LINEE GUIDA SULLA

"VIOLAZIONE DEI DATI PERSONALI"

Procedura da adottare in caso di violazione dei dati personali o personal data breach

1.0 -Anno 2019

Università degli studi di Catania
Direzione generale
Ufficio per la protezione dei dati

SOMMARIO

1 - Cos'è *il data breach* o violazione dei dati personali

La violazione dei dati personali *data breach,* definita dal Regolamento europeo 2016/679 (GDPR), è*:*

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.

La violazione di dati personali è quindi, un incidente di sicurezza, involontario o doloso, nel quale possono essere coinvolti qualsiasi genere di dati di natura personale, sia dati personali comuni (es. dati anagrafici, codici identificativi) che categorie particolari di dati (es. dati inerenti la salute, dati biometrici o genetici, appartenenza a organizzazioni sindacali, orientamento sessuale, appartenenza a razze o etnie, dati giudiziari ecc.).

2. Tipologie di *data breach*

Le violazioni di dati personali sono classificate in base ai seguenti principi della sicurezza delle informazioni:

"**violazione della riservatezza":** in caso di divulgazione o accesso ai dati personali non autorizzato o accidentale;

"violazione dell'integrità": in caso di alterazione non autorizzata o accidentale dei dati personali;

"violazione della disponibilità": in caso di perdita, accesso o distruzione accidentale o non autorizzata di dati personali.

A seconda delle circostanze, una violazione può riguardare la riservatezza, l'integrità o la disponibilità dei dati personali, ma anche qualsiasi combinazione delle stesse.

Un *data breach* può essere un attacco informatico, ma può essere anche un accesso abusivo o un incidente (es. un incendio o una calamità naturale).

Allo scopo di contestualizzare il riconoscimento di un *data breach* si riportano alcuni casi a titolo esemplificativo ma non esaustivo:

- Furto o smarrimento di chiavetta USB o *smartphone o tablet* o *hard disk* su cui sono memorizzati dati personali non cifrati;
- Furto di credenziali di autenticazione a seguito di un attacco di *phishing;*
- Eliminazione accidentale o pubblicazione indesiderata su internet di dati personali;
- Comunicazione di dati personali ad errato destinatario;
- Accesso ad informazioni riservate da parte di utenti non autorizzati;
- Sottrazione di documenti con dati personali.

3. Perché una procedura

Una violazione di dati personali può avere potenzialmente numerosi effetti negativi rilevanti sulle persone fisiche, i quali possono causare danni fisici, materiali o immateriali e conseguentemente deve essere affrontata e gestita nel più breve tempo possibile.

Il GDPR impone al Titolare del trattamento, entro 72 ore dal momento in cui ne viene a conoscenza, di notificare la violazione al Garante per la protezione dei dati personali. Qualora questa comporti un rischio elevato per i diritti delle persone, il Titolare deve comunicarla anche a tutti coloro i cui dati personali sono stati interessati dalla violazione, utilizzando i canali più idonei.

La procedura a seguire è predisposta per documentare le attività per la gestione delle violazioni di dati personali, per:

- valutare se l'incidente possa causare danni ai diritti e alle libertà dei soggetti coinvolti nella violazione dei dati (interessati);
- notificare, nei tempi e nei modi previsti dalla normativa, all'Autorità garante e/o agli interessati dell'avvenuta violazione dei dati personali;

- evitare di incorrere nelle sanzioni previste dalla normativa per omessa notifica;
- porre in atto misure per minimizzare l'impatto della violazione ed evitare che possa ripetersi.

4. Qual è l'ambito di applicazione

Questa procedura si applica a qualunque attività di trattamento di dati personali svolta dal Titolare del trattamento con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi accessibili via web o contenuti su dispositivi mobili o portatili attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.

5. A chi si rivolge la procedura

La procedura di violazione di dati personali è rivolta a tutti coloro che, a qualsiasi titolo, trattano dati personali di competenza del Titolare del trattamento e il suo rispetto è obbligatorio.

6. Cosa fare in caso di *data breach*

Il personale di Ateneo, **appena viene a conoscenza** di una concreta, potenziale o sospetta violazione dei dati personali, dovrà segnalarla immediatamente.

In particolare il segnalante dovrà:

1) raccogliere le informazioni necessarie all'individuazione della violazione;
2) compilare il modulo predisposto di **RILEVAZIONE E SEGNALAZIONE *DATA BREACH*** (all.1);
3) comunicare e trasmettere al Responsabile interno del trattamento, **nel più breve tempo possibile e utilizzando le vie più brevi** (persona, e mail), il modulo **RILEVAZIONE E SEGNALAZIONE *DATA BREACH*** (all.1).

