OGGETTO: REVOCA, AI SENSI DELL'ART. 21 QUINQUIES COMMA 1, DELLA LEGGE N. 241/1990, DELLA DELIBERAZIONE DEL DIRETTORE GENERALE N.532 DEL 13.06.2019 E ADOZIONE DELLA NUOVA PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI PERSONALI (DATA BREACH).

Il Direttore UOC Affari Istituzionali

Alla stregua dell'istruttoria compiuta dal Direttore UOC Affari Istituzionali e dalla Responsabile della UOS Privacy e delle risultanze degli atti tutti richiamati nelle premesse che seguono, costituenti istruttoria a tutti gli effetti di legge, nonché dell'espressa dichiarazione di regolarità tecnica e amministrativa della stessa, resa dallo stesso Dirigente responsabile proponente a mezzo della sottoscrizione della presente;

Dichiarata, espressamente con la sottoscrizione, nella qualità di delegato del Titolare del trattamento anche nella fase di pubblicazione, la conformità del presente atto al Regolamento europeo n. 679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

Dichiarata altresì, allo stato ed in relazione al procedimento di cui al presente atto, l'insussistenza del conflitto di interessi ai sensi dell'art. 6 bis della Legge n. 241/1990, delle disposizioni di cui al vigente Codice di Comportamento Aziendale e delle misure previste dal vigente Piano Triennale della Prevenzione della corruzione e della Trasparenza;

infine, la conformità del presente atto ai princìpi di cui alla legge 6 novembre 2012, n. 190.

PREMESSO:

- che il 24 maggio 2016 entrava in vigore il Regolamento Generale per la Protezione dei Dati personali n. 2016/679 (General Data Protection Regulation o G.D.P.R.);
- che, successivamente, in data 10 agosto 2018 è stato emanato il D.Lgs. 101/2018 avente ad oggetto "Disposizioni per l'adeguamento della normativa nazionale al Regolamento UE 2016/679", con la finalità di adeguare la normativa nazionale ex D.Lgs. 196/2003 (Codice della Privacy) alla nuova normativa comunitaria;
- che, al fine di dare attuazione alle nuove disposizioni normative in materia di protezione dei dati personali, questa Azienda ha adottato il proprio Regolamento, revisionato con Deliberazione del Direttore Generale n. 754 del 16.05.2024;
- che con Deliberazione n. 524 del 29/06/2018 è stato adottato il regolamento per la gestione delle violazioni della sicurezza dai dati personali, successivamente modificato con Deliberazione n. 532 del 13.06.2019;

PRESO ATTO:

- che con Deliberazione del Direttore Generale n. 854 del 20.07.2023 è stato adottato il nuovo Atto Aziendale, approvato con D.G.R.C. n. 470 del 01.08.2023 e attuato con Deliberazioni del Direttore Generale dell'ASL Napoli 3 Sud n. 457 del 22.03.2024 e n. 471 del 25.03.2024;
- che il citato atto ha modificato l'organizzazione aziendale istituendo, all'interno della UOC Affari Istituzionali, la UOS Privacy cui sono stati demandati tutti gli adempimenti in materia di privacy in applicazione del Regolamento UE 2016/679;
- che alla stessa UOS sono state affidate tutte le attività tese a garantire adeguata compliance aziendale nella materia *de qua*;

TENUTO CONTO:
- che tra i principi cardine del G.D.P.R. si annovera la tutela dei soggetti interessati in caso di "Violazione di dati";
- che per violazione di dati si intende la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- che all'articolo 4, comma 12, il Regolamento Europeo 679/2016 (G.D.P.R.) definisce la violazione dei dati personali, ovvero il cosiddetto "Data Breach";
- che agli articoli 33 e 34, il Regolamento Europeo 679/2016 (G.D.P.R.), nei casi di "Violazione dei dati", regolamenta i tempi e le modalità di notifica all'Autorità di Controllo ed all'interessato per i casi più severi;

CONSIDERATO:
- che l'adeguamento al Regolamento UE 2016/679 costituisce una concreta opportunità per migliorare la qualità e la sicurezza dei servizi ICT in Sanità, a tutela sia dei cittadini che utilizzano i servizi sociosanitari, sia dei professionisti che li erogano;
- che negli anni successivi all'entrata in vigore del Regolamento UE 2016/679, l'Autorità Garante per la Protezione dei Dati Personali ha emanato numerosi provvedimenti e linee guida in ordine alla corretta applicazione della normativa;
- che in ossequio a quanto previsto dal G.D.P.R. si rende necessario aggiornare il processo per la gestione delle violazioni di sicurezza, che comportano gravi rischi per la perdita dei diritti e delle libertà individuali degli Interessati, definendone le modalità operative interne;
- che, in tale ottica, si rende doveroso adottare una nuova procedura che consenta all'Azienda di agire prontamente in caso di incidenti di sicurezza al fine di evitare e\o ridurre lesioni dei diritti e delle libertà dei soggetti interessati.

