PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Autore/i: Dott. Aristide Reginelli - Avv. Stefano Rotondo

Accettato da: Dott. Sergio Sellitto

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1.0	2023	Prima versione	Dott. Aristide Reginelli Avv. Stefano Rotondo
2.0	2026	Aggiornamento Procedura	Dott. Aristide Reginelli Avv. Stefano Rotondo
L'ultima revisione sostituisce qualsiasi revisione precedente.			

CAPITOLO 1
GENERALITÀ

Il presente documento descrive il processo per la gestione delle violazioni di sicurezza che comportano gravi rischi per la perdita dei diritti e delle libertà individuali degli Interessati, le cui informazioni personali sono trattate e custodite presso i sistemi IT e presso i locali aziendali.

In particolare, secondo quanto previsto dal WP250 "*Guidelines on Personal data breach notification under Regulation 2016/679*" [5], gli eventi di possibile violazione dei dati personali possono essere suddivisi in tre macro categorie:

- "**violazione di riservatezza**": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "**violazione di disponibilità**": in caso di perdita accidentale o non autorizzata dell'accesso ai dati o di distruzione di dati personali;
- "**violazione di integrità**": in caso di alterazione non autorizzata o accidentale dei dati personali.

A norma dell'art. 33 del GDPR, la **notifica** della violazione all'Autorità Garante deve avvenire senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui se ne sia venuti a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

A norma dell'art. 34 del GDPR, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento **comunica la violazione all'interessato senza ingiustificato ritardo**.

1.1 SCOPO E AMBITO DI APPLICAZIONE

Scopo del presente documento è quello di definire in maniera chiara e comprensibile al personale aziendale preposto al trattamento dati, le attività e le modalità operative che consentano un approccio esaustivo ed omogeneo alla gestione delle violazioni di cui in premessa, secondo i criteri ed i principi stabiliti dalle vigenti normative.

Nello specifico, le linee guida in oggetto si applicano agli Uffici che trattano a qualsiasi titolo e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea) dati personali.

Con questo documento il Titolare del trattamento dei dati personali recepisce e pone in atto gli indirizzamenti cogenti formulati negli artt. 33 e 34 del Regolamento UE 679/2016 e nei vari Regolamenti emessi dal Garante per la tutela dei dati personali, con particolare riferimento al documento WP250 **"***Guidelines on Personal data breach notification under Regulation 2016/679*" [5].

1.2 RUOLO E SUPPORTO DEL DPO

La presente procedura è stata predisposta coerentemente al parere e alle raccomandazioni fornite dal Data Protection Officer (DPO), il cui "**supporto**", fornito per la messa in atto della seguente procedura ed eventualmente per ogni altro futuro intervento inerente la problematica in questione, è sempre di tipo prettamente consulenziale, come previsto dall'art. 39 del GDPR; il DPO, infatti, non può in alcun caso prendere decisioni al posto del Titolare del trattamento o sostituirsi nelle valutazioni rimesse dalla normativa data protection in capo a quest'ultimo.

1.3 DOCUMENTI DI RIFERIMENTO

- [1] Regolamento (UE) 679/2016 (GDPR);
- [2] Garante per la Protezione dei Dati Personali: Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) – 4 aprile 2013;
- [3] D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679;
- [4] WP29 Gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE (dal 25 maggio 2018 prende il nome di EDPB – European Data Protection Board);
- [5] WP250 Guidelines on Personal data breach notification under Regulation 2016/679;
- [6] Linee guida EDPB 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali.

