DATA BREACH

Per **violazione dei dati personali (***data breach*) si intende la divulgazione (intenzionale o meno), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da una pubblica amministrazione (art. 4, comma 2 del Regolamento UE 679/2016, dôora in poi GDPR). Un *data breach*, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali.

Procedura da seguire in caso di data breach

Ogni incaricato del trattamento che si accorga o rilevi (cd. ñscopertaò) che si è verificato un evento tra quelli prima descritti ne dà **immediata comunicazione** via mail al DPO (dpo.privacy@uniparthenope.it) e per conoscenza al Responsabile della struttura coinvolta, indicando i dati coinvolti e descrivendo lôevento secondo la seguente tipologia:

- **Violazione di riservatezza**, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- **Violazione di integrità**, ovvero quando si verifica unôalterazione di dati personali non autorizzata o accidentale;
- **Violazione di disponibilità**, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali;

Università degli Studi di Napoli "Parthenope"
Sede legale: Via Amm. F. Acton, 38 – 80133 – Napoli – ITALIA
P.IVA 01877320638
C.F. 80018240632

-

La comunicazione deve altresì:

a) descrivere la natura della violazione dei dati personali indicando, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare, se ne è a conoscenza, il nome e i dati di contatto del responsabile del trattamento o di chiunque altro possa fornire elementi utili alla valutazione;

c) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

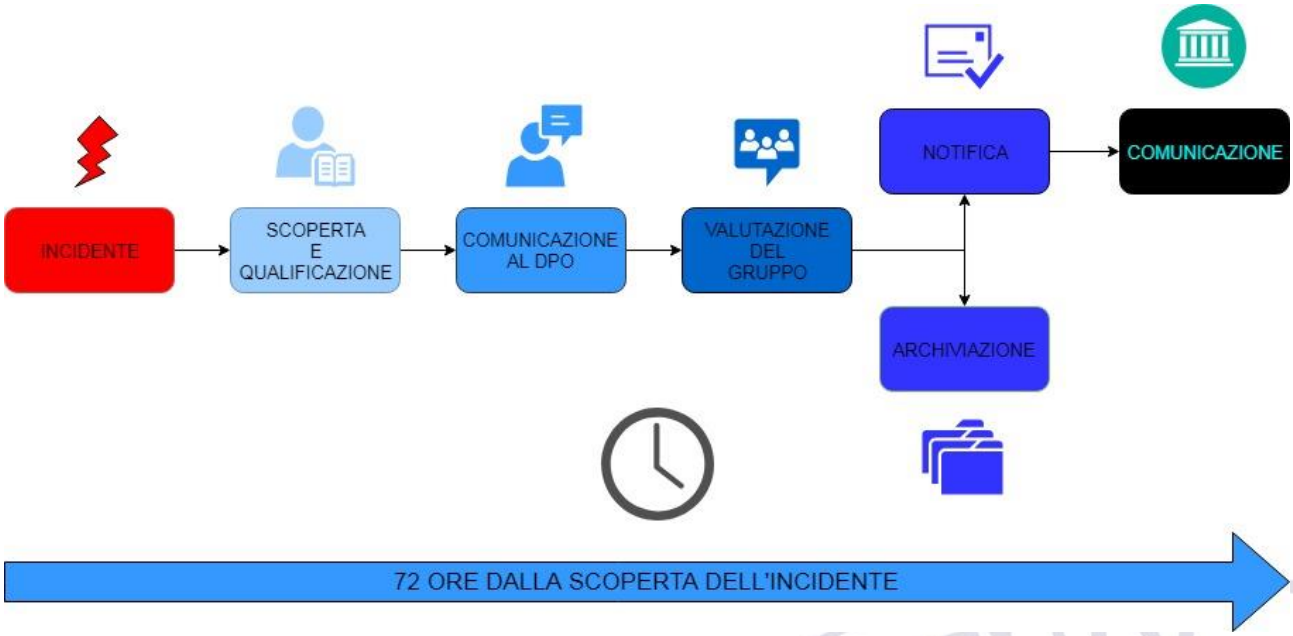
Il DPO inoltra al gruppo di lavoro la comunicazione della violazione al fine di avviare la conseguente valutazione delle conseguenze dellôevento sulla tutela dei diritti e delle libertà delle persone alle quali i dati appartengono.

Entro 72 ore dalla scoperta dellôevento, il DPO e il gruppo di lavoro possono:

- Decidere lôarchiviazione della segnalazione, dandone contezza in ogni caso nel registro delle violazioni;
- Chiedere al Rettore, nella sua qualificazione di ñTitolare del trattamentoò, di notificare al Garante privacy lôavvenuta violazione di dati personali (art. 33 GDPR). Nel caso in cui la violazione venga qualificata dal DPO come suscettibile di produrre un rischio elevato per i diritti e le libertà delle persone, ne viene data contestuale ñcomunicazioneò agli interessati, al fine di consentire a questi ultimi lôadozione di ogni precauzione per ridurre al minimo il potenziale danno derivante dalla violazione dei dati (art. 34 del GDPR).

Università degli Studi di Napoli "Parthenope"
Sede legale: Via Amm. F. Acton, 38 – 80133 – Napoli – ITALIA
P.IVA 01877320638
C.F. 80018240632

Tutto il processo che va dalla scoperta dell'incidente all'eventuale notifica al Garante Privacy può essere riassunto nel seguente schema:



Si raccomanda a tutti gli incaricati del trattamento di provvedere con la massima sollecitudine alla comunicazione al DPO dell'evento dal momento che, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore dalla scoperta dell'evento, dovranno essere esplicitati i motivi del ritardo, anche al fine di non incorrere nelle sanzioni previste dal DGPR.

Università degli Studi di Napoli "Parthenope"
Sede legale: Via Amm. F. Acton, 38 – 80133 – Napoli – ITALIA
P.IVA 01877320638
C.F. 80018240632

La notifica al Garante Privacy deve contenere, ai sensi dellôart. 33 del GDPR:

a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) la descrizione delle probabili conseguenze della violazione dei dati personali;

d) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione agli interessati, ai sensi dellôart. 34 del GDPR, contiene le seguenti informazioni:

a) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

b) la descrizione delle probabili conseguenze della violazione dei dati personali;

c) la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui sopra;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Università degli Studi di Napoli "Parthenope"
Sede legale: Via Amm. F. Acton, 38 – 80133 – Napoli – ITALIA
P.IVA 01877320638
C.F. 80018240632

Eô istituito il registro dei *data breach* nel quale verranno documentate le violazioni di dati personali eventualmente verificatesi, anche se non comunicate alle autorità di controllo, lôesito delle ulteriori verifiche nonché le conseguenze e i provvedimenti adottati. Nel registro verranno documentate anche le ragioni delle decisioni assunte, al fine di poterle produrre, su richiesta al Garante, nei casi in cui non ha proceduto alla notifica, lôha ritardata e nei casi in cui non ha ritenuto necessaria la comunicazione della violazione agli interessati. La tenuta del registro dei *data breach*, così come quella del registro dei trattamenti, è a cura del DPO di Ateneo.

Università degli Studi di Napoli "Parthenope"
Sede legale: Via Amm. F. Acton, 38 – 80133 – Napoli – ITALIA
P.IVA 01877320638
C.F. 80018240632