PRESO ATTO del parere favorevole espresso dal DPO Aziendale ai fini dell'adozione della procedura *de qua*, acquisito al protocollo aziendale n. 63864 del 10/03/2025;

RITENUTO necessario, alla luce di quanto sopra evidenziato, procedere alla revoca della Deliberazione n. 532 del 13.06.2019 e, per l'effetto, adottare in conformità a quanto previsto G.D.P.R. 2016/679, la nuova procedura per la gestione delle violazioni di sicurezza dei dati personali (data breach);

PROPONE AL DIRETTORE GENERALE

-**DI REVOCARE** ai sensi dell'art 21 quinquies, comma 1 della Legge n. 241/1990, la Deliberazione del Direttore Generale n.532 del 13.06.2019 avente ad oggetto "*Presa d'atto ed approvazione nuovo regolamento aziendale in materia di "data breach" - Revoca deliberazione n. 524 del 29 giugno 2018 ad oggetto: presa d'atto ed approvazione del regolamento aziendale in materia di "data breach" ai sensi del regolamento generale dell'unione europea n. 679 del 27.4.2016 sulla protezione dei dati".*

- DI ADOTTARE la nuova Procedura per la gestione delle violazioni di sicurezza dei dati personali (data breach) unitamente agli allegati, che ne costituiscono parte integrante e sostanziale;

- DI DARE MANDATO alla UOS Privacy di trasmettere la presente procedura, unitamente agli allegati, a tutte le articolazioni aziendali e darne la massima diffusione mediante la pubblicazione sul sito istituzionale dell'ASL Napoli 3 Sud nell'apposita sezione "Privacy".

Gli estensori

Il Dirigente Amministrativo
Responsabile della UOS Privacy

Dott.ssa Alessia Cifaldi

Il Coll. Amministrativo Prof.
Compliance Officer
Dott. Giuseppe Napolitano

Il Direttore UOC Affari Istituzionali
Dott. Marco Tullo
(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

Il Direttore Generale

In forza della Delibera della Giunta Regionale della Campania n. 321 del 21 Giugno 2022 e con D.P.G.R.C. n. 111 del 4 Agosto 2022

Preso atto della dichiarazione resa dal dirigente proponente con la sottoscrizione, in ordine alla regolarità tecnica ed amministrativa del presente atto, nonché relativa alla conformità dello stesso atto alle disposizioni vigenti in materia di tutela della privacy;

Sentito il parere favorevole espresso dal Direttore Amministrativo e dal Direttore Sanitario

Il Direttore Amministrativo
dr. Michelangelo Chiacchio

Il Direttore Sanitario
dr. Ferdinando Primiano

(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

DELIBERA

-**DI REVOCARE** ai sensi dell'art 21 quinquies, comma 1 della Legge n. 241/1990, la Deliberazione del Direttore Generale n.532 del 13.06.2019 avente ad oggetto *"Presa d'atto ed approvazione nuovo regolamento aziendale in materia di "data breach" - Revoca deliberazione n. 524 del 29 giugno 2018 ad oggetto: presa d'atto ed approvazione del regolamento aziendale in materia di "data breach" ai sensi del regolamento generale dell'unione europea n. 679 del 27.4.2016 sulla protezione dei dati".*

- DI ADOTTARE la nuova Procedura per la gestione delle violazioni di sicurezza dei dati personali (data breach) unitamente agli allegati, che ne costituiscono parte integrante e sostanziale;

- DI DARE MANDATO alla UOS Privacy di trasmettere la presente procedura, unitamente agli allegati, a tutte le articolazioni aziendali e darne la massima diffusione mediante la pubblicazione sul sito istituzionale dell'ASL Napoli 3 Sud nell'apposita sezione "Privacy".

Il Direttore della UOC Affari Istituzionali e la Responsabile della UOS Privacy saranno responsabili, in via esclusiva, dell'esecuzione della presente deliberazione, che viene resa immediatamente esecutiva, data l'urgenza, curandone tutti i consequenziali adempimenti, nonché quelli di pubblicità e di trasparenza previsti dal D.L.gs 14 marzo 2013 n° 33 e s.m.i.

Il Direttore Generale
dott. Giuseppe Russo
(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

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

Autori:	Dott.ssa Alessia Cifaldi Dott. Giuseppe Napolitano	**UOS Privacy**
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 3

