanza di consapevolezza della sicurezza	errore in uso
	mancanza di meccanismo di monitoraggio	trattamento illecito di dati
	lavoro non supervisionato da parte di personale esterno o addetto alle pulizie	furto di media o documenti
	serie di politiche per l'uso corretto dei media e dei messaggi di telecomunicazione	uso non autorizzato dell'attrezzatura
Site	uso inadeguato o negligente del controllo di accesso fisico agli edifici e alla stanza	distruzione di attrezzature o media
	posizione in una zona suscettibile alle inondazioni	alluvione
	rete elettrica instabile	perdita di alimentazione
	mancanza di protezione fisica dell'edificio, porte e finestre	furto di attrezzature
Organizatio n	mancanza di procedura formale per la registrazione e la cancellazione della registrazione dell'utente	abuso dei diritti
	mancanza di un processo formale per la revisione del diritto di accesso (supervisione)	abuso dei diritti
	disposizioni mancanti o insufficienti (relative alla sicurezza) nei contratti con clienti e / o terzi	abuso dei diritti
	mancanza di procedura di monitoraggio delle strutture di elaborazione delle informazioni	abuso dei diritti
	mancanza di audit regolari (supervisione)	abuso dei diritti
	mancanza di procedure di identificazione e valutazione del rischio	abuso dei diritti
	mancanza di segnalazioni di errori registrate nei registri dell'amministratore e dell'operatore	abuso dei diritti

	risposta di manutenzione del servizio inadeguata	violazione della manutenibilità del sistema informativo
	mancanza o insufficiente accordo sul livello di servizio	violazione della manutenibilità del sistema informativo
	mancanza di procedura di controllo delle modifiche	violazione della manutenibilità del sistema informativo
	mancanza di procedura formale per il controllo della documentazione ISMS	corruzione dati
	mancanza di procedura formale per la supervisione dei registri ISMS	corruzione dati
	mancanza di un processo formale per l'autorizzazione delle informazioni disponibili al pubblico	dati da fonti inaffidabili
	mancanza di un'adeguata allocazione delle responsabilità in materia di sicurezza delle informazioni	diniego di azioni
	mancanza di piani di continuità	guasto dell'attrezzatura
	mancanza di criteri di utilizzo della posta elettronica	errore in uso
	mancanza di procedure per l'introduzione di software nei sistemi operativi	errore in uso
	mancanza di record nei registri degli amministratori e degli operatori	errore in uso
	mancanza di procedure per la gestione di informazioni classificate	errore in uso
	mancanza di responsabilità in materia di sicurezza delle informazioni nelle descrizioni dei lavori	errore in uso
	disposizioni carenti o insufficienti (relative alla sicurezza delle informazioni) nei contratti con i dipendenti	trattamento illecito di dati
	mancanza di un processo disciplinare definito in caso di incidente di sicurezza delle informazioni	furto di attrezzature
	mancanza di una politica formale sull'uso dei computer portatili	furto di attrezzature
	mancanza di controllo delle attività fuori sede	furto di attrezzature
	mancante o insufficiente politica "cancella scrivania e cancella schermo"	furto di media o documenti
	mancanza di autorizzazione per le strutture di elaborazione delle informazioni	furto di media o documenti
	mancanza di meccanismi di monitoraggio stabiliti per violazioni della sicurezza	furto di media o documenti
	mancanza di revisioni periodiche da parte della direzione	uso non autorizzato dell'attrezzatura
	mancanza di procedure per la segnalazione dei punti deboli della sicurezza	uso non autorizzato dell'attrezzatura
	mancanza di procedure di disposizioni rispetto dei diritti intellettuali	utilizzo di software contraffatto o copiato

Per comprendere il livello di impatto e la gravità delle conseguenze per gli interessati all’attività di trattamento:

