BIBLIOTECA

GDPR: panoramica generale e novità

Introduzione

Ciao e benvenuto! In questa videopillola scopriamo insieme quali sono le novità e le principali norme introdotte dal GDPR attraverso una panoramica generale sul nuovo regolamento che disciplina il tema della privacy a livello europeo. Iniziamo!

Cos'è il GDPR

Come prima cosa capiamo cos'è il GDPR.

Il GDPR (General Data Protection Regulation) è un nuovo regolamento generale europeo sulla protezione dei dati.

È entrato in vigore dal 25 maggio 2018 e riguarda 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

Le tre grandi novità introdotte

Rispetto alle precedenti normative in tema di Privacy, il GDPR introduce, oltre all'uniformità a livello internazionale, tre fondamentali novità:

- il concetto di “privacy by design” e “privacy by default”
- il principio di “accountability”
- la designazione del Data Protection Officer (DPO)

Privacy by design e by default

Iniziamo analizzando i concetti di “privacy by design” e “privacy by default”.

Per “privacy by design” si intende che il Titolare del trattamento dei dati deve inserire la privacy nei processi e nell'organizzazione aziendale già nella fase di progettazione del processo.

La “privacy by default”, ovvero la protezione per impostazione predefinita, comporta che il trattamento sia limitato esclusivamente ai dati strettamente necessari alle singole specifiche finalità.

La “privacy by design” e la “privacy by default” sono due tra le più importanti misure tecniche che il Titolare del trattamento può mettere in atto per garantire un livello di sicurezza adeguato ai rischi che i dati personali corrono.

Il principio di “accountability”

Il GDPR cambia il precedente sistema formalistico introducendo la responsabilizzazione (accountability) del Titolare del trattamento dei dati.

Il Titolare (o controller) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento dei dati personali.

Il Titolare dei dati può decidere le modalità con cui uniformarsi al GDPR ma deve essere in grado di dimostrare attraverso un idoneo sistema documentale di gestione della privacy la conformità al DGPR e le motivazioni delle scelte effettuate.

Il Data Protection Officer (DPO)

Arriviamo ora a conoscere il Data Protection Officer (DPO).

Il DPO è il fulcro del nuovo sistema di governance in tema di protezione dei dati personali.

Il GDPR sancisce che sia obbligatoriamente nominato in tre casi:

1) se il trattamento dei dati è svolto da un'autorità pubblica o da un organismo pubblico

2) se l'attività principale del Titolare o del Responsabile consiste nel monitoraggio regolare e sistematico degli Interessati su larga scala

3) se il trattamento su larga scala è relativo a categorie particolari di dati o di dati relativi a condanne penali e reati

I compiti del DPO definiti per legge sono:

- controllare e supportare l'applicazione degli obblighi della nuova normativa, fornendo quando necessario anche la sua consulenza
- fungere da punto di contatto con le Autorità di controllo e gli Interessati per questioni connesse al trattamento

I princìpi fondamentali del GDPR

L'applicazione del GDPR ottempera a 6 princìpi fondamentali:

- liceità, correttezza e trasparenza nei confronti dell'Interessato
- limitazione della 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: informativa e consenso

Una volta conosciuti i princìpi fondamentali del GDPR e le novità introdotte vediamo ora come è possibile applicare concretamente il regolamento.

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.

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

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.

Liceità del trattamento

Una volta ottemperate tutte le misure organizzative e di sicurezza, i dati possono essere trattati secondo le condizioni di liceità sancite dal GDPR.

Affinché il trattamento dei dati sia lecito deve ricorrere almeno una delle seguenti condizioni:

- l'Interessato ha prestato il proprio consenso
- il trattamento è strettamente necessario all'esecuzione di un contratto o di misure pre-contrattuali di cui l'Interessato è parte
- il trattamento è necessario per adempiere a un obbligo legale di cui è soggetto il Titolare
- serve per salvaguardare interessi vitali dell'Interessato
- è necessario per l'esecuzione di compiti di interesse pubblico
- persegue un legittimo interesse del Titolare del trattamento a condizione che tale interesse legittimo sia perfettamente bilanciato con la libertà e i diritti dell'Interessato

Qualora non vengano ottemperati gli obblighi sanciti dal GDPR si può incorrere in sanzioni amministrative e in sanzioni penali.