Roma,
Ottobre, 2025

Politica di risposta agli incidenti che coinvolgono i Dati Personali

DMA–DigitalMadeAccessible

Documento di Indirizzo e Standard Amministrativi

INTRODUZIONE

La presente Politica mira a preparare il DMA ad affrontare la gestione degli incidenti di sicurezza, garantendo una risposta rapida, organizzata ed efficiente, minimizzandone le conseguenze per tutti i soggetti coinvolti.

Il livello di risposta dipenderà dal tipo di dati personali interessati e dalla complessità del trattamento applicato. Ai fini della presente Informativa, per incidente si intende qualsiasi situazione imprevista in grado di alterare il normale ordine delle operazioni e, nel contesto della protezione dei dati, di mettere a rischio le informazioni personali delle persone che si riferiscono al DMA.

Il National Institute of Standards and Technology (NIST) definisce un incidente di sicurezza come una violazione o una minaccia di violazione della politica di sicurezza informatica, della politica di utilizzo accettabile o degli standard delle pratiche di sicurezza.

In conformità con il Regolamento generale sulla protezione dei dati dell'Unione Europea (GDPR – Regolamento UE 2016/679), i titolari e i responsabili del trattamento devono adottare misure tecniche e organizzative adeguate per proteggere i dati personali da accessi non autorizzati e da situazioni accidentali o illecite di distruzione, perdita, alterazione, divulgazione o qualsiasi altra forma di trattamento inappropriato.

Ai sensi dell'articolo 33 del GDPR, la legge sui dati digitali notificherà all'autorità di controllo competente qualsiasi violazione dei dati personali che possa comportare un rischio per i diritti e le libertà delle persone fisiche. Ai sensi dell'articolo 34 del GDPR, quando l'incidente è suscettibile di comportare un rischio elevato, la comunicazione sarà estesa anche agli interessati, in modo chiaro, trasparente e tempestivo, includendo, come minimo:

- una descrizione della natura dei dati personali interessati;
- informazioni sugli interessati coinvolti, ove possibile;
- l'indicazione delle misure tecniche e organizzative applicate per la protezione dei dati;
- la descrizione dei rischi connessi all'incidente;
- le misure adottate o previste per attenuare gli effetti dell'incidente.

Sulla base di quanto sopra, la politica di risposta agli incidenti del DMA seguirà un processo strutturato, che include le fasi di prevenzione, identificazione, contenimento, eradicazione, recupero e comunicazione.

Questi passaggi sono illustrati nella figura seguente e dettagliati nella sequenza di questo documento, fungendo da riferimento ufficiale per le prestazioni del DMA in situazioni di incidenti di sicurezza.

Figura 1: Fasi di Risposta agli Incidenti

Consiste nell'identificare, prevenire e descrivere possibili situazioni di violazione dei dati, nonché le rispettive azioni che verranno intraprese, le scadenze e le forme di registrazione, assicurandosi che, in situazioni reali, sia preventivamente delineato un piano d'azione. Il piano deve contenere almeno:

- la previsione di possibili situazioni di incidente nonché le forme di
- il monitoraggio e le azioni da intraprendere in caso di verifica;
- la definizione dell'area che deve essere informata in caso di insorgenza del
- reclamo e modalità di segnalazione;
- l'individuazione dettagliata delle azioni necessarie tenendo conto della criticità
- evento.

Esempio di detalhamento de incidente:

2. IDENTIFICAZIONE

È la definizione di criteri per rilevare, identificare e registrare le situazioni di incidente e descrivere le risorse utilizzate per identificare gli avvisi di sicurezza e attivare i team responsabili in modo che vengano prese le misure necessarie. Saranno valutate tutte le possibili fonti che potrebbero rappresentare una minaccia per la protezione dei dati. Di seguito sono riportate alcune situazioni che saranno considerate sospette:

- Ricezione di e-mail con caratteri e/o file allegati

Sospetti;

