GESTIONE DEL DATA BREACH

SOMMARIO

1. SCOPO/OBIETTIVO

Lo scopo della presente procedura è di fornire istruzioni precise e dettagliate nel caso che succeda un incidente informatico, e nello specifico una violazione dei dati.

2. CAMPO DI APPLICAZIONE

La presente procedura è indirizzata a tutti gli operatori della Fondazione Onlus Longini Morelli Sironi ed ai servizi coinvolti.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

Autore	Titolo
PARLAMENTO EUROPEO	GDPR 679/2016 – Regolamento Europeo 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
Gruppo di lavoro articolo 29 (WP29)	Linee guida sul data breach (violazione dei dati)

4. ABBREVIAZIONI, DEFINIZIONI E TERMINOLOGIA

Abbreviazioni	
R.S.A.	Residenza Sanitaria Assistenziale
I.O.	Istruzione Operativa
PR	Procedura
Definizioni e terminologia	
violazione dei dati personali	(articolo 4, paragrafo 12 del GDPR) = una violazione della sicurezza che porta la distruzione accidentale o illecita, la perdita, l'alterazione, divulgazione o accesso non autorizzati, i dati personali trasmessi, memorizzati o comunque elaborati.
distruzione di dati personali	i dati non esistono più, o esistono in una forma che non è più di alcuna utilità
danni ai dati	avviene quando i dati personali sono stati modificati, danneggiati, o non sono più completi.
perdita di dati personali	quando i dati possono ancora esistere, ma il titolare del trattamento ha perso il controllo o l'accesso ad essi, o non sono in suo possesso.
titolare del trattamento	persona giuridica o fisica che tratta i dati personali: per la Fondazione onlus Longini Morelli Sironi il Presidente.
incidente di sicurezza informatica	qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore

5. MATRICE DELLE RESPONSABILITÀ

R= responsabile, C= coinvolto

Funzione - Attività	Direzione	Revisore	CdA	Personale
Identificazione di un processo da documentare	R			C
Identificazione di un gruppo di lavoro	R			C
Redazione di Procedura o Istruzione Operativa	R			C
Verifica del documento		R		
Approvazione documento			R	
Emissione del documento	R			
Applicazione documento	R			R

6.PROCESSO/MODALITÀ OPERATIVE

- Descrizione del processo

6.1 La preparazione pre-incidente

La preparazione pre-incidente comprende tutta quella serie di operazioni di tipo preparativo finalizzate alla prevenzione e alla reazione dell'incidente informatico in ambito aziendale. Dato che la durata della fase di preparazione è inversamente proporzionale al tempo di risoluzione del problema, è molto utile consultare l'amministratore per velocizzarla. Più siamo preparati e meno impiegheremo nell'analisi
Entrando più nello specifico, è necessario che:

- siano seguite le procedure previste in caso di incidente per continuare a garantire il servizio
- sia stabilito chi sono i contatti da interpellare in caso di incidente. Possono essere sia interni (personale interno all'azienda, ad esempio l'amministratore del servizio informatico), nel nostro caso dottor Luigi Gogna che esterni (libere categorie come Polizia Giudiziaria, Legali, CERT, eccetera)
- siano definiti i ruoli e le responsabilità all'interno del team di risposta
- sia eseguito un *Hands On* sulla log analysis e sull'esame forense così da cercare il maggior numero di punti di correlazione possibile sulle varie fonti. Per *log analysis* non si intende banalmente solo l'analisi dei log, ma anche la ricostruzione dell'incidente basandosi sul contenuto delle prove. L'e*same forense* è invece l'esame delle prove, ed è eseguita con strumenti di computer forensi che possono essere stand-alone o distribuiti
- siano stabilite le linee guida da seguire per garantire la sicurezza del sistema
- siano scelte le risorse da utilizzare per l'analisi

6.2 Tipi di violazioni dei dati personali

Nel suo parere 03/2014 sulla notifica di violazione, il WP29 ha spiegato che le violazioni possono essere categorizzate secondo i seguenti tre principi di sicurezza ben noti[1]:

- "Violazione di riservatezza" - dove c'è una divulgazione non autorizzata o accidentale, o accesso a, i dati personali
- «Violazione di integrità» - dove c'è un'alterazione accidentale o non autorizzata dei dati personali.
- «Violazione di disponibilità» - dove c'è una perdita accidentale o non autorizzata di accesso[2] a, o distruzione dei dati personali.

