Allegato 5

LINEE GUIDA PER LA GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI PERSONALI

(Data breach)

Storia del documento

Data	Versione	Descrizione modifiche	Autore

66

Sommario

67

68

1 Generalità

Il presente documento descrive il processo adottato dalla Struttura Sanitaria per la gestione delle violazioni di sicurezza che comportano gravi rischi di 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.

1.1 Scopo e ambito di applicazione

I principi guida descritti nel presente documento sono finalizzati a definire in maniera chiara e comprensibile da tutto il personale aziendale interessato, le attività e le modalità operative, che consentano un approccio esaustivo ed omogeneo alla gestione delle violazioni di sicurezza afferenti alla privacy, secondo i criteri ed i principi stabiliti dalle vigenti normative.

Le linee guida si applicano, nello specifico, alle Unità Operative aziendali che trattano a qualsiasi titolo e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea) dati personali.

Con questo documento il Titolare del trattamento dei dati personali recepisce e pone in atto gli indirizzamenti cogenti formulati nell'art. 32 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 "Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" del 4 Aprile 2013 [2].

1.2 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.

1.3 Definizioni

Definizioni	Descrizione
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 di sicurezza	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.
Escalation (dell'incidente)	Attività procedurale predefinita, che stabilisce e regolamenta le modalità di trasferimento di responsabilità nella gestione delle violazioni della privacy, in funzione di specifici parametri che ne definiscono le soglie di gravità e di criticità.
Evento di sicurezza	Qualsiasi occorrenza che si verifica nell'ambito di un determinato asset informativo, rilevata mediante strumenti automatizzati o non automatizzati, la cui valenza è considerata significativa ai fini delle attività di gestione, controllo della sicurezza e contenimento dei rischi ad essa correlati.
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

70

Definizioni	Descrizione
	manifestazioni di possibili violazioni della privacy, non rivestono carattere di rilevanza nello specifico contesto entro il quale si sono verificati.
Incidente di sicurezza	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.
Rischio di sicurezza	Misurazione quantitativa e/o qualitativa che esprime la possibilità che un determinato agente di minaccia possa causare una violazione della sicurezza ovvero arrecare un danno al patrimonio informativo, sfruttando una o più vulnerabilità insite in uno o più asset.
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	Data Protection Officer
RPD	Responsabile della Protezione dei Dati

Tabella 2 – Acronimi

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. 32 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 della privacy.
Gli indirizzamenti formulati in questo paragrafo s'intendono applicabili a qualsiasi modalità di trattamento di dati personali effettuato in modalità automatizzata, semiautomatizzata o non automatizzata, utilizzando informazioni personali custodite in formato digitale o cartaceo.
Le primarie fonti autoritative che forniscono le informazioni necessarie alla definizione dei vari domini di monitoraggio sono:

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

che individuano i trattamenti, la loro tipologia, gli asset sensibili e la loro ubicazione, le minacce, i rischi e gli impatti derivanti dalle possibili violazioni della privacy.
Qualora non fossero disponibili informazioni dettagliate sufficienti, ad esempio per i trattamenti non sottoposti ad obbligo di DPIA, queste possono essere reperite direttamente presso le Funzioni e le Unità Operative che gestiscono i trattamenti (comparto IT, area del personale, amministrazione, reparti e UO mediche ecc..).

72

2.1.1 Monitoraggio degli eventi generati dai sistemi ICT

Il monitoraggio degli eventi ICT è l'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 categorie 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;

73

- Allarmi generati dai sistemi antispamming;
- Allarmi generati dai directory server/service.

Le attività di monitoraggio sono svolte 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 informazioni personali sensibili, 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 informazioni personali sensibili;
- Smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali sensibili;
- Constatazione di effrazione o tentativi di effrazione alle porte di accesso o alle serrature di chiusura degli armadi che custodiscono documenti sensibili;
- Presenza di personale non autorizzato nei locali preposti al trattamento di informazioni personali sensibili.