- Comportamento inappropriato del dispositivo;
- Problemi di accesso a determinati file o servizi;
- Furto di dispositivi di archiviazione o computer con
- informazione;
- Avviso software antivirus;
- Consumo eccessivo e improvviso di memoria su server o
- Elaboratori;
- Traffico di rete insolito;
- Connessioni bloccate dal firewall;
- Analisi dei log dei tentativi di accesso non autorizzati ai server;

Anche le situazioni di mancato rispetto delle procedure interne possono comportare rischi per la sicurezza dei dati personali, per cui il rispetto del Codice di Condotta Etica e della Politica sulla Privacy e sulla Protezione dei Dati è estremamente importante. Tutti i dipendenti, i fornitori di servizi, i fornitori e i partner di DMA sono responsabili della segnalazione di qualsiasi tipo di evento e punto debole che possa causare danni alla sicurezza delle informazioni. La segnalazione deve essere registrata via e-mail al Responsabile della protezione dei dati o tramite il Portale dell'interessato, disponibile sul sito web e negli ambienti virtuali aziendali.

2.1 CATEGORIE DI VIOLAZIONE DELLA SICUREZZA

La violazione della sicurezza sarà classificata tra le seguenti categorie:

a. Fisico: quando l'incidente coinvolge dati memorizzati su dispositivi fisici. Esempi: perdita di supporti dati, smarrimento di cartelle di file, furto o smarrimento di laptop, smartphone o altri dispositivi mobili.

b. Divulgazione non autorizzata: quando si verifica una fuga di dati attraverso comunicazioni verbali o scritte, sia per indiscrezione (commenti su dati personali percepiti da terzi e utilizzati in malafede) sia per trasmissione intenzionale e impropria di informazioni riservate.

c. Cyber: quando l'incidente è correlato a sistemi o tecnologie informatiche. Esempi: attacchi di hacker, gestione impropria delle patch, errori di codifica, misure di sicurezza insufficienti o altri eventi simili.

2.2 VALUTAZIONE DELLE CRITICITÀ PER LA SICUREZZA

Alcuni fattori sono determinanti per definire la criticità di un incidente di sicurezza dei dati personali. Nell'ambito del DMA, gli incidenti saranno valutati in base ai seguenti criteri:

I. Categoria di criticità: In generale, l'incidente sarà classificato in una delle seguenti categorie:

Basso rischio: quando l'incidente riguarda solo dati personali comuni (ad esempio, nome, indirizzo, contatti), senza l'esposizione di identificatori forti o categorie speciali di dati.

Rischio moderato: quando l'incidente riguarda dati personali che includono identificatori forti (ad esempio, numero di passaporto, codice fiscale, numero del documento d'identità nazionale) o

almeno un dato appartenente a categorie speciali di dati, ai sensi dell'articolo 9 del GDPR (ad esempio, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, dati relativi alla salute o alla vita sessuale, dati biometrici o genetici).

Alto Rischio: quando l'incidente interessa più categorie particolari di dati o comporta la possibilità di grave lesione dei diritti e delle libertà dei soggetti, tra cui il rischio di discriminazione, frode di identità, danno reputazionale o perdita significativa di riservatezza.

II. Dati leggibili/illeggibili: se i dati sono stati protetti da misure come la pseudonimizzazione o la crittografia.

III. Volume di dati personali interessati: numero di registri, file o documenti interessati, considerando la proroga temporale (ad esempio, un giorno, una settimana, un anno).

IV. Facilità di identificazione delle persone: grado di possibilità di reidentificazione delle persone sulla base dei dati interessati.

V. Individui con caratteristiche particolari: se l'incidente colpisce gruppi vulnerabili o protetti, come minori, anziani, pazienti o persone in situazioni di fragilità sociale.

VI. Numero totale di individui colpiti: valutati in base alla scala di impatto, ad esempio, sopra i 100 interessati.

3. CONTENIMENTO

Dopo l'identificazione di un incidente caratterizzato come violazione della sicurezza dei dati personali, il DMA procederà al suo immediato contenimento al fine di prevenire la propagazione ad altri sistemi o il verificarsi di ulteriori danni. Saranno pianificate azioni a breve termine, come l'isolamento del sistema e la creazione di copie di backup, e azioni a lungo termine, come la revisione strutturale e il rafforzamento dei controlli di sicurezza. Durante il contenimento, tutte le registrazioni dell'incidente e le misure adottate devono essere documentate, garantendo la conservazione delle prove necessarie per ulteriori indagini.