1.4 DEFINIZIONI

Definizioni	Descrizione
Personal Data Breach	Violazioni di sicurezza che comportano gravi rischi per la perdita dei diritti e delle libertà individuali degli Interessati, le cui informazioni personali sono trattate e custodite presso i sistemi IT e presso i locali aziendali.
Agente malevolo	Soggetto che, sfruttando eventuali vulnerabilità di sicurezza logica, fisica o organizzativa, ovvero abusando dei poteri e delle conoscenze derivanti dal proprio ruolo, compie, volontariamente o accidentalmente, atti che comportano una violazione della riservatezza, dell'integrità e della disponibilità degli asset afferenti ai sistemi informativi aziendali preposti al trattamento di dati personali.
Allarme Privacy	Segnalazione formalmente referenziata, derivante dal rilevamento di uno o più eventi che rappresentano una presunta violazione della privacy.
Analisi post incidente	Insieme di attività finalizzate alla raccolta ed alla analisi delle evidenze utili a stabilire le cause, il contesto e le modalità di attuazione di una violazione della privacy.
Asset Informativo	Insieme definito, individuato e univocamente referenziabile, dei processi, delle informazioni, dei dati, delle infrastrutture tecnologiche hardware e software che costituiscono parte integrante dei trattamenti sottoposti alle norme ed ai regolamenti privacy.
Criticità	Insieme di circostanze avverse, derivanti dalla concomitanza di eventi che costituiscono una minaccia per la sicurezza e la privacy di un determinato contesto.
Dominio di monitoraggio	Insieme definito di asset sottoposti al rilevamento e controllo sistematico degli eventi che si verificano durante il periodo di osservazione.
Evento critico	Qualsiasi evento significativo che, a seguito delle analisi effettuate dal personale incaricato, potrebbe sottintendere, direttamente o indirettamente, una violazione della privacy e/o delle politiche di sicurezza logica, fisica ed organizzativa, applicate al sistema informativo preposto al trattamento di dati personali.
Falso positivo	Evento o insieme di eventi che, pur essendo stati segnalati come manifestazioni di possibili violazioni della privacy, non rivestono carattere di rilevanza nello specifico contesto entro il quale si sono verificati.
Incidente di sicurezza ICT	Qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza ICT fonte di danno per gli asset ICT ovvero per il patrimonio informativo dell'azienda.
Incidente Privacy	Un incidente di sicurezza che comporta violazioni della privacy in grado di arrecare gravi rischi per i diritti e le libertà del/degli Interessato/i.
Monitoraggio degli eventi di sicurezza	Insieme di attività continuative, organizzate, controllate e documentate, finalizzate al tracciamento, al rilevamento ed alla gestione degli eventi di sicurezza, anche con l'ausilio di strumenti automatici.
Minacce	Circostanze o eventi indesiderati, che possono determinare una violazione della sicurezza e della privacy.
Potenziale di aggressività della minaccia	Indicatore valutativo che esprime la pericolosità intrinseca della minaccia, indipendentemente dal contesto in cui questa può verificarsi.

Definizioni	Descrizione
Livello di Gravità di un Data Breach	Misurazione quantitativa e/o qualitativa che esprime la gravità della violazione dei dati personali che comportano gravi rischi per la perdita dei diritti e delle libertà individuali degli Interessati.
Violazione di sicurezza	Azione o insieme di azioni intenzionali o accidentali, intraprese da un agente malevolo, che comportano l'elusione o l'inibizione di una o più misure logiche, fisiche e organizzative, preposte alla tutela della sicurezza e della privacy.
Vulnerabilità	Elemento caratteristico di un determinato asset, che potrebbe essere sfruttato da agenti malevoli per apportare una violazione della sicurezza e della privacy.

Tabella 1– Definizioni

1.4 ACRONIMI

Acronimo	Descrizione
GDPR	General Data Protection Regulation
RAT	Registro delle Attività di Trattamento
DPIA	Data Protection Impact Analysis
DPO/RPD	Data Protection Officer/ Responsabile della Protezione dei Dati

Tabella 2 – Acronimi

CAPITOLO 2
MONITORAGGIO E CLASSIFICAZIONE DEGLI ALLARMI

CAP. 2

I processi di monitoraggio costituiscono la base per una corretta e tempestiva gestione degli incidenti di violazione con impatti sulla privacy, in quanto definiscono i flussi delle attività operative finalizzate al rilevamento di quegli eventi verificatisi entro il perimetro di controllo o *dominio di monitoraggio* che possono configurarsi come fattispecie sottoposta ad obbligo di comunicazione ai sensi dell'art. 33 del GDPR.

2.1 MONITORAGGIO DEGLI EVENTI DI SICUREZZA CON IMPATTI SULLA PRIVACY

I paragrafi successivi descrivono i principi guida per lo svolgimento delle attività operative dedicate al monitoraggio degli eventi che possono sottintendere palesi o presunte violazioni dei dati personali.

Gli indirizzamenti formulati in questo paragrafo s'intendono applicabili a qualsiasi modalità di trattamento di dati personali (automatizzata, semiautomatizzata o non automatizzata) e indipendentemente se in formato digitale o cartaceo.

Gli strumenti normativi previsti dal GDPR che individuano i trattamenti, la loro tipologia, gli asset a supporto e la loro ubicazione, le minacce, i rischi e gli impatti derivanti dalle possibili violazioni della privacy, e quindi necessari alla definizione dei vari domini di monitoraggio sono:

- il Registro dei trattamenti, aggiornato all'ultima versione validata dal Titolare;
- i documenti afferenti alle attività DPIA, svolte sui trattamenti ad elevato rischio per i diritti e le libertà degli interessati;
- i Piani di sicurezza derivanti dalle rispettive DPIA.