1.1 Scopo e ambito di applicazione 3

1.2 Ruolo e supporto del DPO 3

1.3 Documenti di riferimento 4

1.4 Definizioni 4

1.5 Acronimi 5

Capitolo 2 – Monitoraggio e classificazione degli allarmi 5

2.1 Monitoraggio degli eventi di sicurezza con impatti sulla privacy 5

2.1.1 Monitoraggio degli eventi generati dai sistemi ICT 6

2.1.2 Sorveglianza dei locali fisici 6

Capitolo 3 – Procedura operativa gestione data breach 7

3.1 Segnalazione 8

3.2 Identificazione 9

3.3 Valutazione 10

3.3.1 Classificazione e valutazione degli eventi rilevati 10

3.3.1.1 Classificazione e valutazione degli eventi rilevati sui sistemi ICT 10

3.3.1.2 Classificazione e valutazione degli eventi rilevati sulle infrastrutture di sicurezza fisica 11

3.3.1.2.1 Eventi rilevati attraverso i servizi di vigilanza 11

3.3.1.2.2 Eventi rilevati dal personale operativo 11

3.3.2 Valutazione della gravità di una violazione di dati personali e criticità di trattamento 11

3.4 Gestione e risposta 12

3.4.1 Notifica al Garante per la Protezione dei Dati Personali 13

3.4.2 Comunicazione agli interessati 14

3.4.3 Piano di rimedio (Remediation Plan) 14

3.5 Revisione post incidente (Post Incident Review) 15

Capitolo 4 – Allegati 15

4.1 Documenti allegati 15

CAPITOLO 1
GENERALITÀ

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.

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 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.

CAP. 3

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 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 5)***.

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" (allegato 4)***;
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" (allegato 4)*** 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 5)*** 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 5** 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
Trattamenti su dati particolari che perseguono finalità diverse da quelle esplicitamente autorizzate	A	Grave perdita delle libertà individuali

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

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

Il DPO dovrà supportare il Titolare nella predisposizione della notifica e dell'eventuale comunicazione agli interessati, seguendo le regole sintetizzate nella seguente 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 tutte le informazioni contestualmente alla notifica, le stesse possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La notifica, ove necessaria, è curata dalla UOS 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, cosi 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 i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni	**Nome e i 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

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.
Al fine di garantire la corretta comunicazione, il Titolare, coadiuvato dalla UOS Privacy, e con il supporto del DPO, dovrà valutare se ricorre uno dei seguenti casi, di cui all'art. 34, parag.5, GDPR distinguendo tra le seguenti fattispecie:

1. Se sono state adottate preventivamente delle misure di sicurezza tecniche e organizzative adeguate, come ad esempio la cifratura dei dati (atta a rendere gli stessi inaccessibili a terzi) e se predette misure sono state applicate ai dati personali oggetto della violazione;
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.

Nelle ipotesi di cui ai punti 1. e 2. non dovrà essere effettuata alcuna comunicazione agli interessati.

Nell'ipotesi prevista dal punto 3., si dovrà valutare una modalità consona per dare comunicazione pubblica agli interessati al fine di informarli compiutamente. A tal fine, sarà possibile effettuare la comunicazione tramite il sito web istituzionale e\o attraverso informativa all'utenza da collocare nei plessi aziendali etc.

Nel caso in cui la violazione riguardi, invece, un numero esiguo di interessati chiaramente identificabili e sussista ugualmente l'obbligo di notifica, la UOS Privacy dovrà darne comunicazione tramite e-mail e\o lettera raccomandata, impiegando lo schema *"Modulo di Notifica Agli Interessati" (allegato 3)*.

3.4.3 PIANO DI RIMEDIO (REMEDIATION PLAN)

La UOS Privacy, con l'ausilio della UOC Sistemi Informatici, 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 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" (allegato 4)*** 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.

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- protocollo@pec.aslnapoli3sud.it

CAPITOLO 4
ALLEGATI

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	**Registro Eventi e Violazioni Privacy**
Allegato n. 5	**Metodologia di Valutazione della Gravità di un Personal Data Breach**

regione campania aslnapoli3sud

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

VIOLAZIONE DI DATI PERSONALI

MODULO DI COMUNICAZIONE AGLI INTERESSATI

Titolare del trattamento
Denominazione o ragione sociale:
Provincia:
Comune:
Cap:
Indirizzo:
Nome e Cognome persona fisica addetta alla comunicazione:
Funzione rivestita:
Indirizzo PEC e/o EMAIL per eventuali comunicazioni:
Recapito telefonico per eventuali comunicazioni:

DPO
Nome e Cognome DPO:
Riferimenti di contatto del DPO:
Indirizzo PEC e/o EMAIL per eventuali comunicazioni:
Recapito telefonico per eventuali comunicazioni:

Gentile [*Nome dell'interessato*]

Purtroppo, abbiamo riscontrato la seguente violazione dei suoi dati personali in relazione nell'ambito di trattamenti effettuati da ASL Na 3 SUD:

[Descrizione della natura della violazione dei dati personali]

Le possibili conseguenze della violazione dei dati personali sono:

[Descrizione delle possibili conseguenze della violazione dei dati personali]

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

Come previsto dal Regolamento UE 2016/679 abbiamo notificato questa violazione al Garante per la protezione dei dati personali.

Abbiamo individuato le seguenti misure per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi:

[Descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi]

Per ulteriori informazioni si prega di contattare il DPO.