Le constatazioni di violazione o sospetta violazione devono essere comunicate al Responsabile della gestione incidenti privacy entro e non oltre 1 ora dalla constatazione.

2.2 Analisi e classificazione degli eventi di sicurezza

Gli eventi rilevati nel corso delle attività di monitoraggio, ovvero quelli segnalati da altre fonti, devono essere sottoposti ad analisi, da parte del personale preposto alla gestione degli incidenti privacy, al fine di valutare le origini, la natura e l'estensione 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 del/degli Interessato/i.
I criteri di classificazione degli eventi rilevati variano a seconda delle caratteristiche dei *domini di monitoraggio*, così come dettagliato nei paragrafi successivi.

2.2.1 Classificazione degli eventi rilevati sui sistemi ICT

Le attività di classificazione degli eventi sono svolte dagli operatori ICT incaricati dello svolgimento delle attività di gestione operativa degli incidenti privacy (di seguito operatori di sicurezza ICT). La classificazione di un allarme è frutto di analisi ponderate che si articolano secondo i seguenti passi valutativi:

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

2.2.1.1 Analisi degli eventi e valutazione degli impatti privacy

Questa attività consiste nel circoscrivere il perimetro di analisi attraverso l'individuazione degli asset informativi minacciati, rappresentati dai trattamenti e dalle 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. I risultati delle attività di analisi devono essere riepilogati attraverso la compilazione della "Tabella analitica degli eventi rilevati", di seguito esposta:

75

Tabella analitica degli eventi rilevati				
Descrizione evento	Impatto	Sistemi ICT Interessati	Trattamenti	Tipologia dei dati personali trattati

Dove:

- Alla voce "Descrizione evento" deve essere fornita una descrizione sintetica dell'evento rilevato;
- Alla voce "Impatto" deve essere fornito un giudizio sulle possibili conseguenze per la privacy riconducibili all'evento, utilizzando la seguente scala valutativa:
  - **Grave**: giudizio che sottintende una violazione della privacy causa di danni permanenti e non reversibili alla riservatezza, integrità e disponibilità dei dati personali e/o dei processi informatici di trattamento;
  - **Rilevante**: giudizio che sottintende una violazione della privacy causa di danni temporanei e reversibili alla riservatezza, integrità e disponibilità dei dati personali e/o dei processi informatici di trattamento;
  - **Significativo**: giudizio che sottintende una violazione della privacy che non comporta danni permanenti o temporanei tali da compromettere la riservatezza, integrità e disponibilità dei dati personali e/o dei processi informatici di trattamento;
  - **Falso positivo**: giudizio che sottintende eventi teoricamente malevoli che tuttavia non comportano alcuna violazione della privacy nel contesto specifico in esame.
- Alla voce "Sistemi ICT interessati" deve essere fornito l'elenco dei sistemi ICT interessati dall'evento;

76

- Alla voce "Trattamenti interessati" deve essere fornito l'elenco dei trattamenti interessati dall'evento, prendendo come riferimento la nomenclatura utilizzata nel Registro dei Trattamenti;
- Alla voce "Categoria dati personali" deve essere indicata la tipologia di dati personali interessati dall'evento, utilizzando la medesima tassonomia indicata nel Registro dei trattamenti.

Gli eventi che presentano un impatto classificato come "Falso positivo" sono riconducibili a quella tipologia di eventi che, seppure possano apparire come una presunta violazione della sicurezza, a seguito di successive indagini di approfondimento risultano ordinari o tollerabili nel contesto specifico entro il quale sono stati rilevati. Pertanto, qualora si rilevino solo eventi classificati come falso positivo, il processo di classificazione allarmi viene terminato, così come tutte le successive attività afferenti alla gestione degli incidenti privacy.

2.2.1.2 Valutazioni della criticità del trattamento

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

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

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

77

2.2.2 Classificazione degli eventi rilevati sulle infrastrutture di sicurezza fisica

Il rilevamento di uno o più eventi descritti al paragrafo 2.1.2 deve essere comunicato entro 1 ore dalla constatazione dell'evento.