Si deve inoltre osservare che, a seconda delle circostanze, una violazione può interessare la riservatezza, l'integrità e la disponibilità dei dati personali al tempo stesso, come pure qualsiasi combinazione di questi.
Considerando che la determinazione se ci sia stata una violazione della riservatezza o integrità è relativamente chiara, potrebbe essere meno evidente se vi sia stata una violazione di disponibilità. Una violazione sarà sempre considerata come una violazione di disponibilità quando c'è stata una perdita permanente o distruzione dei dati personali.

[1] Si veda il parere 03/2014

[2] È ben stabilito che il "accesso" fondamentalmente è parte della "disponibilità". Vedi, per esempio, NIST SP800 - 53rev4, che definisce "disponibilità" come: "Garantire la tempestivo e affidabile accesso e l'utilizzo di informazioni," disponibile presso http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 si riferisce anche a: "La proprietà di essere accessibile e utilizzabile su richiesta da un ente autorizzato". Vedi https://RMF.org/images/4-CNSS-Publications/CNSSI-4009.pdf ISO/IEC 27000:2016 definisce anche "disponibilità" come "Proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata": https://www.ISO.org/OBP/UI/#ISO:std:iso-iec:27000:ed-4:v1: it

6.3. Gestione degli incidenti informatici

L'organizzazione deve classificare gli incidenti definendone la codifica preventiva e la gestione degli stessi.
Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

1. **Rilevazione** – si scopre l'esistenza di un evento critico e dell'incidente informatico. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni della Direzione e del personale autorizzato all'utilizzo dei software;
2. **Identificazione**/classificazione - si raccolgono i dati relativi all'incidente informatico, si individuano gli elementi utili a classificare nel dettaglio il tipo di incidente informatico, vengono riconosciuti uno o più eventi di sicurezza come incidente e ad ogni incidente viene assegnato un livello di gravità;
3. **Raccolta prove** informatiche **-** si mettono in atto le tecniche di informatica forense per l'acquisizione forense dei dati informatici utili a provare cosa è accaduto, ovvero cosa è successo, quando, chi ha determinato l'incidente, quali sono stati gli effetti;
4. **Analisi dei dati raccolti** - sia per scopi di informatica forense che a fini di riattivazione sicura dei sistemi;
5. **Segnalazione al Garante** (se dovuta) - Quando un titolare del trattamento notifica una violazione all'autorità di vigilanza, l'articolo 33, paragrafo 3 stabilisce che, al minimo, dovrebbe:
   a) descrivere la natura dei dati personali della violazione e ove possibile, le categorie e numero approssimativo di persone interessate e le categorie e il numero approssimativo di record di dati personali interessati;
   b) comunicare il nome e recapiti del responsabile della protezione dei dati o altro punto di contatto dove e possono ottenere ulteriori informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o proposte da adottare con il titolare del trattamento per affrontare i dati personali violazione, compreso, ove opportuno, misure per mitigare i possibili effetti negativi.
   e) fornire informazioni all'autorità di vigilanza.

Intanto, dopo il punto 4), vanno avviate le seguenti fasi:

6. **Contenimento** - vengono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll-back dopo la successiva fase di eliminazione;
7. **Eliminazione** - vengono eliminate le cause che hanno portato al verificarsi dell'incidente;
8. **Ripristino** - si rimettono in funzione in maniera sicura i sistemi coinvolti dall'incidente e vengono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento;
9. **Follow-up – Si valuta se la risposta all'incidente è stata adeguata,** cosa non ha funzionato e si lavora per ridurre i rischi o migliorare l'approccio all'incidente, verificando l'adeguatezza delle procedure di gestione degli incidenti e identificando i possibili punti di miglioramento.

6.4 Documentare le violazioni

Indipendentemente dal fatto o meno che una violazione debba essere notificata all'autorità di vigilanza, il titolare del trattamento deve conservare una documentazione di tutte le violazioni, come l'articolo 33, paragrafo 5 spiega:
"Il titolare del trattamento deve documentare eventuali violazioni di dati personali, comprendenti i fatti riguardanti le violazione dei dati personali, i loro effetti e le misure correttive adottate. Tale documentazione deve consentire alla autorità di vigilanza di verificare la conformità con il presente articolo."

