https://www.agendadigitale.eu/sicurezza/data-breach-nel-gdpr-cose-e-cosa-sapere-per-segnalazione-e-prevenzione/, 19-11-2018

Cos’è il data breach nel Gdpr

Per data breach, nella versione italiana **violazione dei** dati personali si intende 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. Sempre secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, **entro 72 ore**, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L’eventuale ritardo dovrà essere motivato.

Indice degli argomenti

L’obbligo di notifica

A tale proposito, è stato introdotto dall’articolo 33, l’obbligo generalizzato, in capo al titolare del trattamento di notifica di data breach **all’autorità di controllo (DPO)** competente a norma dell’art. 55 **GDPR** e ss., ovvero l’Autorità di controllo dello stabilimento principale o dello stabilimento unico del Titolare interessato dalla violazione o quello ove vi siano gli interessati alla violazione. Le informazioni minime da inserire nella notifica sono incluse nell’art. 33, la DPA competente fornirà una modulistica on line richiedendo informazioni obbligatorie. Tale documentazione consente all’Autorità di controllo di verificare il rispetto delle prescrizioni.

Come dev’essere la notifica di Data breach

La **notifica** deve:

- descrivere la 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;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni
- descrivere le probabili conseguenze delle violazioni dei dati personali

- 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, per attenuarne i possibili effetti negativi.

In Italia prima dell'approvazione del Regolamento erano già presenti obblighi di notifica in 4 fattispecie di trattamento:

- Settore comunicazioni elettroniche (Prov. Garante 161/2013)
- Biometria (Provv. Garante 513/2014)
- Dati sanitari inseriti in Dossier (Provv. Garante 331/2015)
- Dati comunicati fra PA (Provv. Garante 393/2015)

La comunicazione di data breach art. 34 (violazione dei dati personali all'interessato)

Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione. Tale comunicazione non è richiesta all'interessato se:

- il titolare del trattamento ha messo in atto le misure tecniche ed 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;
- 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;

Detta comunicazione richiederebbe sforzi sproporzionati. In tale caso, si procede invece a una comunicazione pubblica o a una misura simile.

La gestione del data breach

Per prevenire, gestire e risolvere episodi di perdita e/o distruzione dei dati personali è necessario:

- Adottare un protocollo di risposta;
- Effettuare test periodici per controllare la validità del protocollo;
- Ottenere una copertura assicurativa per eventuali casi di data breach;
- Tenere un registro dei casi di data breach;

- Compiere attività di indagine per individuare la natura e la portata della violazione.

