PROCEDURA DI NOTIFICAZIONE

IN CASO DI VIOLAZIONE DEI DATI PERSONALI (Data Breach)

L'art. 33 del Regolamento UE 679/16 disciplina la notifica delle violazioni di dati personali all'autorità di controllo.

Principio cardine del Reg. UE 679/16 è quello della responsabilizzazione. Pertanto il Titolare del trattamento (*controller*) deve dimostrare di aver adottate tutte le misure tecniche ed organizzative per far fronte a violazioni di dati personali che comportino un rischio per i diritti e le libertà fondamentali dell'individuo.

Si configura una violazione nei casi di:

- accesso non autorizzato o effettuato in modo illecito, ai dati;
- perdita accidentale, distruzione, alterazione, trasmissione non autorizzata dei dati;

Può verificarsi violazione della riservatezza (*confidentiality breach*) se c'è una divulgazione accidentale o non autorizzata; violazione dell'integrità *(integrity*) se c'è alterazione di dati; indisponibilità del dato (*availability*) se c'è perdita accidentale o illecita dei dati (in questo caso bisogna distinguere se la perdita è temporanea o permanente).

Il danno può essere di tipo materiale o immateriale (danno economico, alla reputazione, all'identità sessuale ecc.)

Il riferimento ai diritti e alle libertà personali riguarda principalmente i diritti alla protezione dei dati e alla vita privata, la libertà di parola, di pensiero, di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Quando notificare all'autorità di controllo?

Il Titolare del trattamento deve provvedere entro 72 ore da quando viene a conoscenza DIRETTA, o PER COMUNICAZIONE del Responsabile esterno (Processor) o per COMUNICAZIONE DELL'INTERESSATO, della violazione.

L'eventuale ritardo va motivato.

Come comunicare al Titolare la violazione?

Colui che ritiene sia stata perpetrata una violazione di dati personali che mette a rischio diritti e libertà fondamentali dell'interessato, deve informare con immediatezza il Responsabile Protezione Dati (RPD o

DPO – Data Protection Officer) di Ateneo trasmettendo nota nella quale dichiara:

- le proprie generalità
- natura della violazione
- Paese in cui si è verificata la violazione (Italia, UE, EXTRA UE)
- quando ha rilevato la violazione (giorno, mese, anno e ora)
- circostanze in cui ha rilevato la violazione
- tipologia specifica della violazione (comunicazione accidentale, distruzione, violazione di sistemi automatizzati, ecc.)
- categorie di dati oggetto della violazione
- misure adottate nell'immediatezza

Deve altresì procedere con la compilazione del modulo MOD/A per la notificazione e segnalazione data breach scaricabile sul sito d'Ateneo https://www.unimib.it/ateneo/protezione-dei-dati-personali nella sezione PROCEDURA DATA BREACH.

Il Titolare, ricevuta la segnalazione ed annessa documentazione debitamente compilata, tramite il RPD deve procedere alla valutazione del rischio e, in presenza dei requisiti previsti dal Regolamento, a notificare al Garante la violazione indicando tutte le informazioni previste nell'art. 33 del GDPR oltre alle possibili conseguenze derivanti dalla violazione stessa.

Il Titolare del trattamento notifica a ciascun interessato la violazione salvo:

- siano state adottate le misure per mettere in sicurezza i dati (ad esempio cifratura)
- siano adottate misure per scongiurare il pericolo di limitazione libertà e diritti persone fisiche
- la comunicazione individuale sia troppo onerosa.

Se l'evento si verifica nelle Aree, la comunicazione della violazione va data al Referente d'Area o al Capo Area, che devono trasmettere subito notizia via mail al RPD.

Nei Dipartimenti, nel caso in cui la violazione sia stata accertata da docenti, va data comunicazione al Referente di Dipartimento o al Direttore del Dipartimento, che devono trasmettere subito notizia via mail al RPD.