Categoria di impatto	Descrizione	Livello di importanza
Impatto psicologico	Impressione di violazione della privacy senza danno reale (fastidio, disagio)	**Basso**
Impatto materiale	Perdita di tempo dovuto alla necessità di ripetizione di azioni già svolte (es. reinserimento dati per formalità, riconfigurazione, etc.)	**Basso**
Impatto psicologico	Disagio per persone più vulnerabili (es. lievi fastidi per minori o persone con necessità di tutori)	**Basso**
Impatto materiale	Fastidio derivante dall’impressione del riutilizzo dei propri dati per pubblicità mirata	**Basso**
Impatto materiale	Ricezione di comunicazioni indesiderate (SPAM)	**Basso**
Impatto fisico	Malessere (es. mal di testa passeggero) o preoccupazione per mancanza di cura per una persona vulnerabile (es. minore)	**Basso**
Impatto psicologico	Sensazione di perdita di controllo dei propri dati e del rispetto per la libertà di navigazione	**Basso**
Impatto materiale	Eccessiva difficoltà di accesso, o mancato accesso, a servizi pubblici o commerciali (non vitali ma necessari)	**Medio**
Impatto fisico	Stress o disturbo minore psicologico o fisico (es. malattia lieve a seguito del mancato rispetto di controindicazioni)	**Medio**
Impatto materiale	Danno materiale non ingente derivante da un aspetto di vita privata che necessita riservatezza	**Medio**
Impatto materiale	Perdita di opportunità di comfort (es. cancellazioni di vacanze, cancellazione di account online, blocco account di servizi online, etc.)	**Medio**
Impatto psicologico	Diffamazione, discredito, danni reputazionali derivanti da comunicazioni mail indesiderate	**Medio**
Impatto psicologico	Intimidazione sui social network	**Medio**
Impatto materiale	Aumenti di costi o conseguenze economiche non previste (es. sanzioni, multe, interessi di mora, perdite di agevolazioni, etc.)	**Medio**
Impatto psicologico	Senso di violazione della privacy senza danni irreparabili, mancanza di riconoscimenti, problemi di relazioni con gli altri, discriminazione sui social network, danno di immagine, etc.	**Medio**
Impatto psicologico	Discriminazione in ambienti professionali o scolastici, opportunità perse di avanzamento carriera	**Medio**
Impatto materiale	Elaborazione di dati incorretti che provocano ad esempio malfunzionamenti negli account bancari o di servizi previdenziali	**Medio**
Impatto materiale	Pubblicità mirata online su aspetti confidenziali che si vogliono tenere nascosti (es. gravidanza, trattamenti relativi a dipendenze, etc.)	**Medio**
Impatto materiale	Profilazione inaccurata o inappropriata	**Medio**

Categoria di impatto	Descrizione	Livello di importanza
Impatto fisico	Disturbi fisici che provocano danni a lungo termine (es. aggravamento dello stato di salute a seguito di mancato rispetto di controindicazioni, o cure non appropriate)	**Alto**
Impatto materiale	Perdite economiche rilevanti , blocco conti bancari, etc.	**Alto**
Impatto materiale	Difficoltà di accesso a servizi pubblici importanti	**Alto**
Impatto materiale	Perdite di opportunità / agevolazioni uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici)	**Alto**
Impatto materiale	Appropriazioni indebite non compensate, difficoltà economiche non temporanee (es. necessità di prendere un prestito)	**Alto**
Impatto materiale	Divieto di tenuta di conti bancari	**Alto**
Impatto materiale	Divieto di spostamenti all’estero	**Alto**
Impatto materiale	Perdita dei dati dei propri Clienti	**Alto**
Impatto psicologico	Senso di violazione della privacy con danno irreparabile	**Alto**
Impatto fisico	Alterazione dell’integrità fisica (es. incidenti o aggressioni)	**Alto**
Impatto psicologico	Separazione o divorzio	**Alto**
Impatto psicologico	Discriminazione, forte sensazione di violazione dei diritti fondamentali e della libertà di espressione	**Alto**
Impatto materiale	Perdita dell’abitazione o del posto di lavoro	**Alto**
Impatto materiale	Esposizione a ricatti	**Alto**
Impatto materiale	Perdite monetarie a seguito di frodi o phishing	**Alto**
Impatto materiale	Danni alle proprietà o perdite monetarie non indennizzate	**Alto**
Impatto fisico	Grave disturbo psicologico (depressione, fobie, fragilità dopo citazioni in giudizio, dopo estorsioni)	**Alto**
Impatto psicologico	Cyber-bullismo, discriminazione, molestie psicologiche o sessuali	**Alto**
Impatto psicologico	Perdita della capacità di agire	**Altissimo**
Impatto fisico	Rapimento, sequestro di persona	**Altissimo**
Impatto materiale	Impossibilità di lavorare o incapacità di ricollocazione	**Altissimo**
Impatto materiale	Impossibilità di citare in giudizio	**Altissimo**
Impatto fisico	Disturbo psicologico a lungo termine o permanente	**Altissimo**
Impatto materiale	Sanzioni penali	**Altissimo**
Impatto fisico	Alterazione permanente dell’integrità fisica	**Altissimo**
Impatto materiale	Cambio di stato amministrativo e/o perdita dell’autonomia legale (necessità di supervisione terza)	**Altissimo**
Impatto materiale	Smarrimento di elementi di prova nell’ambito di un contenzioso	**Altissimo**
Impatto psicologico	Allontanamento o perdita di legami familiari	**Altissimo**
Impatto materiale	Rischio finanziario di indebitamento ingente	**Altissimo**
Impatto materiale	Perdita di accesso a infrastrutture vitali (acqua, elettricità, ecc)	**Altissimo**
Impatto fisico	Decesso	**Altissimo**

Allegato 3 “Linee Guida analisi rischio trattamenti di dati”