Procedura interna per la gestione delle violazioni dei dati personali
(*Data Breach*)

ai sensi degli artt. 33-34 del Regolamento UE 2016/679

ASL FOGGIA

Redatto da	Dirigente Servizi Informativi Aziendali
Verificato da	Responsabile Protezione Dati
Approvato da	Direttore Generale

Data	Ed.	Rev.	Parti modificate
	1	0	Prima emissione

SOMMARIO

1. Premessa

Il *data breach* è una violazione di 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.
Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi sono:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

2. Scopo e ambito di applicazione

Il presente documento si prefigge lo scopo di indicare a tutto il personale aziendale dell'ASL di Foggia, ivi compresi collaboratori professionisti esterni e Fornitori, le opportune modalità di gestione del data breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.
In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la sostenibilità organizzativa, nella gestione delle violazioni di dati, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare per il tramite del Responsabile della protezione dei dati
- modalità e profili di segnalazione all'Autorità Garante per la protezione dei dati personali
- valutazione e ponderazione dell'evento di *data breach*

- eventuale comunicazione agli interessati

La presente procedura operativa si applica nello specifico alle Unità Operative dell'ASL di Foggia che trattano a qualsiasi titolo e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea) dati personali riconducibili alle seguenti categorie di Interessati:

- Personale interno o personale esterno distaccato presso l'ASL di Foggia, collaboratori, professionisti esterni, tirocinanti, borsisti, personale dei Fornitori;
- Assistiti e familiari.

3. Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi degli artt. 37-39 del GDPR;

Delegato del trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda sanitaria che determina specifiche modalità organizzative rispetto ad uno o più trattamenti di competenza;

Persona autorizzata al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

Violazione dei dati personali (c.d. *data breach*):la violazione di 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.

4. Norme di riferimento

- REGOLAMENTO UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34
- DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali"
- DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
- Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)

5. Ruoli e Responsabilità

La seguente tabella descrive i ruoli e le responsabilità, descritte mediante una matrice RACI, dei soggetti coinvolti nel processo di gestione delle violazioni della sicurezza con impatti sui diritti e le libertà degli interessati :

Soggetto	Ruolo assegnato dalla procedura	Responsabilità (RACI)
Titolare del trattamento dei dati personali	Ruolo istituzionale a cui è attribuita la Titolarità degli adempimenti di legge previsti per la gestione degli incidenti (data breach).	Supervisione delle attività ed approvazione dei documenti prodotti nelle fasi di gestione degli incidenti con impatti privacy (Accountable)
Responsabile della protezione dei dati (Data Protection Officer)	Ruolo istituzionale che fornisce il supporto tecnico al Titolare del trattamento, per il corretto indirizzamento delle decisioni intraprese nel corso del processo di gestione degli incidenti con impatti sulla privacy.	Supporto alle decisioni intraprese dal Titolare del trattamento (Collaborate); Responsabile del coordinamento del Comitato di gestione e trattamento degli incidenti (Responsible)
Responsabile della gestione degli incidenti	Ruolo aziendale responsabile del coordinamento di tutto il processo di gestione delle violazioni di sicurezza con impatti sulla privacy.	Responsabile interno del coordinamento del processo di gestione delle violazioni di sicurezza con impatti sulla privacy (Responsible)
Operatori della sicurezza ICT	Personale tecnico delle unità Operative ICT incaricato dello svolgimento delle attività di monitoraggio, rilevamento degli eventi e classificazione degli allarmi di sicurezza ICT con impatti sulla privacy.	Collabora, sotto il riporto funzionale del Responsabile della gestione degli incidenti , nello svolgimento delle attività operative di monitoraggio, analisi eventi, classificazione e gestione degli allarmi di sicurezza ICT con impatti sulla privacy (Collaborate).

6. Monitoraggio eventi di sicurezza

I processi di monitoraggio costituiscono la base per una corretta e tempestiva gestione degli incidenti di sicurezza con impatti sulla protezione dei dati personali, 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. 34 del Regolamento UE 2016/679.
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 elencate alcune categorie di eventi ICT sottoposte a monitoraggio:

a) Log generati dalle attività svolte con *account* riconducibili agli amministratori di sistema, con particolare attenzione a:
- Orari di connessione/disconnessione (log-on / log-off);
- Modifiche alle configurazioni di sistema;
- Qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
- Log relativi 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);
- Qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata).

b) 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);

c) 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.

Le attività di monitoraggio sono svolte dal personale del servizio informatico aziendale incaricato delle attività di gestione operativa della sicurezza, al quale sono assegnati i privilegi di accesso in lettura dei file di tracciamento.

7. Sicurezza fisica

I locali preposti al trattamento di dati 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;
- 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;
- Smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali sensibili.

Le constatazioni di violazioni o sospette violazioni devono essere comunicate al Responsabile della protezione dei dati, entro e non oltre 1 ora dalla rilevazione.