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

it

Azienda Sanitaria Locale Napoli 3 Sud
con sede legale in Torre del greco
via Guglielmo Marconi, 66 - 80059 (NA)
in persona del suo legale rappresentante pro-tempore

All'attenzione del:
DPO
PEC:

VIOLAZIONE DI DATI PERSONALI
MODULO DI SEGNALAZIONE

Oggetto: segnalazione Data Breach

Data e ora della rilevazione dell'evento

Data dell'evento (se differente dalla rilevazione)

Luogo e contesto dell'evento

Nome e dati di contatto della persona che ha effettuato la segnalazione dell'evento (cellulare ed e-mail)

Descrizione dettagliata del contesto dell'evento

Categoria di dati personali coinvolti nell'evento e numero approssimativo di interessati

Descrizione delle eventuali azioni intraprese sin dal momento della rilevazione

Note aggiuntive

regione campania
aslnapoli3sud

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

METODOLOGIA DI VALUTAZIONE DELLA GRAVITA' DI UN PERSONAL 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.			

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

Metodologia di valutazione della gravità di un Personal Data Breach

Di seguito viene riportata la metodologia per la valutazione della gravità delle violazioni dei dati personali adottata. Tale metodologia è stata definita sulla base delle indicazioni fornite **dall'ENISA (European Union Agency for Network and Information Security)** contenute all'interno del documento "Recommendations for a methodology of the assessment of severity of personal *data breach*[1]".

Gli elementi chiave da tenere in considerazione in sede di valutazione della gravità, anche con riferimento al dominio di monitoraggio, risultano essere i seguenti:

- *Contesto dell'elaborazione dati* ovvero la natura dei dati violati valutata nel contesto in cui gli stessi vengono utilizzati (**DPC: Contesto elaborazione dati**)[2]
- *Facilità di identificazione dell'individuo* in base ai dati violati (**EI: Facilità di identificazione**); [3]
- *Circostanze della violazione* (violazione di riservatezza, integrità e disponibilità dei dati), che hanno un'influenza aggiuntiva sulla gravità di una violazione (**CB: Circostanze della violazione**)[4]

La valutazione della gravità della violazione, secondo la metodologia, è articolata nelle seguenti fasi operative:

- **Fase 1: Valutazione del DPC**: in questa fase si definisce il perimetro dei dati personali oggetto della violazione e si classificano gli stessi sulla base dell'appartenenza ad una delle categorie di dati previste dall' ENISA (Dati Ordinari, Dati Comportamentali, Dati Patrimoniali, Dati Particolari). La classificazione comporta l'attribuzione di un punteggio base che può essere aumentato o diminuito in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati;
- **Fase 2: Determinazione della EI**: rappresenta il fattore di correzione del DPC. Infatti la criticità complessiva di una violazione dei dati può essere ridotta in base al valore di EI, ovvero in relazione alla facilità con cui, il soggetto che entra in possesso dei dati oggetto della violazione, può ricondurli o meno all'interessato a cui appartengono;
- **Fase 3: Valutazione delle CB:** in questa fase si valutano gli scenari di violazione (violazione di riservatezza, violazione di integrità, violazione di disponibilità, o eventuali intenzioni

[1] https://www.enisa.europa.eu/publications/dbn-severity

[2] Data Processing Context (DPC): Addresses the type of the breached data, together with a number of factors linked to the overall context of processing (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

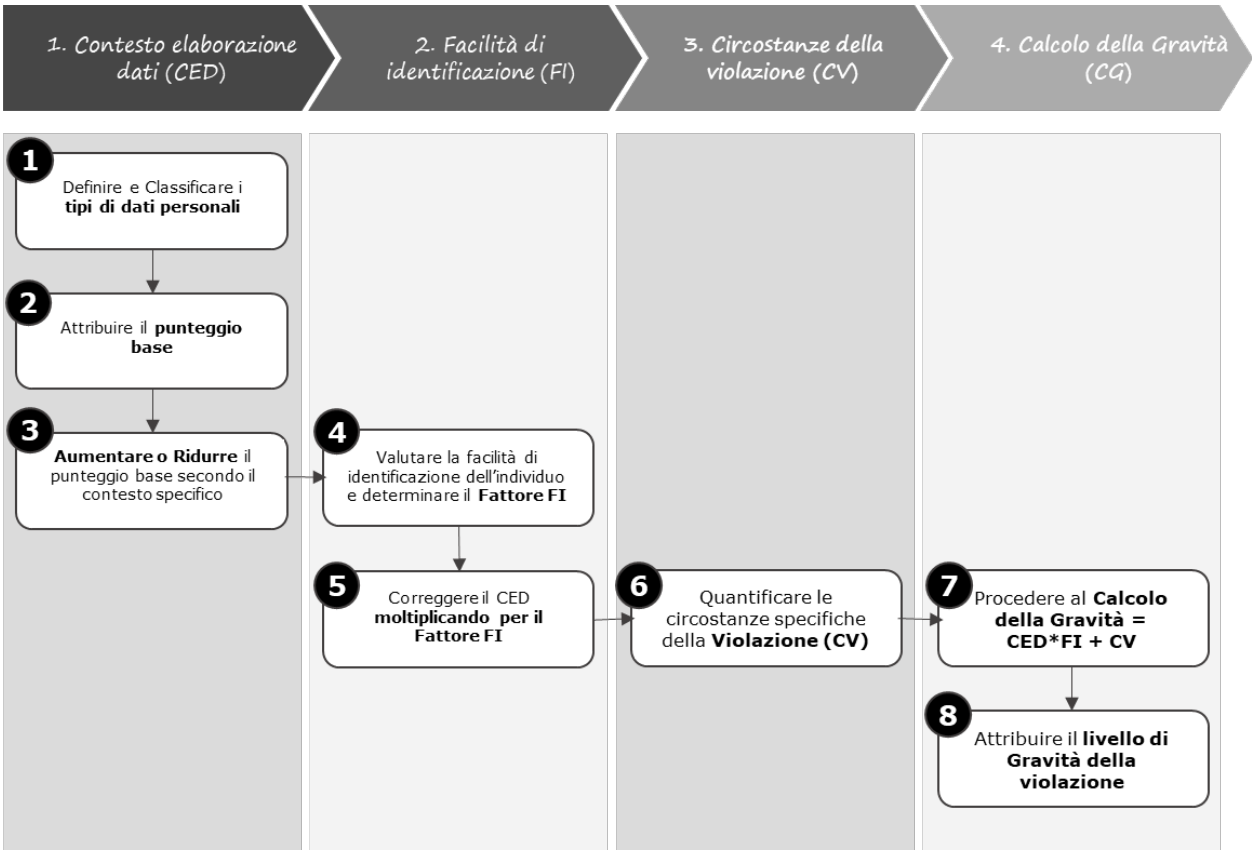
[3] Ease of Identification (EI): Determines how easily the identity of the individuals can be deduced from the data involved in the breach (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

