iubenda

Introduzione al GDPR

Regolamento Generale sulla Protezione dei Dati

CHE COS'È IL GDPR E QUANDO SI APPLICA

GDPR sta per General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati) e, in estrema sintesi, chiarisce come i dati personali debbano essere trattati, incluse le modalità di raccolta, utilizzo, protezione e condivisione.

CHE COS'È IL GDPR E QUANDO SI APPLICA

Il GDPR si applica quando:

- la base operativa dell'organizzazione si trova nell'UE;
- l'organizzazione, seppure non avente sede nell'UE, offre beni o servizi (anche gratuitamente) a cittadini europei; o
- l'organizzazione, seppure non avente sede nell'UE, monitora il comportamento delle persone che vi risiedono, a patto che tale comportamento abbia luogo all'interno del territorio UE.

Un ambito di applicazione così ampio copre quasi tutte le attività, e pertanto si può concludere che il GDPR si applichi indipendentemente dal fatto che la tua organizzazione si trovi o meno nell'UE.

RUOLI DEFINITI DAL GDPR

Il GDPR definisce dei ruoli specifici per i soggetti coinvolti nel trattamento dei dati personali.

Utente/interessato

Un individuo i cui dati personali sono trattati da un titolare del trattamento o da un responsabile del trattamento.

Titolare del trattamento

Una qualsiasi persona fisica o giuridica coinvolta nella determinazione delle finalità e delle modalità del trattamento dei dati personali degli utenti.

Responsabile del trattamento

Una qualsiasi persona fisica o giuridica coinvolta nel trattamento dei dati personali degli utenti per conto del titolare del trattamento.

iubenda

RUOLI DEFINITI DAL GDPR

DPO (Responsabile per la Protezione dei Dati)

Una persona fisica o giuridica con una conoscenza approfondita della legislazione in materia di protezione dei dati, il cui ruolo comprende l'assistenza al titolare del trattamento o al responsabile del trattamento per il controllo della conformità interna al GDPR, e per la supervisione e l'attuazione della strategia di protezione dei dati. Il DPO è competente nella gestione dei processi informatici, nella sicurezza dei dati e in altre questioni critiche relative al trattamento di dati personali e sensibili.

Il DPO deve essere nominato quando c'è un monitoraggio regolare e sistematico degli interessati su larga scala, oppure l'organizzazione si occupa di attività di trattamento di dati sensibili o giudiziari, o quando il trattamento è effettuato da un'autorità o un organismo pubblico.

RUOLI DEFINITI DAL GDPR

Rappresentante nell'UE

Una persona fisica o giuridica che deve essere nominata quando il titolare del trattamento ha sede al di fuori dell'UE, ma offre beni o servizi (anche gratuitamente) a persone fisiche che si trovano nell'UE o monitora il loro comportamento posto in atto all'interno dell'UE.

BASI GIURIDICHE

Ai sensi del GDPR, i dati possono essere trattati solo se sussiste almeno una base giuridica del trattamento.

- Il **consenso** dell'utente per una o più specifiche finalità
- L'esecuzione di un **contratto** al quale l'utente ha aderito, o per intraprendere azioni preliminari alla stipula del contratto
- Un **obbligo di legge** al quale il titolare del trattamento è soggetto
- **Interesse legittimo** del titolare del trattamento o di terzi, a meno che non prevalgano gli interessi, i diritti e le libertà dell'utente (in particolare se l'utente è un minore)
- Il trattamento è necessario per la tutela di **interessi vitali** dell'utente o di terzi
- Il trattamento è necessario per l'esecuzione di un'attività di **interesse pubblico**, o che rientra nell'ambito dei poteri pubblici conferiti al titolare del trattamento

REQUISITI DEL CONSENSO

Quando la base giuridica per il trattamento dei dati è il consenso, il titolare del trattamento deve raccogliere un consenso **libero, specifico, esplicito e informato**.

Il GDPR inoltre pone in capo al titolare **l'onere di una prova inequivocabile** che dimostri di aver raccolto un consenso valido. Queste prove dei consensi devono contenere **informazioni specifiche** per essere considerate valide:

- **chi** ha prestato il consenso;
- **quando e come** è stato acquisito il consenso del singolo utente;
- il **modulo di raccolta** del consenso presentato all'utente in fase di raccolta dello stesso;
- un riferimento ai **documenti legali e alle condizioni** in essere nel momento in cui il consenso è stato acquisito.

