BIBLIOTECA

Il GDPR: cos'è e come si applica

Introduzione

In questo video vedremo insieme:

- cos'è il GDPR e qual è il suo scopo
- i dati personali, le tipologie e le tutele
- i princìpi fondamentali del GDPR
- come si applica il GDPR

Cos'è il GDPR

Dal 25 maggio 2018 è entrato in vigore un nuovo regolamento generale europeo sulla protezione dei dati, il GDPR (General Data Protection Regulation).

Il GDPR è un'unica serie di norme sulla protezione dei dati per tutte le imprese che operano nell'UE, indipendentemente dalla loro sede.

Lo scopo del GDPR

Scopo del GDPR è garantire:

- alle persone maggiore controllo sui loro dati personali
- alle imprese condizioni di parità e uniformità all'interno dell'UE

Definizione di dato personale

Ma che cos'è un dato personale?

Il GDPR definisce “dato personale” qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Il concetto di dati giudiziari

Il GDPR non parla più di “dati sensibili” ma introduce il concetto di “dati giudiziari” cioè categorie particolari di dati che rivelino:

- l'origine razziale o etnica
- le opinioni politiche
- le convinzioni religiose o filosofiche
- l'appartenenza sindacale
- i parametri genetici, biometrici (come l'impronta digitale) e relativi allo stato di salute
- l'orientamento e la vita sessuale
- le condanne penali, i reati e connesse misure di sicurezza

Tipologie di dati

Il GDPR considera 4 tipologie di dati:

- provided, cioè forniti consapevolmente dall'utente (ad esempio in fase di registrazione)
- observed, cioè desumibili dalla navigazione dell'utente
- derived, cioè derivati da una precedente raccolta (come ad esempio la profilazione)
- inferred, cioè aggregati su cui vengono fatte previsioni statistiche

Di tutti questi dati quelli che potrebbero sembrare più importanti sono quelli economici (come ad esempio il pin, l'IBAN, il numero di carta di credito) ma in realtà questi dati sono modificabili.

I dati maggiormente rilevati sono invece i nostri dati di navigazione, i nostri gusti, le nostre abitudini e addirittura i dati biometrici di uno smartwatch. Questi dati sono ancora più preziosi in quanto non modificabili.

I princìpi fondamentali del GDPR

Per proteggere questi dati l'applicazione del GDPR ottempera a 6 princìpi fondamentali:

- liceità, correttezza e trasparenza nei confronti dell'Interessato
- limitazione delle finalità (i dati devono cioè essere raccolti per finalità determinate, esplicite e legittime e trattati in base ad esse)
- minimizzazione dei dati che devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità dichiarate
- esattezza, ciò implica che i dati siano precisi ed aggiornati oppure tempestivamente rettificati o eliminati
- limitazione della conservazione che permette di conservare i dati solo per il tempo necessario alla finalità del trattamento
- integrità e riservatezza che devono tutelare i dati dalla diffusione, dalla perdita e dalla distruzione

Applicazione del GDPR

Vediamo ora come applicare concretamente il GDPR.

Per attuare correttamente le norme sancite dal GDPR il Titolare del trattamento deve fornire a ciascun Interessato un'informativa contenente tutti i dettagli relativi al trattamento dei dati personali.

L'informativa può essere fornita:

- in forma scritta (in formato cartaceo o elettronico)
- con altri mezzi, inclusa la forma orale

Caratteristiche dell'informativa

L'informativa deve essere:

- concisa
- trasparente
- intellegibile cioè con un linguaggio semplice e accessibile
- chiaramente differenziata dalle condizioni contrattuali
- comprensibile da un membro medio del pubblico di riferimento previsto

Contenuto dell'informativa

L'informativa deve contenere tutti i dettagli del trattamento e in particolare:

- l'identità e i dati di contatto del Titolare del trattamento, del suo Rappresentante e dell'eventuale Responsabile della protezione dei dati (il DPO)
- le finalità del trattamento e la base giuridica
- gli eventuali destinatari e categorie di destinatari dei dati personali
- l'intenzione del Titolare di trasferire i dati personali a un Paese extra UE o a un'organizzazione internazionale
- il periodo di conservazione dei dati personali
- l'esistenza dei diritti esercitabili dall'Interessato

Se i dati vengono raccolti presso terzi l'informativa deve contenere anche:

- le categorie dei dati personali trattati
- la fonte da cui hanno origine i dati e l'eventualità che provengano da fonti accessibili al pubblico.

Tempistiche dell'informativa

Se i dati sono raccolti direttamente presso l'Interessato l'informativa deve essere fornita contestualmente alla raccolta dei dati e prima del trattamento.

Se i dati NON sono raccolti presso l'Interessato l'informativa deve essere fornita in un tempo ragionevole e comunque non superiore ai 30 giorni successivi all'acquisizione.

Il consenso dell'Interessato

Una volta ricevuta l'informativa, l'Interessato può manifestare la sua volontà prestando il suo consenso al trattamento dei dati.

Il consenso deve essere sempre:

- libero, cioè privo di condizionamento
- informato, ovvero preceduto da un'informativa
- inequivocabile, deve esserci certezza che sia stato prestato
- specifico per ciascuna finalità

Il consenso non è obbligatorio e può essere revocato in ogni momento.

Il GDPR impone al Titolare del trattamento di dimostrare i consensi acquisiti. Per questo motivo tutti i presunti consensi dei quali non viene conservato un riferimento o basati su una forma di azione più implicita (come ad esempio una casella preselezionata) non sono conformi alla normativa e devono essere rinnovati.