[4] Circumstances of breach (CB): Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security

malevole) interessati o meno in seguito al Personal Data Breach. Pertanto il fattore CB, laddove presente, può solo incrementare la gravità di una specifica violazione;

- **Fase 4: Calcolo della gravità:** si giunge al calcolo della gravità della violazione sulla base dei 3 precedenti elementi DPC, EI, CB.

Viene riportata di seguito una rappresentazione del processo di valutazione della gravità della violazione sotto forma di diagramma di flusso:



Fase 1: Valutazione del contesto dell'elaborazione dei dati DPC

Il punteggio attribuito al DPC è al centro della Metodologia in quanto consente di valutare la criticità e la dimensione della violazione nel contesto di trattamento specifico.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
1- Definire e Classificare i tipi di dati personali	Definire e classificare la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro macro-categorie: • Dati Ordinari; • Dati Comportamentali; • Dati Patrimoniali; • Dati Particolari.	*Procedura Operativa Gestione Data Breach)*
2- Attribuire il punteggio base	Attribuisce il punteggio base secondo la **Tabella 3 - DPC**	*TABELLA 3 – CONTESTO ELABORAZIONE DATI (DPC)*
3- Aumentare o Ridurre il punteggio base secondo il contesto specifico	Aumenta o riduce il punteggio base in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati (ad es. volume di dati, caratteristiche speciali dei Titolari o degli individui, inesattezza dei dati, disponibilità del dato al pubblico prima della violazione, natura del dato). Il punteggio del DPC può variare da 1 a 4.	*TABELLA 3 – CONTESTO ELABORAZIONE DATI (DPC)*

Di seguito si riporta la Tabella da utilizzare **per la valutazione del DPC:**

Contesto Elaborazione Dati (DPC):		Punteggio
Dati Ordinari	**Esempio Dati Ordinari: Nome, Cognome Numero di Telefono, Indirizzo, Email, Fotografia, Data di nascita, Stato di famiglia, Titolo di Studi, Lavoro, Inquadramento lavorativo, etc.**	
	Punteggio Base: quando la violazione riguarda "Dati Ordinari" e non si è a conoscenza di alcun fattore aggravante.	**1**
	Il punteggio DPC potrebbe essere **aumentato di 1**, ad esempio quando il volume di "Dati Ordinari e/o le caratteristiche del Titolare sono tali da ricavare un profilo della persona o possono essere formulate assunzioni sullo stato sociale/finanziario dell'individuo.	**2**
	Il punteggio DPC potrebbe essere **aumentato di 2**, ad esempio quando i "Dati Ordinari" e/o le caratteristiche del Titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	**3**
	Il punteggio DPC potrebbe essere **aumentato di 3**, ad esempio quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche / psicologiche.	**4**