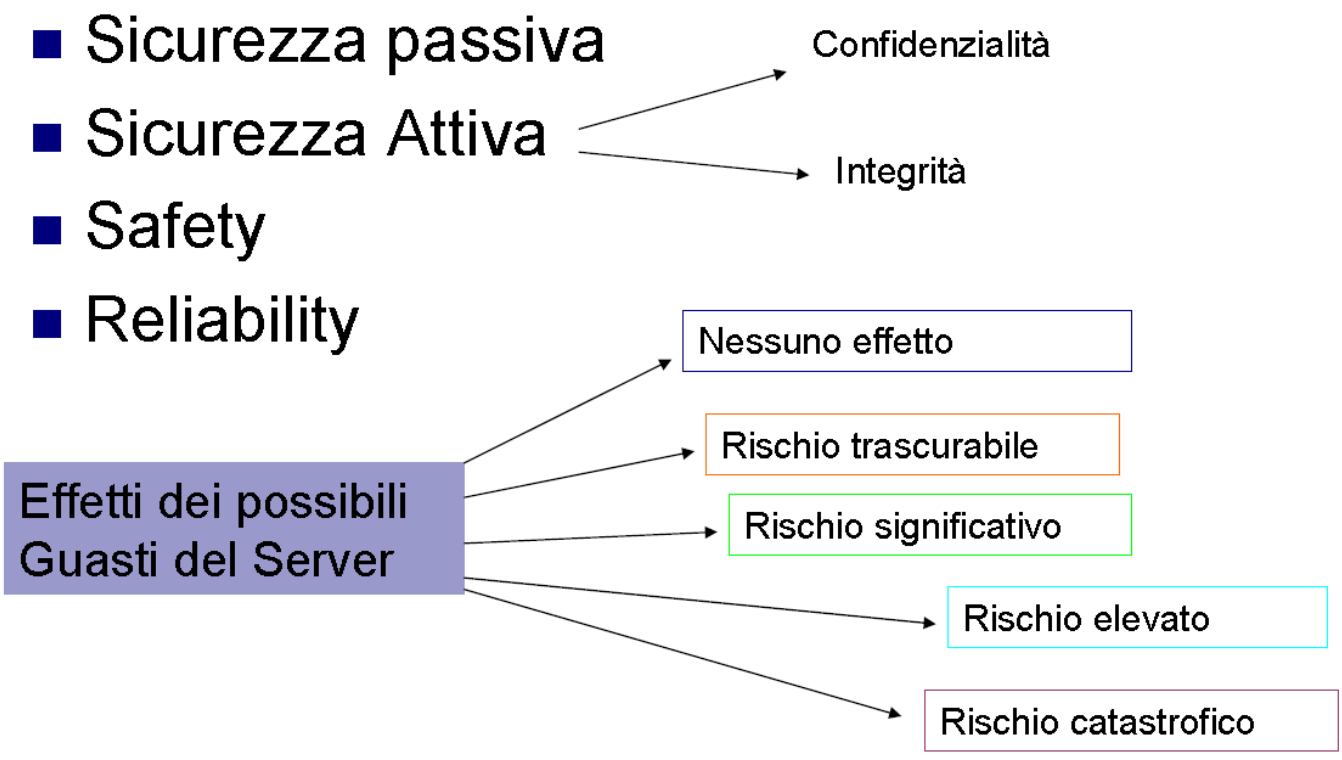
Il protocollo di risposta

Il Titolare del trattamento deve adottare un protocollo di risposta, ossia procedure da seguire per gestire e risolvere eventuali episodi di distruzione e/o perdita di dati. L'adozione del protocollo coinvolge numerose dipartimenti aziendali e strutture pubbliche quali ministeri, asp, etc. Questo protocollo dovrà indicare un modo coerente, sistematico e proattivo per gestire questi incidenti che coinvolgono i dati personali. Per la soluzione di questi incidenti l'azienda/ente pubblico potrà farsi coadiuvare da terzi fornitori di servizi quali:

- Call center;
- Servizi di assistenza agli utenti e pubbliche relazioni;
- Sistemi di monitoraggio;
- Sistemi di risoluzione dei casi di furto di identità.

La sicurezza informatica contro il data breach

Al fine di prevenire una violazione di data breach è necessario utilizzare un modello di sicurezza informatica così strutturato:



Altri strumenti di prevenzione

- sviluppo e manutenzione di sistemi (System Development and Maintenance)
- Accertare che la sicurezza sia stata costruita all'interno delle operazioni di sistema;
- impedire la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione;
- proteggere la riservatezza l'autenticità e l'integrità delle in formazioni;
- accertarsi che le attività di progetto e supporto alle attività siano condotte in modo sicuro e per mantenere la sicurezza del software e dei dati del sistema;
- gestione continuità operativa (Business Continuity Management);
- Neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari e dagli effetti dei guasti;
- adeguatezza (Compliance);
- Evitare il mancato rispetto delle leggi civili, penali e di qualsiasi requisito di sicurezza;
- Per elevare l'efficacia e minimizzare l'interferenza per il processo di verifica del sistema;

Effettuare test periodici

È importante condurre regolarmente dei test di verifica del protocollo adottato per garantire che le procedure seguite dall'Azienda per prevenire e risolvere casi di data breach siano efficienti e condotte da personale formato adeguatamente per implementare il protocollo. E' altresì, importante stipulare un'adeguata polizza assicurativa per assicurare l'Azienda contro il rischio di Data Breach ed ottenere indennizzo dalla Compagnia Assicuratrice in occorrenza di violazioni di dati. L'assicurazione risarcisce i costi che l'Azienda deve sostenere per riparare le conseguenze della violazione e può anche coprire le eventuali spese legali che l'Azienda dovrà affrontare.

Tenere un registro di data breach

Il DPO (Data Protection Officer) deve promuovere la tenuta di un Registro dei casi di data breach, sia dei casi di violazione effettivamente occorsi sia le minacce potenziali, per identificare il tipo e la natura delle violazioni più ricorrenti

Tracciare i casi di data breach

Il tracciamento dei casi di violazione dei dati personali viene effettuato allo scopo di:

- individuare e tenere sotto controllo i fattori di rischio, ossia i fattori che determinano con più frequenza una violazione dei dati personali

- Misurare l’efficacia delle policy e delle procedure adottate
- Elaborare un piano di conformità che fissi gli obiettivi da raggiungere per essere “compliant” rispetto a leggi, best practices, e che aiuti a dimostrare la conformità in sede di audit di verifica/ispezioni/test
- Indagini forensi e data breach
- Per gestire e risolvere i casi di data breach l’azienda/ente pubblico può stabilire al suo interno una funzione investigativa e demandare a personale interno indagini forensi “in house” e cioè siglare contratti con investigatori esterni ai quali demandare queste attività di indagine, compiere attività di indagine per individuare la natura e la portata della violazione. Le indagini investigative servono per:
- Determinare la natura e la portata della violazione
- Aiutare a prevenire ulteriori perdite di dati
- Conservare le prove della violazione in modo che possano essere usate anche in un’eventuale azione giudiziaria