Sede Legale – Torre del Greco
Via Marconi 66,
www.aslnapoli3sud.it

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI PERSONALI (DATA BREACH)

Autori: Dott.ssa Alessia Cifaldi — **UOS Privacy**
Dott. Giuseppe Napolitano

Approvato da: Avv. Stefano Rotondo — **DPO**

Accettato da: Dott. Giuseppe Russo — **Direttore Generale ASL Napoli 3 Sud**

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1	2025	Prima versione	UOS Privacy
L'ultima revisione sostituisce qualsiasi revisione precedente.			

ASL NAPOLI 3 SUD

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI PERSONALI (DATA BREACH)

Sommario

CAPITOLO 1

GENERALITÀ

CAP. 1

Il presente documento descrive il processo adottato dall' ASL Napoli 3 Sud 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*, 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 la distruzione di dati personali;

• "**Violazione di integrità**": in caso di alterazione non autorizzata o accidentale dei dati personali.

A norma dell'articolo 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 alle Unità Operative aziendali che trattano dati personali a qualsiasi titolo e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea).

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, applicabili al Servizio Sanitario Nazionale, con particolare riferimento al documento WP250 *"Guidelines on Personal data breach notification under Regulation 2016/679"*

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) dell'ASL Napoli 3 Sud. Come previsto dall'art. 39 del GDPR il "**supporto**" fornito dal DPO per la realizzazione della seguente procedura, è sempre di tipo prettamente consulenziale. Infatti, lo stesso non può in alcun caso sostituirsi al Titolare del trattamento nelle valutazioni e nelle decisioni che competono a quest'ultimo, in base a quanto previsto dalla normativa vigente.

1.3 DOCUMENTI DI RIFERIMENTO

[1] Regolamento (UE) 679/2016 (GDPR);
[2] Garante Privacy: Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013;
[3] Garante Privacy: Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
[4] Garante Privacy: Linee guida in materia di Dossier sanitario - 4 giugno 2015;
[5] Garante Privacy: Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015;
[6] D. Lgs 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.
[7] WP29 Gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE (dal 25 Maggio prende il nome di EDPB – European Data Protection Board)
[8] WP250 Guidelines on Personal data breach notification under Regulation 2016/679

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'Organizzazione.
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.
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

CAP. 2

MONITORAGGIO E CLASSIFICAZIONE DEGLI ALLARMI

I processi di monitoraggio costituiscono la base per una corretta e tempestiva gestione degli incidenti di sicurezza 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[1].

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.

Le procedure formulate in questo paragrafo s'intendono applicabili a qualsiasi modalità di trattamento di dati personali (automatizzata, semiautomatizzata o non automatizzata) sia in formato digitale che cartaceo.

Gli strumenti previsti dal GDPR che consentono di definire i domini di monitoraggio (relativi ai trattamenti dati in essere, la loro tipologia, gli asset, le minacce, i rischi e gli impatti derivanti dalle possibili violazioni della privacy) 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 fisici ovvero le attività e le funzioni delle Unità Operative che materialmente gestiscono i trattamenti (comparto IT, area del personale, amministrazione, reparti e UO mediche 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, con particolare riferimento agli eventuali archivi cartacei contenenti le informazioni sanitarie degli assistiti, 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 portatili, contenenti di 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

CAP. 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 delle strutture operative 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 dove con il termine "allarme", s'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 degli Interessati.

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 **ruoli e responsabilità dei soggetti coinvolti** nel processo di gestione dell'evento.

- **Al Titolare del Trattamento** compete la responsabilità decisionale 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"*.
- **Al DPO aziendale** compete la responsabilità di:
  - supervisionare le attività dei soggetti aventi ruoli e funzioni nella gestione del processo di un "*Personal Data Breach"*;

  - cooperare col Garante e fungere da punto di contatto con gli interessati;

  - supportare **la UOS Privacy** nella corretta organizzazione della procedura operativa di gestione di un Personal Data Breach.