Tra gli asset da monitorare, oltre a quelli IT ed organizzativi, vanno ovviamente considerati quelli logistici e fisici ovvero le attività e le funzioni degli uffici che materialmente gestiscono i trattamenti (comparto IT, area del personale, amministrazione, ecc.).

2.1.1 MONITORAGGIO DEGLI EVENTI GENERATI DAI SISTEMI ICT

Il monitoraggio degli eventi ICT è rappresentato dall'insieme delle attività di controllo sistematico, finalizzate al rilevamento degli eventi, tracciati dai sistemi informatici e dalle infrastrutture di sicurezza perimetrale, che assumono carattere di rilevanza ai fini della sicurezza informatica.

Di seguito sono enunciate, a titolo esemplificativo e non esaustivo, alcune tipologie di eventi ICT sottoposte a monitoraggio:

- log generati dalle attività svolte con account riconducibili agli amministratori di sistema, con particolare attenzione a:
  - ✓ orari di connessione/disconnessione (log-on/log-off);
  - ✓ log afferenti alla gestione dei profili utente (es. creazione di nuove utenze, modifica dei privilegi di accesso, blocco di utenze, forzato cambio password, riassegnazione di account ad altro utente);
  - ✓ modifiche alle configurazioni di sistema;
  - ✓ escalation o tentata escalation a profili con privilegi di accesso superiori;
  - ✓ qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
  - ✓ qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dalle attività svolte da utenti ordinari, con particolare attenzione a:
  - ✓ orari di connessione/disconnessione (log-on/log-off);
  - ✓ accessi negati;
  - ✓ escalation o tentata escalation a profili con privilegi di accesso superiori;
  - ✓ qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
  - ✓ qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dai sistemi di sicurezza:
  - ✓ tentativi di violazione delle politiche di firewalling (es. drop/reject);
  - ✓ allarmi generati dai sistemi antivirus;
  - ✓ allarmi generati dai sistemi antispamming;
  - ✓ allarmi generati dai directory server/service.

Tali attività di monitoraggio sono svolte, anche attraverso strumenti automatici, dal personale IT incaricato delle attività di gestione operativa della sicurezza al quale sono assegnati i privilegi di accesso in lettura dei file di tracciamento.

2.1.2 SORVEGLIANZA DEI LOCALI FISICI

I locali preposti al trattamento di dati personali devono essere controllati quotidianamente dal personale preposto alla vigilanza, ove previsto. In ogni caso sia il personale di guardiania o di vigilanza, sia il personale operativo, autorizzato all'accesso ai locali o al trattamento dei dati personali, è tenuto a comunicare tempestivamente qualsiasi evento di presunta o palese violazione della privacy, come ad esempio:

- smarrimento o furto di documenti cartacei contenenti dati personali;
- smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali;
- constatazione di effrazione o tentativi di effrazione alle porte di accesso o alle serrature di chiusura degli armadi che custodiscono dati personali;
- presenza di personale non autorizzato nei locali preposti al trattamento di dati personali;
- distruzione di dati.

CAPITOLO 3
PROCEDURA OPERATIVA
GESTIONE DATA BREACH

Gli eventi rilevati nel corso delle attività di monitoraggio, ovvero quelli segnalati da fonti interne (delegati al trattamento dati, personale aziendale a vario titolo autorizzato al trattamento dati o addetto al controllo degli accessi fisici) o altre fonti (responsabili esterni, fornitori, consulenti o altri soggetti che collaborano a vario titolo con il Titolare), devono essere sottoposti ad analisi, **da parte del personale preposto alla gestione degli incidenti privacy e dai responsabili degli Uffici che li segnalano**, al fine di valutare le origini, la natura, i trattamenti interessati e la dimensione di una presunta violazione.

Queste attività sono funzionali alla generazione di un allarme privacy, laddove con il termine "allarme" si intende l'insieme degli eventi, rilevati su un determinato asset o gruppo omogeneo di asset, aventi la medesima origine o presunta origine, ed i medesimi impatti sulla privacy del/degli Interessato/i.

I criteri di classificazione degli eventi rilevati variano a seconda delle caratteristiche dei *domini di monitoraggio*, così come dettagliato nei paragrafi successivi e nella definizione della ***Metodologia di valutazione della gravità di un Personal Data Breach*** (**allegato 4**).