Il Responsabile interno del trattamento, ne prende atto ed è tenuto senza ingiustificato ritardo, possibilmente entro le 24 ore dal momento in cui ne è venuto a conoscenza, a:

1) intraprendere eventuali azioni contenitive e correttive del danno (da riportare al Responsabile della protezione dei dati – RPD), e qualora sia possibile, mettere immediatamente in atto misure contenitive del danno derivato dalla violazione dei dati personali
2) inviare il modulo di RILEVAZIONE E SEGNALAZIONE *DATA BREACH* con le osservazioni, a:
   - Responsabile della protezione dei dati **rpd@unict.it**
   - Ufficio per la protezione dei dati **privacy@unict.it**

7. Valutazione del rischio

La normativa non considera la valutazione del rischio quale attività propedeutica alla notifica al Garante, ma è anche vero che senza la valutazione non sarebbe possibile stimare il rischio a cui si è andati incontro ed individuare l'esigenza di procedere o meno alla notifica all'Autorità garante.

Il Responsabile della protezione dei dati, di concerto con il Responsabile interno alla struttura in cui si è verificata la violazione presunta e/o con il Dirigente dell'Area dei sistemi informativi (qualora i dati fossero contenuti in sistemi informatici), appena ricevuta la comunicazione effettua la valutazione del rischio, anche a fine di identificare eventuali obblighi di notifica e/o comunicazione.

Al termine della valutazione preliminare, l'Ateneo si considera "venuto a conoscenza" della violazione e, conseguentemente, da tale momento inizieranno a decorrere i termini per la eventuale notifica e comunicazione.

8. Individuazioni azioni correttive

A seguito degli esiti della valutazione dei rischi, il Responsabile della protezione dei dati, di concerto con il Responsabile interno del trattamento e il Dirigente dell'Area dei servizi informativi (qualora siano coinvolti sistemi informatici), individuerà le azioni correttive e preventive per evitare il ripresentarsi del rischio.

9. Comunicazione della valutazione e delle azioni da intraprendere

Il Responsabile della protezione dei dati e il Responsabile interno del trattamento stileranno una relazione nella quale saranno descritte l'incidente di sicurezza, le categorie di interessati, i dati personali coinvolti, gli esiti della valutazione del rischio e le azioni correttive e preventive da mettere in atto per evitare che si ripeta la violazione.

10. La notifica al Garante

L'Ateneo, per mezzo del Responsabile della protezione dei dati, ricevute le informazioni ed effettuate le valutazioni di rischio, entro le 72 ore successive, qualora fosse necessario, notifica al Garante la violazione dei dati personali attraverso il **MODULO DI NOTIFICA AL GARANTE** (ALL.3).

La notifica al Garante non è dovuta qualora sia "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".

11. Comunicazione agli interessati

Qualora la violazione comporti un rischio elevato per i diritti delle persone, a meno che abbia già preso misure tali da ridurne l'impatto, l'Ateneo per mezzo del Responsabile interno del trattamento, nel più breve tempo possibile, attraverso il **MODULO DI COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO** (all.2), informa i singoli interessati, ossia le persone fisiche i cui dati sono stati violati, che si è verificato un data breach dei loro dati

personali e sulle possibili conseguenze, con eventuali consigli e azioni da tenere per poter attenuare i potenziali effetti negativi che potrebbero derivare dalla violazione.

La comunicazione dovrà essere effettuata, attraverso i mezzi che vengono abitualmente utilizzati per le comunicazioni con i soggetti interessati (via e-mail, tramite sms, etc...).

La comunicazione deve essere individuale e compiuta per iscritto con un "linguaggio semplice e chiaro".

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

− il Titolare del trattamento ha messo in atto misure di sicurezza tecniche e organizzative adeguate e tali misure sono state applicate ai dati personali oggetto della violazione;

- il Titolare del trattamento ha adottato, successivamente all'incidente, misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

− la comunicazione richiederebbe sforzi sproporzionati; in tal caso, si procede attraverso una comunicazione pubblica (banner o post su sito internet, pubblicazione di annuncio sul giornale, etc...) purché gli interessati ne siano informati con uguale efficacia del fatto che si è verificato un *data breach*.

12. Documentazione delle violazioni

L'Ateneo è obbligato alla tenuta del Registro delle violazioni che deve essere mantenuto aggiornato e contenere le informazioni relative ad ogni *data breach*, le sue conseguenze, i provvedimenti adottati per porvi rimedio e tutta la relativa documentazione, nella misura in cui può essere chiamato a fornire prove all'Autorità di controllo.

Pertanto, concluse le fasi precedenti il responsabile interno del trattamento dovrà inserire all'interno del **REGISTRO DELLE VIOLAZIONI** (All.4) tutte le informazioni richieste e conservarne la documentazione.

ALLEGATI

All.1 Modulo di rilevazione e segnalazione della violazione dei dati personali.

All.2 Modulo di comunicazione della violazione all'interessato.

All.3 Modulo di notifica al Garante.

All.4 Registro delle violazioni dei dati personali

Vers.1.0 - 2019