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

Contesto Elaborazione Dati (DPC):		Punteggio
Dati Comportamentali	**Esempio di Dati Comportamentali: Abitudini, preferenze personali e interessi, vita sociale, affidabilità, spostamenti, ubicazione etc.**	
	Punteggio Base: quando la violazione comporta "Dati Comportamentali" e non si è a conoscenza di fattori aggravanti o di diminuzione.	**2**
	Il punteggio DPC potrebbe essere **diminuito di 1**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio DPC può essere **aumentato di 1**, ad esempio quando il volume di "Dati Comportamentali" e / o le caratteristiche del controllore sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	**3**
	Il punteggio DPC può essere **aumentato di 2**, ad esempio se è possibile creare un profilo basato sui dati sensibili di una persona.	**4**
Dati Patrimoniali	**Esempio di Dati Patrimoniali: IBAN, Numero di conto, Saldo conto, Transaction History, Informazione di base sulla carta di credito (senza CVC), Complete informazioni sulla carta di credito (con CSV), Dati sui mutui/prestiti**	
	Punteggio Base: quando la violazione riguarda "Dati Patrimoniali" e non si è a conoscenza di fattori aggravanti o di diminuzione.	**3**
	Il punteggio DPC potrebbe essere **diminuito di 2**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni patrimoniali dell'individuo (ad esempio, il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	**1**
	Il punteggio DPC potrebbe essere **diminuito di 1**, ad esempio quando il set di dati specifici include alcune informazioni patrimoniali ma non fornisce ancora informazioni significative sullo stato / sulla situazione patrimoniale dell'individuo (ad esempio: i numeri di conti bancari semplici senza ulteriori dettagli).	**2**
	Il punteggio DPC potrebbe essere **aumentato di 1**, ad esempio quando a causa della natura e / o del volume dell'insieme di dati specifici, vengono divulgate informazioni complete patrimoniali (ad esempio: informazioni complete sulla carta di credito con il codice CVC)	**4**
Dati Particolari	**Esempio di Dati Particolari: Dati Sanitari, Razza / origine etnica, Orientamento politico e religioso, Orientamenti sessuali, Procedimento penale / condanna, Dati biometrici, Dati genetici**	

Contesto Elaborazione Dati (DPC):		Punteggio
	Punteggio Base: quando la violazione riguarda "Dati Sensibili" e non si è a conoscenza di alcun fattore di diminuzione.	**4**
	Il punteggio DPC potrebbe essere **diminuito di 3**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni sui Dati Sensibili o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio DPC potrebbe essere **diminuito di 2**, ad esempio quando la natura dei dati può portare a ipotesi generali e non specifiche di un individuo.	**2**
	Il punteggio DPC potrebbe essere **diminuito di 1**, ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili di un individuo.	**3**

TABELLA 3 – CONTESTO ELABORAZIONE DATI (DPC)

Se i dati corrispondono a più di una categoria, è necessario seguire i passaggi sopra indicati per ogni categoria applicabile. In questi casi il valore da utilizzare per il calcolo complessivo della gravità **sarà il punteggio massimo raggiunto.**

Fase 2: Determinazione del punteggio per la facilità di identificazione (EI)

Il punteggio del EI è il fattore di correzione del DPC e consente di valutare, secondo la Tabella 4, la facilità di identificazione del soggetto interessato in base ai dati violati.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
4- Valutare la facilità di identificazione del soggetto interessato e determinare il fattore EI	Valuta la **facilità di identificazione** del soggetto interessato ed attribuisce un punteggio secondo la **Tabella 4 - EI** definita dalla Metodologia secondo i seguenti quattro livelli: • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione EI può variare da 0,25 a 1. Il **punteggio più basso** viene attribuito quando la possibilità di identificare il soggetto interessato è trascurabile, il che significa che è estremamente difficile abbinare i dati a una determinata persona, ma comunque potrebbe essere possibile con determinate condizioni. Al contrario, il **punteggio più alto** viene attribuito quando l'identificazione è possibile direttamente dai dati violati, senza alcuna ricerca specifica per determinare l'identità dell'individuo.	*TABELLA 4 – FACILITÀ DI IDENTIFICAZIONE (EI)*
5- Correggere il DPC moltiplicando con il fattore EI	Una volta individuato il fattore di correzione, esso viene moltiplicato per il DPC, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	***DPC * EI***

Di seguito si riporta la Tabella da utilizzare per la **valutazione del criterio (EI):**

Facilità di identificazione (EI)	Punteggio	Livello
La violazione riguarda dati identificativi o dati personali **non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese, indirizzo email che non rileva altre informazioni come il nome dell'individuo e che non è usato come indirizzo email principale nei siti internet, nei forum o per i social networks, immagine non nitida e vaga)**	**0,25**	**Trascurabile**
La violazione riguarda i dati identificativi **di un individuo ma non facilmente identificabile (ad esempio: nome/cognome condiviso da poche persone in un intero paese, immagine non chiara e nitida ma che contiene informazioni aggiuntive come uno specifico luogo)**	**0,5**	**Limitata**
La violazione riguarda dati identificativi e **rivela ulteriori informazioni di identificazione dell'individuazione (ad esempio: nome completo con l'indicazione dell'indirizzo email di questa persona, indirizzo email che non rileva altre informazioni come il nome dell'individuo**	**0,75**	**Significativo**

ma è usato come indirizzo email principale nei siti internet, nei forum o per i social networks, immagina nitida ma che non fornisce informazioni aggiuntive)		
La violazione riguarda dati identificativi o dati personali **direttamente identificativi (ad esempio: nome completo con l'indicazione della data di nascita e l'indirizzo email di questa persona, indirizzo email che rileva il nome dell'individuo e che è usato come indirizzo email principale nei siti internet, nei forum e per i social networks, immagine chiara che rileva ulteriori informazioni sull'appartenenza di un individuo ad uno specifico gruppo o indirizzo di casa)**	**1**	**Massimo**