Ciò premesso, stante il limitato arco temporale a disposizione per gestire e comunicare l'eventuale **Personal Data Breach** (72 ore solari dalla ricezione della segnalazione) è opportuno definire espressamente, oltre a quelli del Titolare e del DPO, **ruoli e responsabilità** nel processo di gestione di un Personal Data Breach:

- **Titolare del Trattamento**: A cui competono le responsabilità decisionali circa la gestione e la compilazione delle risposte e delle eventuali notifiche (al Garante e agli interessati) a seguito del verificarsi di un "*Personal Data Breach"*;
- **DPO aziendale**: A cui competono le responsabilità di supervisionare le attività dei soggetti aventi ruoli e funzioni nella gestione del processo di un "*Personal Data Breach"*; di cooperare col Garante e fungere da punto di contatto con gli interessati; di indirizzare il **Referente Privacy** nella corretta organizzazione della procedura operativa di gestione di un Personal Data Breach;
- **Referente Privacy Aziendale**: il Responsabile dell'Ufficio Privacy che rappresenta il punto di contatto primario aziendale a cui compete la responsabilità di **raccogliere la segnalazione di un qualsivoglia dubbio su una presunta presenza di un incidente privacy** ed avviare**,** organizzare e coordinare le corrette procedure di gestione dell'eventuale "*Personal Data Breach"*;
- **Responsabile Servizi ICT**: il Responsabile dei Servizi Informativi a cui compete la funzione di identificare gli asset informatici minacciati (base dati, sistemi hardware, sistemi software, sistemi di protezione informatica, servizi in cloud, etc.) che sono a supporto dei trattamenti dei dati personali, la cui sicurezza potrebbe essere compromessa dagli eventi rilevati, nonché la responsabilità di collaborare, per gli eventi di natura informatica, strettamente con il Referente Privacy nell'intera gestione del processo di Data Breach;
- **Referente della Segnalazione**: I Responsabili/ Delegati dei singoli Uffici che, direttamente o indirettamente attraverso i soggetti autorizzati al trattamento dati, rilevano l'eventuale incidente privacy; a loro compete la responsabilità di comunicarlo prontamente al **Referente Privacy e,** nel caso di segnalazione relativa ad un incidente informatico **al Responsabile dei Servizi ICT,** e supportarli nella identificazione e nella valutazione del "*Personal Data Breach"* e di collaborare col DPO se necessario.

Alla luce di quanto definito, tutti gli Uffici riceventi le segnalazioni, in caso di qualsivoglia dubbio su una presunta presenza di un Personal Data Breach, sono tenuti a confrontarsi prontamente (non oltre 2 ore dalla scoperta) con Referente Privacy aziendale, col Responsabile dei Servizi ICT (nel caso di presunto incidente informatico) e/o con il DPO.

Ogni violazione dei dati personali occorsa deve essere gestita in linea con quanto previsto nelle fasi descritte e rappresentate di seguito:

A. **Segnalazione** – Fase di identificazione di un potenziale "*Personal Data Breach"* e di tempestiva segnalazione al Titolare, ovvero al Referente Privacy aziendale, al Responsabile Servizi ICT e/o al DPO;
B. **Identificazione** – Fase in cui la segnalazione ricevuta viene identificata come un *"Personal Data Breach"* o come altro incidente di sicurezza che, seppure possa apparire come una presunta violazione della sicurezza, a seguito di ulteriori approfondimenti risulta ordinario o tollerabile (**falso positivo**). In ogni caso, in tale fase viene predisposto il ***"Personal Data Breach Report"*** (**allegato 1**); se si tratta di *"Personal Data Breach"*, vengono effettuate tutte le successive fasi del processo di gestione delle violazioni privacy, mentre nel caso di falso positivo si procede direttamente alla fase di Revisione Post Incidente con conseguente annotazione nel ***"Registro degli Eventi e Violazioni Privacy"*** (**allegato 3**);
C. **Valutazione** – Fase di valutazione e stima della gravità del *"Personal Data Breach"* sulla base delle informazioni raccolte nella precedente fase di identificazione e riportate nel "*Personal Data Breach Report"*, con riferimento ai diritti e libertà delle persone fisiche coinvolte;
D. **Gestione e Risposta** – In base al livello di gravità del *"Personal Data Breach"*, si dovrà comunicare la violazione all'Autorità Garante e/o agli interessati; inoltre, in tale fase viene definito il Piano di Rimedio al fine di porre rimedio alla violazione per attenuarne i possibili effetti negativi;
E. **Revisione Post Incidente (Post Incident Review)** – Fase conclusiva della gestione del *"Personal Data Breach"* e di analisi ex post della violazione al fine di comprendere le root causes, le lesson learned e le opportunità di miglioramento.