- **Titolare del trattamento:** una volta identificato l'incidente di sicurezza dei dati personali, l'area responsabile deve informare immediatamente il Responsabile della **protezione dei dati (DPO)** e avviare azioni di contenimento.
- **Responsabile del trattamento:** gli operatori dei dati, compresi i partner e i fornitori che elaborano i dati per conto di DMA, hanno l'obbligo di segnalare immediatamente qualsiasi incidente di sicurezza al Titolare del trattamento e al DPO.
- **Responsabile della protezione dei dati (DPO):** dopo essere stato informato, il DPO supporterà la valutazione dell'incidente, verificherà l'esistenza di un piano d'azione applicabile e garantirà la corretta documentazione del caso. Nel caso in cui risulti accertata la possibilità di una fuga di dati personali che possa comportare un rischio per gli interessati, il Titolare provvederà a darne comunicazione all'Autorità di controllo competente (art. 33 del GDPR) e, ove applicabile, agli interessati (art. 34 del GDPR).

4. ERADICAZIONE

Dopo aver contenuto la minaccia, il DMA intraprenderà sforzi strutturati per sradicare completamente la causa principale dell'incidente, eliminando le vulnerabilità tecniche, i fallimenti organizzativi o le debolezze procedurali che ne hanno reso possibile il verificarsi. Questo passaggio può includere:

- rimozione di software dannosi, accessi non autorizzati o configurazioni improprie;
- correzione di guasti nei sistemi, nei processi o nei controlli interni;
- applicazione di patch di sicurezza o aggiornamenti critici;
- Revoca delle credenziali compromesse o reimpostazione delle autorizzazioni di accesso.

Tutte le misure adottate saranno documentate, con l'obiettivo non solo di ripristinare l'operatività, ma anche di rafforzare i meccanismi di prevenzione, nel rispetto dell'articolo 32 del GDPR sull'integrità, la riservatezza e la resilienza dei sistemi.

5. RECUPERO

Una volta terminata la fase di eradicazione, DMA procederà con il ripristino in sicurezza dei sistemi interessati, garantendo che tornino a operare in un ambiente di produzione stabile e affidabile. Questo passaggio includerà:

- validazione tecnica dell'integrità dei sistemi e dei dati ripristinati;
- esecuzione di test e audit di sicurezza per confermare la standardizzazione;
- un monitoraggio rafforzato nel periodo successivo, per individuare eventuali segni di persistenza o ricorrenza della minaccia;
- comunicazione strutturata agli interessati e all'autorità di controllo, ove previsto dagli articoli 33 e 34 del GDPR.

La responsabilità del coordinamento di questa fase sarà affidata al Titolare, con il supporto tecnico delle aree coinvolte e il monitoraggio da parte del DPO, che garantirà il rispetto normativo e l'adeguata documentazione delle azioni.

6. LEZIONI APPRESE

Tutti gli incidenti di sicurezza saranno soggetti a registrazione dettagliata e valutazione critica, al fine di mantenere uno storico completo degli eventi e delle risposte adottate. Questa fase comprenderà:

- preparazione di un rapporto post-incidente, contenente la descrizione dell'evento, la sua origine, gli impatti, le misure di contenimento, eradicazione e recupero applicate;
- analisi dell'efficacia delle misure messe in atto e dei fallimenti che hanno permesso l'incidente;
- raccomandazione di miglioramenti tecnici, procedurali e organizzativi;
- aggiornare i piani di risposta agli incidenti, le politiche interne e le misure di sicurezza applicabili;

- formazione e sensibilizzazione delle équipe coinvolte, per rafforzare la cultura della sicurezza e della prevenzione.

Questo processo di "lezioni apprese" sarà condotto in conformità con i principi di responsabilità del GDPR, al fine di dimostrare che il DMA adotta meccanismi proattivi e continui per la mitigazione del rischio e la protezione dei dati personali.