- **Alla UOS Privacy,** che rappresenta il referente primario del Titolare, nonché punto di contatto per le Articolazioni aziendali, compete la responsabilità di **raccogliere le segnalazioni in ordine a possibili incidenti privacy** ed avviare**,** organizzare e coordinare le corrette procedure di gestione dell'eventuale "*Personal Data Breach"*, con il supporto del DPO Aziendale.
- **Alla UOC Sistemi Informatici** compete l'identificazione degli asset informatici minacciati (database, 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. Altresì, è tenuta a collaborare, per gli eventi di natura informatica, con la UOS Privacy nell'intera gestione del processo di Data Breach.
- **I soggetti segnalanti** sono individuati nei Responsabili delle Unità Operative che, direttamente o indirettamente, attraverso i soggetti autorizzati al trattamento dati afferenti alla loro struttura, rilevano l'eventuale incidente privacy. In tal caso, sono tenuti a comunicarlo prontamente alla **UOS Privacy e,** laddove si tratti di un incidente informatico, anche **alla UOC Sistemi Informatici,** fornendo adeguato supporto ai fini dell'identificazione e della valutazione del "*Personal Data Breach"*.

Alla luce di quanto definito, i Soggetti segnalanti, laddove ravvisino gli estremi di un potenziale Personal Data Breach, sono tenuti a confrontarsi prontamente (non oltre 2 ore dall'avvenuta presa di conoscenza dell'evento) con la UOS Privacy, con la UOC Sistemi Informatici (nel caso di presunto incidente informatico) e/o con il DPO.

Ogni violazione dei dati personali deve essere gestita in linea con quanto previsto nelle fasi descritte di seguito e rappresentate nel *"Flow Chart"* di cui all'**allegato 1**:

A. **Segnalazione** – Fase di identificazione di un potenziale "*Personal Data Breach"* e di tempestiva segnalazione al Titolare, e contestualmente, alla **UOS Privacy**, alla **UOC Sistemi Informatici** (in caso di incidente di sicurezza di tipo informatico) 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 un **falso positivo**. In ogni caso viene predisposto il ***"Personal Data Breach Report" (allegato 2)***. 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"***;
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 citato "*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 Remediation Plan al fine di attenuare i possibili effetti negativi dell'evento occorso ed evitare il ripresentarsi di eventi analoghi.
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 della Unità Operativa a cui appartengono che, altrettanto tempestivamente, la comunicherà alla UOS Privacy alla mail: uosprivacy@aslnapoli3sud.it e, in caso di presunto incidente informatico, anche agli indirizzi di posta della UOC Sistemi Informatici. In maniera altrettanto tempestiva, la UOS Privacy informerà il Titolare ed il DPO ai rispettivi indirizzi: affari.ist@aslnapoli3sud.it (PEC: affari.ist@pec.aslnapoli3sud.it) e dpo@aslnapoli3sud.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 dell'Azienda);
- 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 quali, ad esempio, tablet, computer portatili di dotazione aziendale, computer desktop aziendali etc. o cartacei quali i documenti contenuti in archivi,faldoni o cartelle, siano essi in originale o in copia;
- **Accesso non autorizzato o intrusione a sistemi informatici**, tramite l'utilizzo di credenziali di autenticazione acquisite indebitamente o accessi illeciti per il tramite di attacchi informatici, compiuti dall'esterno o dall'interno dell'infrastruttura informatica aziendale;
- **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 al rilascio di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di documenti di qualsiasi tipo a soggetti diversi dall'effettivo destinatario, o errata gestione di supporti informatici.

3.2 IDENTIFICAZIONE

Dopo aver raccolto tutte le informazioni necessarie e disponibili, la UOS Privacy e, in caso di potenziale incidente informatico, la UOC Sistemi Informatici, con il supporto del Responsabile della Unità Operativa che ha rilevato l'incidente privacy e quello consulenziale del DPO, esaminano la segnalazione ricevuta e:

- Nel caso in cui non ricorrano gli estremi di un *"Personal Data Breach"* (c.d. **falso positivo)** si procederà come di seguito indicato**:**
  - ✓ se si verifica l'ipotesi di un diverso incidente di natura informatica, sarà cura della UOC Sistemi Informatici gestire la segnalazione come un incidente di sicurezza, fatte salve ulteriori valutazioni che 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 in cui, invece, si configuri il cd. **Falso Positivo**, non si attiveranno le ulteriori fasi di gestione del processo. La UOS Privacy provvederà ad aggiornare, in ogni caso, il ***"Registro Eventi e Violazioni Privacy"*** con la corrispondente classificazione dell'evento.
- se si configura, invece, un *"Personal Data Breach"*, la UOS Privacy, unitamente alla UOC Sistemi Informatici, laddove si tratti di incidente informatico, sentito il Responsabile dell'Unità Operativa coinvolta dalla violazione:
  - ✓ procederà alla fase successiva di *Valutazione* consultandosi, ove necessario, con il DPO;
  - ✓ raccoglierà tutte le ulteriori informazioni necessarie al completamento delle fasi successive compilando il "*Personal Data Breach Report"* da sottoporre al DPO.