8. Analisi degli Eventi

L'attività di analisi consiste nel circoscrivere il perimetro 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 è 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" o report equivalente, di seguito riportata:

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;
- Alla voce "Trattamenti interessati" deve essere fornito l'elenco dei trattamenti interessati dall'evento;
- Alla voce "Categoria dati personali" deve essere indicata la tipologia di dati personali interessati dall'evento (personali, sensibili e giudiziari).

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.

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 valutazioni d'impatto sulla protezione dei dati (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.

9. Criticità degli Eventi

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 riportata:

Impatto degli eventi	Criticità del trattamento	Criticità dell'allarme
GRAVE	ALTA	ALTA
RILEVANTE	ALTA	ALTA
SIGNIFICATIVO	ALTA	MEDIA
GRAVE	MEDIA	MEDIA
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 (*c.d. escalation*).

10. Gestione allarmi e priorità

Sulla base delle valutazioni di criticità dell'allarme, effettuate nelle precedenti fasi, il personale incaricato della gestione degli incidenti, devono procedere all'apertura di una scheda di gestione allarme (**allegato Mod-DB-02_Gestione-Incident**), che consenta di attivare il contatore temporale per la rendicontazione dei livelli di servizio (SLA) applicati alle attività di trattamento dell'allarme in essere.

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.

11. Gestione incidenti di sicurezza

Nell'ambito della presente procedura, si definisce "incidente di sicurezza con impatti sulla protezione dei dati" qualsiasi evento, intenzionale o involontario che comporta 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 sui diritti e le libertà delle persone fisiche, è attivato dall'apertura di una "scheda di gestione incidente", secondo i criteri e le modalità definite precedentemente e si esplica attraverso l'esecuzione delle seguenti attività:

- Classificazione dell'incidente di sicurezza;
- Escalation delle responsabilità di gestione dell'incidente;
- Notifica all'Autorità Garante, nei casi previsti dalla norma;
- Notifica all'interessato, nei casi previsti dalla norma;
- 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.

12. Classificazione incidente

La classificazione dell'incidente di sicurezza è un'attività posta sotto la diretta responsabilità del Responsabile dei Sistemi informativi aziendali che può avvalersi del supporto del Responsabile della protezione dei dati (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 unto [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 sui diritti e le libertà delle persone fisiche, 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 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	Violazione dei diritti individuali

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

In particolare la decisione di notifica all' Autorità Garante per la protezione dei dati 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.

Il Titolare del trattamento può avvalersi della collaborazione del Responsabile della protezione dei dati come supporto nello svolgimento delle seguenti attività:

- Analisi degli elementi che indirizzano o meno l'obbligo di notifica al Garante;
- 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 principio guida che possono essere utilizzati come supporto decisionale per l'applicazione degli obblighi di notifica :

- Gli incidenti di sicurezza attribuiti alla Categoria o Classe di Rilevanza [A] suggeriscono la necessità di notifica sia al Garante che al/agli Interessato/i.
- 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.
  La notifica all'Autorità Garante per la protezione dei dati (via pec protocollo@pec.gpdp.it) 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.
  Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

  Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.
  Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di Euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.

13. Analisi ex-post incidente

Le analisi ex-post incidente rappresentano un insieme di attività, coordinate dal Responsabile dei Sistemi Informativi aziendali e supportate da Responsabile della protezione dei dati, 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 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 presentare 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 ASL di Foggia, il Titolare può disporre anche l'applicazione di sanzioni disciplinari al personale ritenuto responsabile o corresponsabile dell'incidente.

14. Rapporto chiusura incidente

Il rapporto di chiusura incidente è un documento ad uso interno, attraverso il quale il Responsabile dei Sistemi Informativi comunica al Titolare del trattamento e al Responsabile della protezione dei dati 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 dei Sistemi Informativi aziendali.

15. Eventi rilevati da personale esterno

Ogniqualvolta l'ASL di Foggia, in qualità di Titolare del trattamento, si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico "contratto" che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto. Ciò al fine di obbligare il Responsabile del trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679, ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*.
Ad ogni Responsabile del trattamento deve essere comunicato il contatto del Responsabile della protezione dei dati, al quale effettuare la predetta segnalazione.
Ogni Responsabile del trattamento, qualora venga a conoscenza di un potenziale *data breach* che riguardi dati di cui l'ASL di Foggia sia Titolare del trattamento, ne dà avviso senza ingiustificato ritardo al Responsabile della protezione dei dati, tramite il modulo allegato (Mod-DB-01_Data-Breach).
Per "ingiustificato ritardo" si considera la notizia pervenuta al Titolare al più tardi entro 12 ore dalla rilevazione iniziale da parte del Responsabile.
Il Responsabile della protezione dei dati effettua una valutazione dell'evento avvalendosi, nel caso, del Gruppo Privacy e di eventuali altre professionalità necessarie per la corretta analisi dell'evento e dei rischi per i diritti e le libertà degli interessati.
Con riferimento agli eventi rilevati dal personale preposto alla vigilanza attiva dei locali fisici presso le sedi dell'ASL di Foggia, svolti anche con l'ausilio di dispositivi di videosorveglianza, devono essere riportati al Responsabile dei Sistemi informativi dell'ASL di Foggia 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 strumenti o dispositivi informatici che custodiscono dati personali sensibili.