TABELLA 4 – FACILITÀ DI IDENTIFICAZIONE (EI)

Fase 3: Valutazione delle Circostanze della Violazione (CB)

Il punteggio del CB quantifica le **circostanze specifiche della violazione,** ovvero gli scenari di ambiti di violazione, che possono essere presenti o meno in una particolare situazione.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
6- Quantificare le circostanze specifiche della violazione (CB)	Attribuisce il punteggio relativo **alle circostanze della violazione** classificate secondo le seguenti macro categorie: • violazione di riservatezza; • violazione di disponibilità; • violazione di integrità dei dati; • eventuali intenzioni malevole. Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione. Il punteggio del CB può incrementare il punteggio precedentemente ottenuto delle gravità di 0,25 o 0,5 a seconda dei casi.	*TABELLA 5 – CIRCOSTANZE DELLA VIOLAZIONE (CB)*

Di seguito si riporta la tabella da utilizzare per la **valutazione del terzo indicatore (CB):**

Circostanze della violazione (CB)		Punteggio
Violazione di riservatezza	**Definizione:** La perdita di riservatezza si verifica quando le informazioni **sono accessibili da parti che non sono autorizzate o che non hanno uno scopo legittimo** di accedervi. L'entità della perdita di riservatezza varia a seconda della portata della divulgazione, ovvero il numero potenziale e il tipo di parti che possono avere accesso illecito all'informazione.	

Circostanze della violazione (CB)		Punteggio
	Esempi di dati esposti a rischi di riservatezza **senza prove che l'elaborazione illegale si è verificata:** - Un file cartaceo o un laptop si perde durante il transito; - L'attrezzatura è stata smaltita senza distruzione dei dati personali.	**0**
	Esempi di dati trasmessi verso un certo numero **di destinatari conosciuti:** - Un'e-mail con dati personali è stata inviata erroneamente a un certo numero di destinatari conosciuti; - Alcuni clienti possono accedere agli account di altri clienti in un servizio online.	**0,25**
	Esempi di dati trasmessi verso un certo numero **di destinatari sconosciuti:** - I dati sono pubblicati su una bacheca internet; - I dati vengono caricati su un sito P2P; - Un dipendente vende un CD ROM con i dati degli utenti; - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.	**0,5**
Violazione di integrità	**Definizione:** La perdita di integrità si verifica **quando le informazioni originali vengono alterate** e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando esistono gravi possibilità che i dati modificati siano stati utilizzati in un modo che potrebbe danneggiare l'individuo.	
	Esempi di **dati modificati** ma **senza alcun uso errato o illegale** identificato: - Le registrazioni di un database con dati personali sono state erroneamente aggiornate ma è stata effettuata una copia dell'originale prima del verificarsi della modifica.	**0**
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale ma con possibilità di recupero**: - Un dato necessario per la fornitura di un servizio online è stato modificato e l'individuo deve richiedere il servizio in modalità offline. - È stato modificato un dato importante per l'accuratezza del file di un individuo in un servizio medico online.	**0,25**
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale senza possibilità di recupero**: - Valgono gli esempi precedenti con l'aggravante che i dati originali non possono essere recuperati.	**0,5**
Violazione di disponibilità	**Definizione:** La **perdita di disponibilità** si verifica quando non è possibile accedere ai dati originali quando ce n'è bisogno. Può essere temporaneo (i dati sono recuperabili ma richiederà un periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).	
	Esempi di dati che **possono essere recuperati senza difficoltà**:	**0**

Circostanze della violazione (CB)		Punteggio
	- Una copia del file è persa ma sono disponibili altre copie. - Un database è danneggiato ma può essere facilmente ricostruito da altri database.	
	Esempi di **indisponibilità temporale**: - Un database è corrotto ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione. - Un file è perso ma l'informazione può essere fornita di nuovo dall'individuo	**0,25**
	Esempi di **indisponibilità totale** (i dati non possono essere recuperati dal controllore o dai singoli): - Un file è perso / database danneggiato, non c'è il backup di queste informazioni e non può essere fornito dall'individuo.	**0,5**
Intenzioni malevole	**Definizione:** La violazione è **dovuta a un'azione intenzionale malevola**, ad esempio al fine di causare problemi al Titolare o danneggiare gli interessati.	
	Esempi di violazione dovuta a un'azione intenzionale: - Un dipendente di un'azienda condivide intenzionalmente dati privati dai clienti in un sito pubblico di social media. - Un dipendente di un'azienda vende dati privati dei clienti a un'altra società. - Un membro di un social network invia intenzionalmente delle informazioni sugli altri membri ai propri familiari al fine di danneggiarli.	**0,5**

TABELLA 5 – CIRCOSTANZE DELLA VIOLAZIONE (CB)

Fase 4: Calcolo della Gravità

Il punteggio finale mostra il livello di gravità di una determinata violazione, tenendo conto dell'impatto sui diritti e libertà delle persone fisiche.