3.1 SEGNALAZIONE

In qualsiasi momento i dipendenti che rilevino un potenziale *"Personal Data Breach"*, devono darne tempestiva comunicazione (annotando una breve descrizione dell'evento, data e luogo ed eventuali soggetti interessati) al responsabile dell'Ufficio a cui appartengono, che altrettanto tempestivamente la comunicherà al Referente Privacy alla mail: s.sellitto@interportocampano.it e, nel caso di presunto incidente informatico, al Responsabile dei Servizi ICT alla mail: a.luongo@interportocampano.it; in maniera altrettanto tempestiva, il Referente Privacy informerà il Titolare ed il DPO agli indirizzi mail: info@interportocampano.it e privacy@interportocampano.it.
Nel caso di segnalazioni provenienti da terze parti esterne, come già definite, che dovessero erroneamente essere ricevute attraverso uno dei seguenti canali:

- posta ordinaria (es. presso la sede legale del Titolare);
- fax;
- indirizzo e-mail non di competenza o differente da quello del DPO;

queste vanno ricondotte immediatamente negli appropriati canali procedurali.

A titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazione, risultanti dalle suddette attività di monitoraggio, che potrebbero tradursi in *"Personal Data Breach"* qualora dovessero coinvolgere i dati personali degli interessati:

- **Distruzione di dati informatici o documenti cartacei** intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi, conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato) o fisica (es. rottura di dispositivi di

memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti);

- **Perdita di dati, conseguente a smarrimento/furto di supporti** informatici (es. tablet, computer portatili, HD, memory card) o cartacei (faldoni, contratti, altri documenti cartacei in originale o in copia);
- **Accesso non autorizzato o intrusione a sistemi informatici**, ad esempio in caso di sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione o di compromissione o rilevazione abusiva di credenziali di autenticazione (es. user id e password) per l'accesso ai sistemi;
- **Modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o intervento umano;
- **Rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di documenti di valore contrattuale a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici.

3.2 IDENTIFICAZIONE

Dopo aver raccolto tutte le informazioni necessarie e disponibili, il Referente Privacy e il Responsabile dei Servizi ICT, con il supporto del Responsabile/Delegato dell'Ufficio che ha rilevato l'incidente privacy e quello consulenziale del DPO, valutano la segnalazione ricevuta e:

- se ritengono che non si tratti di un *"Personal Data Breach"* (c.d. **falso positivo)** ma**:**
  - ✓ di un diverso incidente di natura informatica: concordano che il Responsabile dei Servizi ICT provvederà a gestire la segnalazione come un incidente di sicurezza, fatte salve ulteriori valutazioni dello stesso che lo portino a considerare la segnalazione come violazione dei dati personali e quindi a dover procedere con le successive fasi di gestione del processo del Personal Data Breach. Nel caso invece venga confermato che si tratta di Falso Positivo, non si attiveranno le ulteriori fasi di gestione del processo e il Referente Privacy provvederà ad aggiornare comunque il ***"Registro Eventi e Violazioni Privacy"*** (**allegato 3**) con la corrispondente classificazione dell'evento;
  - ✓ di un incidente non informatico fuori ambito privacy che coinvolge dati di tipo non personale (es. dati confidenziali, informazioni riservate aziendali, informazioni rilevanti per gli investitori): procederà in autonomia ad applicare, di volta in volta in base al caso di specie, le procedure aziendali previste per la gestione e risoluzione della particolare tipologia di incidente.
- se ritengono che si tratti di un *"Personal Data Breach"*, il Referente Privacy e il Responsabile dei Servizi ICT, se si tratta di incidente informatico, consultando il Responsabile/ Delegato dell'Ufficio coinvolto dalla violazione:
  - ✓ procedono con la fase successiva di *Valutazione* consultandosi, ove necessario, con il DPO*;*
  - ✓ raccolgono tutte le ulteriori informazioni necessarie al completamento delle fasi successive e compilano il "*Personal Data Breach Report"* (allegato 1) da sottoporre al DPO.

3.3 VALUTAZIONE

All'esito delle informazioni raccolte nelle fasi precedenti e riportate nel "*Personal Data Breach Report"*, il Referente Privacy, sempre con il contributo del Responsabile dei Servizi ICT e del responsabile dell'Ufficio presso il quale sono stati rilevati gli eventi e con il supporto del DPO, valuta la "*magnitudo*" del *"Personal Data Breach"* mediante la "***Metodologia di valutazione della gravità di un Personal Data Breach***" (**allegato 4**), stimando il potenziale rischio per i diritti e le libertà delle persone fisiche.