2.2.2.1 Eventi rilevati attraverso i servizi di vigilanza

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

Ferme restando le procedure operative e i livelli di servizio prestabiliti per queste tipologie di servizi, devono essere riportati al Responsabile della gestione degli incidenti privacy i seguenti eventi:

- Constatazioni di effrazione rilevate sui punti di accesso a locali all'interno dei quali sono trattati dati personali;
- Constatazione di furto di documenti cartacei;
- Constatazione di furto di strumenti o dispositivi informatici che custodiscono dati personali sensibili.

2.2.2.2 Eventi rilevati dal personale operativo

Rientrano in questa categoria gli eventi rilevati dal personale interno o esterno alla Struttura Sanitaria che a vario titolo, è autorizzato ad accedere ai locali presso i quali si svolgono trattamenti di dati personali.

Ferme restando le procedure in essere per la segnalazione di furti o smarrimenti di beni o documenti aziendali, devono essere riportati al Responsabile della gestione degli incidenti privacy i seguenti eventi, occasionalmente rilevati nel corso dello svolgimento delle normali attività lavorative:

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

78

La segnalazione degli eventi sopra riportati può essere effettuata, anche solo in forma verbale, al responsabile dell'Unità Operativa presso la quale sono stati rilevati gli eventi che provvederà a sua volta ad informare il Responsabile della gestione degli incidenti privacy, entro 1 ora dal ricevimento della segnalazione.

2.2.2.3 Analisi degli eventi e valutazione degli impatti privacy

Il Responsabile della gestione degli incidenti privacy, a seguito delle segnalazioni descritte nei paragrafi 2.2.2.1 e 2.2.2.2, ovvero a seguito di segnalazioni provenienti da altre fonti, svolge un'analisi di approfondimento finalizzata a valutare gli eventuali impatti sulla privacy, documentata attraverso la seguente tabella analitica:

Tabella analitica degli eventi rilevati				
Descrizione evento	Impatto	Siti interessati	Trattamenti	Tipologia dei dati personali trattati

Dove:

- Alla voce "Descrizione evento" deve essere fornita una descrizione sintetica dell'evento rilevato;
- Alla voce "Impatto" deve essere fornito un giudizio sulle possibili conseguenze per la privacy riconducibili all'evento, utilizzando la seguente scala valutativa:
    - **Grave**: giudizio che sottintende una violazione della privacy causa di danni permanenti e non reversibili alla riservatezza, integrità e disponibilità dei dati personali e/o che comportano gravi violazioni dei vincoli di trattamento a cui sono applicabili sanzioni di grande entità;

79

- **Rilevante**: giudizio che sottintende una violazione della privacy causa di danni temporanei e reversibili alla riservatezza, integrità e disponibilità dei dati personali e/o che compartano violazioni dei vincoli di trattamento a cui sono applicabili sanzioni di rilevante entità;
- **Significativo**: giudizio che sottintende una violazione della privacy che non comporta danni permanenti o temporanei tali da compromettere la riservatezza, integrità e disponibilità dei dati personali che tuttavia comportano probabili violazioni dei vincoli di trattamento a cui sono applicabili sanzioni di lieve entità;
- **Falso positivo**: giudizio che sottintende eventi teoricamente malevoli che tuttavia non comportano alcuna violazione della privacy nel contesto specifico in esame.

- Alla voce "Siti interessati" deve essere fornito l'elenco dei locali all'interno dei quali è stato constatato l'evento;
- Alla voce "Trattamenti interessati" deve essere fornito l'elenco dei trattamenti interessati dall'evento, prendendo come riferimento la nomenclatura utilizzata nel Registro dei Trattamenti;
- Alla voce "Categoria dati personali" deve essere indicata la tipologia di dati personali interessati dall'evento, utilizzando la medesima tassonomia indicata nel Registro dei trattamenti.

