Incaricato cantonale della protezione dei dati
6501 Bellinzona
www.ti.ch/protezionedati

22.03.2023

Procedura in caso di violazione della sicurezza dei dati

1. Violazione della sicurezza dei dati

Una violazione della sicurezza dei dati è data quando, illecitamente o involontariamente, dati personali vengono persi, cancellati, distrutti o modificati oppure quando vengono divulgati o resi accessibili a persone non autorizzate.

Esempi di violazione della sicurezza dei dati:

- Prelievo/furto di dati personali in seguito a un cyber-attacco da parte di hackers
- Perdita o furto di supporti di dati quali chiavi USB, laptop, tablet, disco rigido
- Trasmissione di dati a persone non autorizzate a riceverli
- Punti di vulnerabilità in un sistema

2. Competenze

I collaboratori, i fornitori di prestazioni IT o terzi segnalano al più presto possibile i casi di violazione della sicurezza dei dati effettivi o incombenti al funzionario dirigente o al mandante, i quali a loro volta informano l'IT e il responsabile interno della protezione dei dati. Segnalano in particolare il tipo di incidente di sicurezza, le categorie di dati e il numero di persone interessate, la data e l'orario dell'incidente e della costatazione.

Qualora un incidente che coinvolge dati personali mette a repentaglio i diritti fondamentali, in particolare il diritto all'autodeterminazione informativa e il diritto alla protezione della sfera privata, il titolare dell'elaborazione di dati (non il mandatario) segnala la violazione della sicurezza all'Incaricato cantonale della protezione dei dati. La segnalazione deve essere presentata anche qualora sussistano dubbi sul fatto che i diritti fondamentali siano a rischio (vedi obbligo di segnalazione di un incidente che coinvolge dati personali: https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Spiegazioni__Segnalazione_DatiPersonali.pdf).

I fattori che determinano la gravità del rischio per i diritti delle persone interessate sono:

- Tipo di violazione della sicurezza
- Sensibilità dei dati (ad esempio, dati di persone minorenni)
- Facilità di identificazione di persone
- Cerchia delle persone interessate e numero delle categorie di dati interessate
- Combinazione tra gravità degli effetti sui diritti e probabilità della ripetizione della violazione

3. Misure di sicurezza

Più è probabile una violazione della sicurezza dei dati e più sono gravi le conseguenze per le persone interessate, più sono elevati i requisiti per le misure di sicurezza da implementare (sulle misure di sicurezza, vedi: https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/TEMI/Guida_alle_misure_tecniche_e_organizzative_della_sicurezza_dei_dati.pdf).

Le misure di sicurezza vanno determinate in funzione della necessità di protezione dei dati e del rischio di violazione. La necessità di protezione dei dati viene valutata secondo i criteri della tipologia di dati trattati e dello scopo, del tipo e della portata dell'elaborazione. Il rischio di violazione dei dati viene valutato secondo i criteri delle cause dei rischi e dei principali pericoli (identificazione del rischio), delle misure di sicurezza intraprese o pianificate e della probabilità e della gravità di una violazione della sicurezza dei dati malgrado le misure intraprese o pianificate.

4. Avvenimenti (cause) alla base di un rischio per la sicurezza dei dati

Possibili cause di un rischio sono:

- Elaborazione illecita o illegale
- Elaborazione contraria alla buona fede
- Divulgazione o accesso illecito a dati
- Perdita, distruzione o danneggiamento involontario di dati

5. Pericoli che possono portare a una violazione della sicurezza dei dati

Possibili pericoli sono:

- Perdita del controllo su dati personali
- Rimozione illecita della pseudonimizzazione
- Violazione di una norma di confidenzialità (segreto professionale, segreto fiscale, segreto dell'assistenza sociale, ecc.)
- Importanti svantaggi economici o sociali

6. Ripristino della sicurezza dei dati

- Cambiare la parola chiave
- Garantire che i dati siano stati liberati da possibili Malware
- Analizzare accessi di hackers a banche dati sensibili
- Valutare la sicurezza dei dati
- Attualizzare le Policies di sicurezza
- Prendere in considerazione vie legali
- Ecc.