Inoltre, in tale fase, a seguito della valutazione della gravità del *"Personal Data Breach"*, si identificano le eventuali azioni di rimedio da porre in essere, organizzative e tecniche (Piano di Rimedio/Remediation Plan); queste ultime dovranno essere preventivamente sottoposte al Responsabile dei Servizi ICT nel rispetto delle idonee procedure di Verifica e Validazione.

3.3.1 CLASSIFICAZIONE E VALUTAZIONE DEGLI EVENTI RILEVATI

Le attività di classificazione e la valutazione degli eventi rilevati, nell'ambito dei domini di monitoraggio, sono svolte secondo i seguenti passi operativi:

1. Analisi degli eventi e valutazione degli impatti privacy;
2. Valutazione della gravità della violazione e criticità del trattamento.

3.3.1.1 CLASSIFICAZIONE E VALUTAZIONE DEGLI EVENTI RILEVATI SUI SISTEMI ICT

Le attività di classificazione e la valutazione di tale tipologia di eventi sono svolte dagli operatori di sicurezza ICT. Queste attività consistono nel circoscrivere il perimetro di analisi attraverso l'individuazione degli asset informativi minacciati e che sono a supporto delle attività di trattamento dei dati personali la cui riservatezza, integrità e disponibilità potrebbe essere compromessa dall'evento rilevato.

La correlazione tra eventi rilevati e asset minacciati deve essere svolta dal personale tecnico, incaricato della gestione degli incidenti privacy in ambito ICT (operatori di sicurezza ICT), sotto la stretta supervisione del Responsabile dei Servizi ICT.

3.3.1.2 CLASSIFICAZIONE E VALUTAZIONE DEGLI EVENTI RILEVATI SULLE INFRASTRUTTURE DI SICUREZZA FISICA

Il rilevamento di uno o più eventi del tipo in oggetto deve essere comunicato **entro 2 ore dalla constatazione dell'evento**. Tale comunicazione, anche solo in forma verbale, va effettuata al responsabile/delegato dell'Ufficio presso il quale sono stati rilevati gli eventi, che provvederà a sua volta ad informare il Referente privacy aziendale, nei tempi suddetti.

3.3.1.2.1 EVENTI RILEVATI ATTRAVERSO I SERVIZI DI VIGILANZA

Rientrano in questa categoria gli eventi rilevati dal personale preposto alla vigilanza attiva dei locali fisici, svolti anche con l'ausilio di dispositivi di videosorveglianza.

Ferme restando le procedure operative e i livelli di servizio prestabiliti per queste tipologie di servizi, devono essere riportati al Referente privacy, a titolo esemplificativo, i seguenti eventi:

- Constatazioni di effrazioni rilevate sui punti di accesso a locali all'interno dei quali sono trattati dati personali;

- Constatazione di furto di documenti cartacei;
- Constatazione di furto di strumenti o dispositivi informatici che custodiscono dati personali.

3.3.1.2.2 EVENTI RILEVATI DAL PERSONALE OPERATIVO

Rientrano in questa categoria gli eventi rilevati dal personale interno che a vario titolo, è autorizzato ad accedere ai locali presso i quali si svolgono trattamenti di dati personali.
Ferme restando le procedure in essere per la segnalazione di furti o smarrimenti di beni o documenti aziendali, devono essere riportati al Referente privacy, a titolo esemplificativo, i seguenti eventi, occasionalmente rilevati nel corso dello svolgimento delle normali attività lavorative:

- Constatazione di furto di documenti cartacei contenenti dati personali;
- Smarrimento di documenti cartacei o di supporti rimuovibili contenenti dati personali;
- Constatazione di furto di strumenti o dispositivi informatici che custodiscono dati personali.

3.3.2 VALUTAZIONE DELLA GRAVITÀ DI UNA VIOLAZIONE DI DATI PERSONALI E CRITICITÀ DI TRATTAMENTO

La valutazione della criticità del trattamento è l'insieme delle attività analitiche finalizzate alla valutazione della criticità del contesto entro il quale sono stati rilevati eventi riconducibili a violazioni della sicurezza.

Per la valutazione della criticità del trattamento si può fare riferimento anche alle DPIA, che forniscono razionali di criticità ponderati sul rischio effettivo, derivante dalla violazione della privacy. Qualora nel registro dei trattamenti non sia prevista la DPIA, se ne deduce che la criticità del trattamento può essere considerata BASSA. Qualora, sebbene indicato nel registro dei trattamenti, non sia stata ancora effettuata una DPIA, il Titolare del trattamento si assumerà la responsabilità di dare indicazioni in merito al valore di criticità del trattamento da attribuire, da scegliersi preferibilmente tra ALTA e MEDIA.