Gli eventi che presentano un impatto classificato come "Falso positivo" sono riconducibili a quella tipologia di eventi che, seppure possano apparire come una presunta violazione della sicurezza, a seguito di successive indagini di approfondimento risultano ordinari o tollerabili nel contesto specifico entro il quale sono stati rilevati. Pertanto, qualora si rilevino solo eventi classificati come falso positivo, il processo di analisi e valutazione degli eventi viene terminato, così come tutte le successive attività afferenti alla gestione degli incidenti privacy.

2.2.2.4 Valutazioni della criticità del trattamento

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

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

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

2.3 Valutazioni di criticità degli allarmi

La criticità dell'allarme esprime un giudizio complessivo ricavato dal valore massimo rilevato su tutti i giudizi di IMPATTO e dal valore massimo rilevato su tutti i giudizi di CRITICITÀ precedentemente attribuiti, seguendo la tabella decisionale di seguito esposta:

Tabella decisionale per la valutazione di criticità dell'allarme		
Impatto degli eventi	Criticità del trattamento	Criticità dell'allarme
GRAVE	ALTA	ALTA
RILEVANTE	ALTA	ALTA
SIGNIFICATIVO	ALTA	MEDIA
GRAVE	MEDIA	ALTA
RILEVANTE	MEDIA	ALTA
SIGNIFICATIVO	MEDIA	MEDIA
GRAVE	BASSA	ALTA
RILEVANTE	BASSA	MEDIA
SIGNIFICATIVO	BASSA	BASSA

La valutazione della criticità dell'allarme stabilisce le priorità e le modalità di attuazione delle misure di contenimento degli impatti privacy anche in termini di responsabilità di gestione (escalation).

3 Trattamento degli allarmi privacy

Sulla base delle valutazioni di criticità dell'allarme, effettuate nelle precedenti fasi, gli operatori incaricati della gestione degli incidenti privacy, devono procedere all'apertura della **scheda di gestione allarme**, che attiva il contatore temporale per la rendicontazione dei livelli di servizio (SLA) applicati alle attività di trattamento dell'allarme in essere.

La priorità di trattamento di un allarme viene attribuita secondo il giudizio di criticità, osservando i seguenti livelli di servizio:

- Allarmi con criticità **BASSA**: apertura della "scheda di gestione allarme" ed avviamento delle misure di contrasto/contenimento entro **6 ore** dal rilevamento degli eventi che hanno generato l'allarme;
- Allarmi con criticità **MEDIA**: apertura della "scheda di gestione allarme" ed avviamento delle misure di contrasto/contenimento entro **4 ore** dal rilevamento degli eventi che hanno generato l'allarme;
- Allarmi con criticità **ALTA**: apertura della scheda di "gestione incidente" e comunicazione alle funzioni interessate entro **2 ore** dal rilevamento degli eventi che hanno generato l'allarme.

L'apertura di una "scheda di gestione allarmi" attiva le attività di contenimento degli impatti privacy mentre l'apertura di una "scheda di gestione incidente" attiva il processo di gestione ed escalation delle responsabilità descritto nel capitolo 0.

4 Gestione degli incidenti di sicurezza con impatti sulla privacy

Nell'ambito della presente linea guida, si definisce "incidente di sicurezza con impatti sulla privacy: *"qualsiasi evento, intenzionale o involontario che comporti compromissioni irreversibili della riservatezza, integrità e disponibilità dei dati personali e/o gravi violazioni dei vincoli di trattamento prestabiliti, tali da compromettere le libertà individuali e l'esercizio dei diritti dell'interessato*".

Il processo di gestione degli incidenti di sicurezza con impatti sulla privacy è attivato dall'apertura di una "scheda di gestione incidente", secondo i criteri e le modalità definite al paragrafo 2.3 e si esplica attraverso l'esecuzione delle seguenti attività:

- Classificazione dell'incidente di sicurezza;
- Escalation delle responsabilità di gestione dell'incidente;
- Notifica al garante, nei casi ritenuti opportuni;
- Notifica all'interessato, nei casi ritenuti opportuni;
- Analisi post incidente;
- Definizione delle misure compensative e dei piani di rientro;
- Stesura del rapporto di chiusura incidente.

