Progettato e realizzato da

Commissionato da

CORSO GDPR - Regolamento UE 2016/679 - e sicurezza informatica

commissionato da Università degli Studi di Torino

realizzato e progettato da CSI Piemonte

Modulo 1 – Tecnologie e strumenti

Sommario

Obiettivi

In questa terza sezione dedicata alle novità del GDPR – ambito di intervento **Strumenti e Tecnologie** – analizziamo le seguenti tematiche:

- ✓ **Misure di sicurezza adeguate**
- ✓ **Data breach**

Torna al sommario

Misure di sicurezza (art. 32)

Si passa **dalle misure "minime" e "idonee"** del codice privacy **alle misure «adeguate»** per garantire un livello di sicurezza adeguato ai rischi.

Le misure devono essere discrezionalmente scelte tenuto conto:

- ✓ dello stato dell'arte e dei costi di attuazione
- ✓ della natura e dell'oggetto del trattamento
- ✓ del contesto e delle finalità
- ✓ dei rischi per i diritti e le libertà delle persone, in particolare: la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso accidentale o illegale ai dati trattati.

Le misure adeguate comprendono:

La pseudonimizzazione consiste nel trattamento dei dati personali in modo tale che **i dati personali non possano più essere attribuiti a un interessato specifico** senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a **garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.**

L'anonimizzazione consiste nel trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico in alcun modo.

La cifratura è quel processo che tramite applicazione di algoritmo matematico (basato su apposizione di una chiave simmetrica o asimmetrica) rende inintelligibili i dati a chi non è in possesso della chiave di cifratura.

La capacità di assicurare la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento.
La capacità di **ripristinare** tempestivamente la disponibilità e l'accesso ai dati personali, in caso di incidente fisico o tecnico.
Una procedura per **verificare regolarmente l'efficacia** delle misure.

Torna al sommario

Data breach

Data breach = violazione dei dati personali
*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" (*4 comma 1 n. 12, GDPR).
Il titolare deve documentare qualsiasi violazione di dati personali

Notifica di una violazione di dati personali (art. 33)

In caso di violazione di dati personali, il Titolare deve notificare la violazione all'Autorità di Controllo, senza giustificato ritardo e comunque **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone.
Se la violazione presenta **un rischio elevato** per i diritti e le libertà delle persone, il Titolare deve inoltre **notificare la violazione agli interessati.**

Contenuti della notifica

I contenuti della notifica all'autorità sono indicati, **in via non esclusiva, agli artt. 33 e 34 del regolamento**.

L'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico già dal 2013 ed intende rielaborarlo al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il GDPR.

Il Data breach era già normato dal Garante anche per i casi di: interscambio dati fra pubbliche amministrazione, trattamenti di dati biometrici e dossier sanitario elettronico.

La notifica agli interessati

La notifica agli interessati NON deve essere fatta se è soddisfatta una delle seguenti condizioni:

- ✓ le misure di sicurezza applicate sono adeguate (es. cifratura)
- ✓ sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato
- ✓ la comunicazione richiederebbe sforzi sproporzionati. In tal caso è prevista una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono informati
- ✓ la notifica agli interessati può essere richiesta anche dall'Autorità di controllo

Torna al sommario

Conclusioni

Bene! Hai concluso le sezioni dedicata a PERSONE E RUOLI, PROCESSI E DOCUMENTI e TECNOLOGIE E STRUMENTI.

Prosegui con il corso, puoi ora affrontare la sezione **Controlli.**

Torna al sommario