Per quanto concerne invece la valutazione del **livello di gravità del Personal Data Breach** si fa riferimento a quanto riportato nell'**allegato 4** circa la "***Metodologia di valutazione della gravità di un Personal Data Breach***" che in ogni caso potrà essere:

Livello	Descrizione
Basso	È **improbabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, che potrebbero solamente subire degli inconvenienti minori facilmente risolvibili (necessità di inserire nuovamente i propri dati personali, disagi minori, irritazione, etc.).
Medio	È **probabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare taluni disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, discriminazione lieve, stress, etc.).
Alto	È **probabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento delle condizioni di salute, etc.).
Molto Alto	È **probabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare conseguenze significative, o addirittura irreversibili, che difficilmente riusciranno a superare (difficoltà finanziarie, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, gravi lesioni o morte, etc.).

TABELLA 3 – LIVELLO DI GRAVITÀ

Nel caso in cui siano presenti trattamenti con diversi livelli di criticità, il giudizio di sensibilità deve essere ricondotto al solo punteggio massimo ottenuto.

3.4 GESTIONE E RISPOSTA

L'organizzazione della risposta ad un *"Personal Data Breach"*, ovvero l'eventuale espletamento delle operazioni di notifica, oltre che derivante dalle analisi e dalle valutazioni precedenti, richiede, sotto la diretta responsabilità del Titolare del trattamento che può avvalersi del supporto del Data Protection Officer (DPO), una **complementare e conclusiva** classificazione dell'incidente di sicurezza per:

1. Esaminare la correttezza dei parametri e dei giudizi valutativi che hanno condotto alla apertura del "*Personal Data Breach Report"* e al conseguente avvio della gestione del processo di "*Personal Data Breach"*;
2. Esaminare l'esaustività della documentazione prodotta a corredo del suddetto processo, al fine di produrre i razionali richiesti per una eventuale notifica al Garante e, nei casi ritenuti opportuni, al/agli Interessato/i;
3. Definire una classe di rilevanza dell'incidente privacy al fine di facilitare il processo decisionale in base al quale sono disposti gli obblighi di notifica, ovvero incidenti di:
   - Classe A: Incidenti di sicurezza che comportano gravi lesioni delle libertà individuali;
   - Classe B: Incidenti di sicurezza che possono precludere la qualità del servizio erogato senza tuttavia comportare gravi lesioni delle libertà individuali dell'Interessato.

La tabella successiva fornisce, a titolo esemplificativo ma non esaustivo, alcune tipologie di incidente afferenti all'una o all'altra categoria.

ESEMPIO DI TIPOLOGIE DI INCIDENTE		
Esempio di incidente	Categoria	Conseguenze per l'Interessato
Temporanea indisponibilità degli archivi informatici	B	Parziale disservizio nell'esercizio dei propri diritti
Disallineamento negli aggiornamenti o violazioni reversibili dell'integrità referenziale dei data base	B	Parziale disservizio nell'esercizio dei propri diritti
Cancellazione/modifica di dati personali sottoposti a backup da parte di operatori autorizzati	B	Parziale disservizio nell'esercizio dei propri diritti
Accesso non autorizzato ai trattamenti o ai dati personali ordinari	B	Lieve perdita delle libertà individuali
Perdita irreversibile di dati personali	A	Impossibilità parziale o totale di esercitare i propri diritti
Accesso non autorizzato ai trattamenti o ai dati personali particolari	A	Grave perdita delle libertà individuali
Trattamenti su dati particolari che perseguono finalità diverse da quelle esplicitamente autorizzate	A	

L'identificazione dell'incidente privacy in una delle classi suddette, unitamente alla valutazione del "***livello della gravità del Personal Data Breach***" corrispondente, consente al Referente Privacy, con l'avallo del Titolare, di procedere alla predisposizione ed organizzazione della:

- notifica al Garante Privacy;
- comunicazione agli interessati coinvolti;

che quest'ultimo dovrà effettuare secondo le regole sintetizzate in tabella (*l'opzione SI/NO indica la discrezionalità della valutazione del Titolare, data la tipologia di violazione e la gravità della stessa*):

LIVELLO DI RISCHIO	Ove possibile entro le 72 ore	Senza ingiustificato ritardo	Ove possibile entro le 72 ore	Senza ingiustificato ritardo
	INCIDENTI DI CLASSE A		INCIDENTI DI CLASSE B	
	Notifica al garante	*Comunicazione all'interessato*	*Notifica al garante*	*Comunicazione all'interessato*
Rischio alto / molto alto	SI	SI	SI	NO
Rischio medio	SI	NO	SI/NO	NO
Rischio basso	SI/NO	NO	SI/NO	NO