Nei paragrafi successivi sono dettagliati i criteri decisionali e le modalità operative che regolamentano lo svolgimento delle suddette attività.

4.1 Classificazione dell'incidente di sicurezza

La classificazione dell'incidente di sicurezza è un'attività posta sotto la diretta responsabilità del Titolare del trattamento che può avvalersi del supporto del Data Protection Officer (DPO) per:

A. Esaminare la correttezza dei parametri e dei giudizi valutativi attribuiti che hanno condotto all'apertura della scheda di gestione incidente;
B. Esaminare l'esaustività della documentazione prodotta a corredo della scheda di gestione incidente, al fine di produrre i razionali richiesti per una eventuale notifica al Garante e, nei casi ritenuti opportuni, al/agli Interessato/i;

C. Attribuire una classe di rilevanza dell'incidente al fine di facilitare il processo decisionale in base al quale sono disposti gli obblighi di notifica.

Qualora, a seguito delle verifiche di cui al punto [A], non si rilevino gli estremi per una dichiarazione di incidente, si procederà alla chiusura dell'incidente ed alla eventuale apertura della scheda di gestione allarme.

Gli incidenti di sicurezza con impatti sulla privacy sono classificabili in due categorie anche dette "classi di rilevanza" e precisamente:

- Categoria A: Incidenti di sicurezza che comportano gravi lesioni delle libertà individuali;
- Categoria B: Incidenti di sicurezza che possono precludere la qualità del servizio erogato senza tuttavia comportare gravi lesioni delle libertà individuali dell'Interessato.

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

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

La categorizzazione dell'incidente, anche se svolta dal DPO deve comunque essere approvata dal Titolare del trattamento.

4.2 Escalation della responsabilità di gestione dell'incidente

La dichiarazione di incidente comporta il passaggio automatico delle responsabilità di gestione al Titolare del trattamento, che assume il ruolo di supervisore e coordinatore anche di tutte le attività operative, in quanto il GDPR non consente alcuna delega di responsabilità in caso di incidente privacy.

In particolare, la decisione di notifica al Garante Privacy ed eventualmente agli interessati, è sottoposta alla discrezionalità del Titolare, che può decidere se adempiere o meno a tale disposizione, indipendentemente da ogni altro parametro valutativo prodotto a seguito dell'applicazione della presente procedura.

4.3 Adempimento agli obblighi di notifica

Fermi restando i principi di responsabilità e discrezionalità enunciati nel paragrafo precedente, il Titolare del trattamento può avvalersi della collaborazione del DPO come supporto nello svolgimento delle seguenti attività:

- Analisi degli elementi che indirizzano o meno l'obbligo di notifica al Garante Privacy;
- Analisi degli elementi che indirizzano o meno l'obbligo di notifica all'Interessato;
- Gestione delle comunicazioni con l'esterno (es. comunicati stampa, relazioni con il Garante, relazioni con l'Interessato).

Di seguito sono esposti i principi guida che possono essere utilizzati come supporto decisionale per l'applicazione degli obblighi di notifica:

1. Gli incidenti di sicurezza attribuiti alla Categoria o Classe di Rilevanza [A] suggeriscono la necessità di notifica sia al Garante Privacy che al/agli Interessato/i.
2. Gli incidenti di sicurezza attribuiti alla Categoria o Classe di Rilevanza [B] escludono la necessità di comunicazione al/agli Interessato/i, nei casi in cui la temporanea perdita dell'esercizio dei propri diritti sia contenuta entro limiti temporali ragionevoli. È invece

lasciata alla discrezionalità del Titolare la valutazione di applicabilità del solo obbligo di notifica al Garante Privacy.

La notifica al Garante Privacy deve avvenire entro 72 ore dalla constatazione dell'incidente il cui conteggio è calcolato a partire dalla classificazione dell'allarme che sottintende un presunto incidente privacy.