Nella tabella seguente sono riassunte le attività inerenti **la fase di Calcolo della gravità (CG):**

Attività	Descrizione	Strumenti
7- Procedere al Calcolo della Gravità	Calcola la gravità della violazione applicando la formula definita dalla Metodologia	*Formula:* ***CG = DPC * EI + CB***

Attività	Descrizione	Strumenti
8- Definire il livello di gravità della violazione	Definisce il livello di gravità (basso, medio, alto e molto alto) secondo il risultato finale della valutazione. Il risultato viene classificato secondo quattro livelli di gravità: • Basso (punteggio finale è **inferiore a 2**) • Medio (punteggio finale è **tra 2 e 3**) • Alto (punteggio finale è **tra 3 e 4)** • Molto alto (punteggio finale è **superiore a 4**)	*TABELLA 6 – LIVELLO DI GRAVITÀ*

Di seguito si riporta la tabella da utilizzare **per la valutazione del livello di gravità:**

Punteggio	Livello	Descrizione
Gravità < 2	**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.)
2 ≤ Gravità < 3	**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.).
3 ≤ Gravità < 4	**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.).
4 ≤ Gravità	**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 6 – LIVELLO DI GRAVITÀ

<u>Ulteriori valutazioni</u>

Ai sensi delle "*Guidelines on Personal data breach notification under Regulation 2016/679*"[5] (WP250rev.01) qualora la violazione di dati personali subita riguardi:

- **Dati personali adeguatamente cifrati** (i) con algoritmi considerati sufficientemente sicuri e adeguati (ii) dove la chiave di sicurezza non risulti in alcun modo compromessa;

E, al contempo:

- Siano presenti **copie e/o backup dei dati** coinvolti nella violazione, che ne consentono un

[5] Si veda pag. 18 del WP250 rev.01

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

pronto ripristino.

si può affermare che i dati personali non sono accessibili da terze parti non autorizzate al trattamento e che **non sussistono** - o che sono improbabili **- rischi per i diritti e le libertà degli interessati.**

Pertanto, in tale ipotesi il livello finale di gravità di una determinata violazione sarà automaticamente valutato come **Basso**.

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

it

Azienda Sanitaria Locale Napoli 3 Sud
con sede legale in Torre del greco
via Guglielmo Marconi, 66 - 80059 (NA)
in persona del suo legale rappresentante pro-tempore

All'attenzione del:
DPO
PEC:

VIOLAZIONE DI DATI PERSONALI
MODULO DI SEGNALAZIONE

Oggetto: segnalazione Data Breach

Data e ora della rilevazione dell'evento

Data dell'evento (se differente dalla rilevazione)

Luogo e contesto dell'evento

Nome e dati di contatto della persona che ha effettuato la segnalazione dell'evento (cellulare ed e-mail)

Descrizione dettagliata del contesto dell'evento

Categoria di dati personali coinvolti nell'evento e numero approssimativo di interessati

Descrizione delle eventuali azioni intraprese sin dal momento della rilevazione

Note aggiuntive

regione campania
aslnapoli3sud

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
Tel 081/8490645- PROTOCOLLO@pec.aslnapoli3sud.it

.it

FLOW CHART DEL PROCESSO DI GESTIONE DI UN DATA BREACH

SEGNALAZIONE DI POSSIBILE PERSONAL DATA BREACH

Verifica Segnalazione

IDENTIFICAZIONE DELLA SEGNALAZIONE RICEVUTA

SI CONFIGURANO DUE POSSIBILI IPOTESI

1. Possibile Data Breach: si procede alla successiva fase di Valutazione

2.Falso Positivo

Il Processo si interrompe. L'evento verrà annotato nel Registro Eventi e Violazioni

FASE DI VALUTAZIONE

Valutazione e stima della gravità del Data Breach

Individuazione azioni di rimedio sia tecniche che organizzative

FASE DI GESTIONE E RISPOSTA

- Si procederà alla notifica all'Autorità Garante.
- In caso di evidenti pregiudizi per gli interessati, si procederà anche alla contestuale notifica.

REVISIONE POST - INCIDENTE

- L'evento verrà annotato nel Registro Eventi e Violazioni.
- Verrà predisposto il Piano di Rimedio e saranno individuate le opportunità di miglioramento per prevenire incidienti futuri.

SI RAPPRESENTA CHE IN TUTTE LE FASI DEL PROCESSO DI GESTIONE DI UN DATA BREACH, DOVRANNO ESSERE COINVOLTI:

- Il Responsabile del Servizio presso cui si è verificata la presunta violazione.
- La UOS Privacy.
- La UOC Sistemi Informatici, in caso di incidente informatico.
- Il DPO Aziendale, per il supporto di competenza.