TABELLA 4 – NOTIFICA AL GARANTE/COMUNICAZIONE ALL'INTERESSATO

3.4.1 NOTIFICA AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A norma dell'articolo 33 GDPR è prevista la notifica della violazione all'Autorità Garante senza ingiustificato ritardo, entro 72 ore dal momento in cui il Titolare del trattamento ne sia venuto a conoscenza, a meno che la natura dell'incidente renda oggettivamente impossibile o irragionevole tale tempistica o sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora e nella misura in cui **non sia possibile fornire le informazioni contestualmente**, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La notifica, ove necessita, è curata dal Referente Privacy e dal DPO, e trasmessa dal Titolare attraverso la procedura resa disponibile dal Garante Privacy sul suo sito web.

Al fine di garantire uniformità delle notifiche/comunicazioni dirette rispettivamente all'autorità di controllo e all'interessato/i, il legislatore europeo ha indicato le informazioni minimali che le stesse devono contenere, così come di seguito indicato:

CONTENUTO NOTIFICA DIRETTA ALL'AUTORITÀ DI CONTROLLO	CONTENUTO COMUNICAZIONE ALL'INTERESSATO
Natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione.	**Descrizione** con linguaggio semplice e chiaro circa la **natura della violazione** dei dati personali.
Nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni.	**Nome e dati di contatto del DPO** o di altro punto di contatto presso cui ottenere più informazioni.
Probabili conseguenze della violazione dei dati personali.	**Probabili conseguenze della violazione** dei dati personali.
Descrizione delle **misure adottate o di cui si propone l'adozione** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.	Descrizione delle **misure adottate o di cui si propone l'adozione** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3.4.2 COMUNICAZIONE AGLI INTERESSATI

Qualora la valutazione della *magnitudo* del *"Personal Data Breach"* presenti un rischio alto/molto alto per i diritti e le libertà delle persone fisiche, il Titolare, coadiuvato dal Referente Privacy, e con il supporto del DPO, dovrà valutare se ricorre uno dei seguenti casi, ai sensi dell'art. 34, par.5 del GDPR:

1) se sono state adottate preventivamente delle misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
2) se sono state adottate misure successive alla violazione che garantiscano la riduzione del rischio ad un livello considerato come medio/basso per i diritti e le libertà degli interessati;
3) se la comunicazione all'interessato comporta sforzi sproporzionati.

Nei casi 1) e 2) non dovrà essere effettuata alcuna comunicazione agli interessati.

Nel caso 3) si dovrà valutare una modalità consona per darne comunicazione pubblica in modo tale che gli interessati vengano informati in modo efficace.

Nel caso in cui non siano soddisfatte le precedenti condizioni, il Referente Privacy dovrà darne comunicazione agli interessati, secondo lo schema "*Modulo di Notifica Agli Interessati*" (**allegato 2**), senza ingiustificato ritardo tramite e-mail e/o lettera raccomandata.

3.4.3 PIANO DI RIMEDIO (REMEDIATION PLAN)

Il Referente Privacy, con l'ausilio del Responsabile dei Servizi ICT, cura l'implementazione del piano di rimedio, sottoposto a validazione del Titolare, che ne monitora periodicamente l'attuazione.

3.5 REVISIONE POST INCIDENTE (POST INCIDENT REVIEW)

La fase di Revisione Post Incidente è la fase conclusiva di integrazione, da parte del Referente Privacy, del processo di gestione del *"Personal Data Breach"* e di analisi *ex post* della violazione, al fine di comprendere le root causes, le lesson learned e le opportunità di miglioramento.

Il Referente Privacy provvederà ad annotare le informazioni relative all'evento di violazione, raccolte nel *"Personal Data Breach Report"*, all'interno del **"*Registro degli Eventi e Violazioni Privacy*"** (**allegato 3**) che consentirà al Titolare di documentare "qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio." (art. 35, par. 5 GDPR).

Tale Registro consentirà all'Autorità Garante di verificare, in caso di ispezione o richiesta di specifica, il rispetto degli adempimenti in capo al Titolare nella gestione delle violazioni dei dati personali.

CAPITOLO 4
ALLEGATI

CAP. 4

4.1 DOCUMENTAZIONE ALLEGATA

Allegato n. 1: Personal Data Breach Report
Allegato n. 2: Modulo di Notifica agli Interessati
Allegato n. 3: Registro Eventi e Violazioni Privacy

Allegato n. 4: Metodologia di valutazione della gravità di un Personal Data Breach