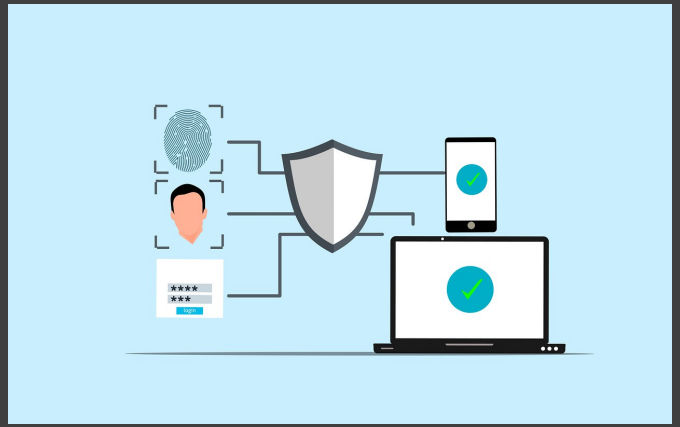
Data Protection & Security

Introduzione ai concetti fondamentali



Data Processing

Vuol dire intraprendere qualsiasi azione con i dati personali di qualcuno.
Ciò include:

- registrarli,
- conservarli,
- modificarli,
- utilizzarli,
- eliminarli

Principi GDPR

I dati personali devono:

- Essere trattati in modo lecito, equo e trasparente
- Essere utilizzati per uno scopo specifico
- Essere pertinenti a tale scopo
- Essere accurati
- Essere conservati non più a lungo del necessario
- Essere conservati in modo sicuro

Categorie di dati particolari

I dati di categoria “particolare” includono:

- origine razziale o etnica
- opinioni politiche
- credenze religiose o filosofiche
- appartenenza a sindacati
- informazioni genetiche
- informazioni biometriche (ad esempio, un'impronta digitale)
- questioni sanitarie (ad esempio, informazioni mediche)
- questioni sessuali o orientamento sessuale

Legittimità del Trattamento

Le basi giuridiche che legittimano il trattamento dei dati personali sono:

- Consenso
- Contratto
- Obbligo legale
- Interessi vitali
- Interesse pubblico
- Interessi legittimi

Informativa sul Trattamento

L’informativa resa all’interessato (persona fisica cui i dati personali si riferiscono) deve ricomprendere:

- quali informazioni personali stai condividendo
- perché le stai condividendo
- con chi le stai condividendo e per cosa le useranno
- come condividerai le loro informazioni e
- il processo per revocare il consenso

Diritti dell'interessato

Il Titolare del Trattamento deve consentire l'esercizio dei seguenti diritti:

- Accedere alle informazioni personali che possiedi su di loro, che è anche nota come Diritto di accesso
- Richiedere modificare informazioni personali inaccurate che possiedi su di loro
- Richiedere di rimuovere le loro informazioni personali o i loro record
- Richiedere di limitare l'elaborazione delle loro informazioni personali e
- Richiedere di interrompere l'elaborazione delle loro informazioni personali

Fonte Normativa

Il Regolamento UE n.679/2016 anche noto come GDPR, è entrato in vigore il 25 maggio 2018, rappresenta una fonte normativa dell'UE che rende le norme immediatamente applicabile all'interno dei paesi membri, a differenza delle Direttive, che richiedono un provvedimento normativo di adozione specifico da parte dei singoli Stati membri.

Attualmente il GDPR rappresenta la principale fonte normativa in materia di Data Protection

Principi generali GDPR

Principio di Proporzionalità

I dati che vengono raccolti e trattati devono essere **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati (cosiddetta “minimizzazione dei dati”)

Portabilità dei Dati

l’interessato ha il diritto di vedersi garantita la trasmissione diretta dei dati personali da un titolare all’altro, se tecnicamente fattibile, senza impedimenti

Principi generali GDPR

Privacy by Design
Il GDPR obbliga di assicurare che le misure adottate attuino efficacemente i principi normativi fin dalla fase della progettazione;

Privacy by Default
per impostazione predefinita, deve essere previsto che il trattamento si limiti ai soli dati necessari al perseguimento delle finalità dichiarate;

Consenso dell'interessato

Il consenso deve essere esplicito e prestato liberamente;

il GDPR richiede che l'interessato acconsenta al trattamento dei propri dati personali in maniera libera, specifica e inequivocabile;

Il consenso reso deve essere adeguatamente informato sul trattamento dei dati personali che lo riguardano

Modalità del trattamento

Le modalità di trattamento dei dati devono essere ispirate a:

- Liceità, correttezza e trasparenza
- finalità determinate, esplicite, legittime;
- dati trattati in modo non incompatibile con le finalità dichiarate
- I dati devono essere esatti e quindi aggiornati
- La loro conservazione non può essere superiore al tempo necessario alle finalità del trattamento
- Integrità e riservatezza
- Accountability - responsabilizzazione

Soggetti del trattamento

I soggetti del trattamento sono i seguenti:

- Interessati
- Titolare e Contitolari
- Responsabili
- Incaricati

N.B. Il DPO non è soggetto del Trattamento

Doveri del Titolare

Ha l'obbligo di trattare i dati rispettando i principi by default e by design;

quindi deve trattare meno dati personali possibili e proteggerli fin dall'inizio in modo adeguato, tenendo conto di tutte le tecnologie disponibili effettuando una **valutazione del rischio** associato al trattamento posto in essere;

su di esso incombe l'obbligo di progettare in maniera efficace il sistema di Data Protection del quale diventa **accountable** (ovvero è chiamato a rispondere delle decisioni organizzative adottate).