4.4 Analisi post incidente

Le analisi post incidente rappresentano un insieme di attività, coordinate dal Titolare del trattamento e supportate da DPO, finalizzate a rilevare ulteriori elementi utili a definire:

- Le cause che hanno reso possibile il verificarsi dell'incidente;
- Le circostanze che hanno consentito lo sfruttamento di vulnerabilità logiche, fisiche ed organizzative;
- La natura delle vulnerabilità e la riconducibilità a circostanze fortuite o cause di forza maggiore ovvero ad errori umani o anomalie hw/sw ovvero alla mancata o parziale applicazione delle misure di sicurezza indirizzate dalle baseline e dalle eventuali DPIA;
- L'eventuale evidenza di aver applicato diligentemente adeguate misure preventive o di contenimento, secondo criteri di proporzionalità tra costi sostenibili e benefici per la tutela delle libertà individuali.

Le analisi post incidente possono fornire informazioni utili a:

- Evadere eventuali ulteriori richieste di descrizione circostanziata formulate dal Garante Privacy e/o dal/dagli Interessato/i;
- Fornire elementi utili all'attuazione delle misure compensative adeguate a evitare o contenere i rischi di reiterazione dell'incidente.

Inoltre, nei casi previsti dal Codice di Procedura Penale è data facoltà al Titolare del trattamento di esporre denuncia presso le istituzioni rispettivamente competenti in materia di reati informatici, furti e atti vandalici. Nei casi previsti dal Contratto di Lavoro e dai regolamenti interni della Struttura

87

Sanitaria, il titolare può disporre anche l'applicazione di sanzioni disciplinari al personale ritenuto responsabile o corresponsabile dell'incidente.

4.5 Definizione delle misure compensative e dei piani di rientro

A seguito delle analisi dettagliate descritte al paragrafo precedente, il DPO convoca e coordina un "Comitato di indirizzamento degli adempimenti privacy", costituito dai responsabili delle Unità Operative coinvolti a vario titolo nel processo di trattamento dei rischi privacy. Scopo del comitato è quello di definire un adeguato insieme di misure compensative volte a prevenire, limitare e contenere i rischi di reiterazione dell'incidente.

Al termine dei lavori il Comitato produce un "Piano di rientro", contenente:

- I requisiti che indirizzano l'implementazione delle misure compensative logiche, fisiche, procedurali ed organizzative;
- La matrice di responsabilità nell'attuazione delle misure compensative;
- I tempi previsti per l'attuazione di ciascuna misura compensativa;
- La finestra temporale di esposizione al rischio derivante dai tempi necessari al completamento di tutte le misure compensative.

Il Piano di Rientro, redatto dalle Unità Operative responsabili, sottoposto a verifica da parte del DPO e successivamente all'approvazione del Titolare del trattamento, costituisce il primo atto formale per l'attivazione dell'iter di approvvigionamento delle risorse necessarie all'implementazione delle misure compensative.

4.6 Stesura del rapporto di chiusura incidente

Il rapporto di chiusura incidente è un documento ad uso interno, attraverso il quale il Responsabile della gestione degli incidenti privacy comunica al Titolare del trattamento e al DPO la chiusura di tutte le attività di gestione dell'incidente, fornendo una sintesi di riepilogo delle seguenti informazioni:

- Eventi rilevati che hanno condotto alle valutazioni di criticità e conseguentemente all'apertura della scheda incidente;

- Asset interessati (es. sistemi informatici, locali operativi);
- Data e ora di apertura della scheda di gestione incidente;
- Data e ora di comunicazione del Rapporto di chiusura incidente;
- Riepilogo degli SLA osservati nel corso del processo di gestione incidenti ed eventuale giustificazione dei motivi che ne possono aver causato un ritardo;
- Copia allegata della notifica al Garante Privacy e riepilogo delle comunicazioni istituzionali intercorse;
- Copia allegata della eventuale notifica al/agli Interessato/i e riepilogo delle comunicazioni istituzionali intercorse;
- Copia allegata dell'eventuale Piano di Rientro prodotto.

L'approvazione, così come l'archiviazione del Rapporto di chiusura incidente è in carico al Responsabile della gestione degli incidenti privacy.

89