Come prevede l'articolo 33, paragrafo 5, il titolare del trattamento deve registrare i dettagli concernenti la violazione, che comprenda le cause, che cosa è avvenuto e i dati personali interessati nonché gli effetti e le conseguenze della violazione, insieme con le misure correttive adottate dal titolare del trattamento.
Il GDPR non specifica un periodo di conservazione per tale documentazione, ma quando tali record contengano dati personali, è incombente sul titolare del trattamento determinare il periodo appropriato di conservazione in conformità con i principi, in relazione al trattamento dei dati personali[3] e per soddisfare una legittima base per l'elaborazione[4].
In particolare, se non viene notificata una violazione, una giustificazione per quella decisione deve essere documentata. In questo caso il titolare del trattamento dovrà includere i motivi perché il titolare del trattamento ritiene la violazione è improbabile che causi un rischio per i diritti e le libertà degli individui[5].
In alternativa, se il titolare del trattamento ritiene che le condizioni nell'articolo 34, paragrafo 3 siano soddisfatte, allora dovrà essere in grado di fornire adeguate prove che questo è il caso.
Dove il titolare del trattamento notifica una violazione all'autorità di vigilanza, ma la notifica è in ritardo, il titolare del trattamento deve essere in grado di fornire ragioni per quel ritardo; documentazione relativa a questo potrebbe aiutare per dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo. Ove il titolare del trattamento comunica una violazione agli individui colpiti, dovrebbe essere trasparente sulla violazione e comunicare in modo efficace e tempestivo. Di conseguenza, sarebbe d'aiuto al titolare del trattamento per dimostrare responsabilità e conformità, conservare prove di tale comunicazione.
Per facilitare la conformità con gli articoli 33 e 34, è opportuno, per il titolare del trattamento ed i responsabili, avere una **procedura di notifica documentata in luogo**, che stabilisce il processo da seguire una volta che sia stata rilevata una violazione, compreso il modo di contenere, gestire e recuperare l'incidente, così come la valutazione del rischio e la notifica della violazione[6].
A questo proposito, per dimostrare la conformità con GDPR potrebbe anche essere utile dimostrare che **i dipendenti sono stati informati circa l'esistenza di tali procedure e meccanismi e che sanno come reagire alle violazioni**. Dovrebbe essere notato che l'omissione di documentare correttamente una violazione può condurre all'autorità di vigilanza all'esercizio dei suoi poteri ai sensi dell'articolo 58 e, o l'imposizione di una sanzione amministrativa in conformità con Articolo 83.

In particolare, se una violazione non viene notificata, il titolare del trattamento deve giustificare e documentare il perché della decisione, adducendo i motivi che lo inducono a ritenere che la violazione è improbabile che causi un rischio per i diritti e le libertà degli individui[7].
Ugualmente, quando il titolare del trattamento ritenga che le condizioni nell'articolo 34, paragrafo 3 siano soddisfatte, dovrà essere in grado di fornire adeguate prove a supporto del caso.
Se il titolare del trattamento notifica in ritardo una violazione all'autorità di vigilanza deve documentarne le motivazioni, per dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo.
Il titolare del trattamento comunica una eventuale violazione, agli individui colpiti, tempestivamente, in maniera trasparente, ed efficace, conservando le prove di tale comunicazione per dimostrare responsabilità e conformità agli articoli 33 e 34.
Per facilitare questa conformità il titolare del trattamento ha predisposto una **procedura di notifica documentata in luogo** (alleg. 1), che stabilisce il processo da seguire quando venisse rilevata una violazione, come contenere, gestire e recuperare l'incidente, come valutare il rischio e quando notificare la violazione[8].
A questo proposito, per dimostrare la conformità con GDPR, il titolare del trattamento **ha informato tutti i**

[3] Cfr. articolo 5
[4] Vedi articolo 6 e l'articolo 9.
[5] Cfr. considerando 85
[6] Vedi linee guida WP29
[7] Cfr. considerando 85
[8] Vedi linee guida WP29

dipendenti che la Fondazione Onlus Longini Morelli Sironi ha adottato specifiche procedure e meccanismi per contenere le violazioni; grazie alla conoscenza di queste norme, perciò, tutti i dipendenti sono in grado di reagire correttamente in presenza di eventuali violazioni.

Bisogna sottolineare che non documentare correttamente una violazione può condurre all'autorità di vigilanza all'esercizio dei suoi poteri ai sensi dell'articolo 58 e, o, l'imposizione di una sanzione amministrativa in conformità con Articolo 83.

Flow chart del processo