3.3 VALUTAZIONE

All'esito delle informazioni raccolte nelle fasi precedenti e riportate nel "*Personal Data Breach Report"*, la UOS Privacy, con il contributo della UOC Sistemi Informatici e del responsabile dell'Unità Operativa presso la quale sono stati rilevati gli eventi, nonché 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)*** ed effettua una valutazione in merito al 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 sia organizzative che tecniche (Piano di Rimedio/Remediation Plan), da porre in essere, preventivamente condivise con la UOC Sistemi Informatici 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 dai dipendenti della UOC Sistemi Informatici, addetti alle attività di sicurezza informatica. 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 delle informazioni personali la cui riservatezza, integrità e disponibilità potrebbe essere compromessa dall'evento/i rilevato/i.

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 Direttore della UOC Sistemi Informatici.

3.3.1.2 CLASSIFICAZIONE E VALUTAZIONI 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 dell'Unità Operativa presso la quale sono stati rilevati gli eventi, che provvederà a sua volta ad informare la UOS Privacy, 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, a titolo esemplificativo, alla UOS Privacy i seguenti eventi:

- Constatazioni di avvenuta effrazione di 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 o esterno all' Azienda 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 alla UOS Privacy, a titolo esemplificativo, i seguenti eventi, 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 particolari;
- 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 a individuare la criticità del contesto entro il quale sono stati rilevati eventi riconducibili a violazioni della sicurezza.

Per la valutazione delle criticità del trattamento si può fare riferimento anche alle DPIA, che forniscono indici 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

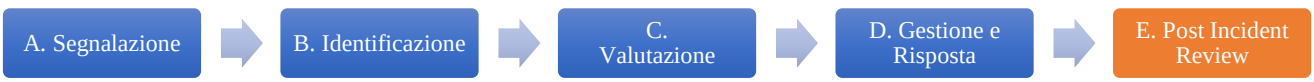
L' organizzazione della risposta ad un *"Personal Data Breach"*, ovvero l'eventuale espletamento delle operazioni di notifica, oltre che derivante dalle analisi e dalle valutazioni precedenti, richiede una **complementare e conclusiva** classificazione dell'incidente di sicurezza, che dovrà essere condotta dal Titolare del trattamento. Quest'ultimo, potrà avvalersi del supporto della UOS Privacy, del Data Protection Officer, nonché di consulenti legali e tecnici al fine di:

1. Esaminare la correttezza dei parametri e dei giudizi valutativi attribuiti che hanno condotto alla apertura del "*Personal Data Breach Report"* e, quindi, all'avvio della gestione del processo di "*Personal Data Breach"*;
2. Esaminare l'esaustività della documentazione prodotta a corredo del suddetto processo, al fine di acquisire gli elementi 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 alle summenzionate categorie.

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

3.5 REVISIONE POST INCIDENTE (POST INCIDENT REVIEW)



La fase di Revisione Post Incidente è la fase conclusiva di integrazione 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. Tale attività viene condotta da parte della UOS Privacy con il supporto del DPO Aziendale e con il coinvolgimento della UOC Sistemi Informatici.

La UOS Privacy e la UOC Sistemi Informatici provvederanno ad annotare le informazioni, raccolte nel *"Personal Data Breach Report",* relative all'evento di violazione nel ***"Registro degli Eventi e Violazioni Privacy"*** 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, parag. 5, GDPR)

Tale Registro consentirà all'Autorità Garante di verificare, in caso di ispezione o richiesta 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	**Flow Chart Procedura Operativa Gestione Data Breach**
Allegato n. 2	**Personal Data Breach Report**
Allegato n. 3	**Modulo di Notifica agli Interessati**
Allegato n. 4	**Metodologia di Valutazione della Gravità di un Personal Data Breach**