DIRITTI DELL'UTENTE

Ai sensi del GDPR, gli utenti devono avere i seguenti diritti:

- Il diritto ad **essere informati**
- Il diritto di **accesso**
- Il diritto di **rettifica**
- Il diritto di **opporsi**
- Il diritto alla **portabilità dei dati**
- Il diritto alla **cancellazione**
- Il diritto a **limitare il trattamento**
- Diritti relativi ai **processi decisionali automatizzati ed alla profilazione**

TRASFERIMENTO DI DATI ALL'ESTERO

Il GDPR consente il trasferimento dei dati di cittadini UE al di fuori dello Spazio Economico Europeo (SEE) solo se sono soddisfatte determinate condizioni.

In particolare, il paese in cui i dati vengono trasferiti deve avere un livello "adeguato" di protezione dei dati personali, al pari degli standard europei.

In caso contrario, i trasferimenti possono comunque essere consentiti in presenza di clausole contrattuali standard (SCC) o di norme vincolanti d'impresa (BCR) o, in ultimo, qualora l'utente abbia espresso il proprio **consenso esplicito ed informato**.

REQUISITI DI CONFORMITÀ OFFLINE

Il GDPR ha impatti significativi anche a livello di privacy aziendale interna.
Ad esempio, richiede che il titolare del trattamento si occupi di:

- nominare i **responsabili del trattamento, i DPO e/o i rappresentanti nell'EU**;
- informare l'autorità di controllo in caso di **data breach**;
- mantenere un **registro del trattamento**;
- svolgere delle **valutazioni d'impatto sulla protezione dei dati** (DPIA).

REGISTRO DEL TRATTAMENTO

Il GDPR obbliga sia i titolari che i responsabili del trattamento a redigere e mantenere aggiornato un registro “completo e esaustivo” delle attività di trattamento dati effettuate.

Questo requisito si applica a tutte le organizzazioni che hanno più di 250 dipendenti, o ad organizzazioni con meno di 250 dipendenti se sussiste almeno **una** delle seguenti condizioni:

- il trattamento dati **non è occasionale**;
- il trattamento include **dati sensibili o “categorie speciali di dati”**; o
- il trattamento comporta un **rischio elevato** per i diritti e le libertà degli interessati.

Le casistiche di cui sopra coprono dunque quasi tutti i titolari e i responsabili del trattamento.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Una DPIA è una procedura adottata per aiutare il titolare ad ottemperare al GDPR in maniera effettiva e garantire che siano attuati i principi di responsabilizzazione, "privacy by design" e "privacy by default".

In generale, la DPIA è obbligatoria solo nei casi in cui l'attività di trattamento dei dati comporti un rischio elevato per gli interessati (ad esempio quando si introduce una nuova tecnologia di trattamento).

IUBENDA

iubenda è la soluzione più semplice, completa e professionale per adeguarsi alle leggi internazionali e alle normative sulla privacy

iubenda adotta un approccio a 360° per l'adeguamento alle normative.

Oltre 65.000 clienti in tutto il mondo hanno scelto le soluzioni software di iubenda per il rispetto di GDPR, Cookie Law, CCPA e di altre leggi internazionali.

iubenda offre un set completo di soluzioni SaaS che ti consentono di rispettare facilmente i requisiti sui cookie, di creare un registro dei consensi e di generare documenti personalizzati di Privacy e Cookie Policy e Termini e Condizioni.

GENERATORE DI PRIVACY & COOKIE POLICY

La soluzione per creare, gestire e aggiornare Privacy e Cookie Policy

√ PER GDPR √ PER CCPA

Genera e gestisci facilmente una Privacy e Cookie Policy professionale, aggiornata automaticamente, personalizzabile grazie ad oltre 1300 clausole, disponibile in 8 lingue, redatta da un team legale internazionale e allineata alle principali normative internazionali.

CONSENT SOLUTION

Tieni traccia dei consensi GDPR e documenta opt-in e opt-out CCPA

√ PER GDPR √ PER CCPA

Memorizza e gestisci prove del consenso, opt-in e opt-out ai sensi di GDPR e CCPA tenendo traccia di moduli di raccolta dati compilati e documenti legali accettati. Include un'intuitiva dashboard per accedere in qualsiasi momento all'archivio delle informazioni registrate.

INTERNAL PRIVACY MANAGEMENT

Documenta le attività di trattamento all'interno della tua organizzazione

√ PER GDPR

Genera un registro del trattamento tenendo traccia di tutte le attività di trattamento effettuate all'interno della tua organizzazione grazie ad oltre 1300 opzioni pre-configurate. Dividile per area, assegna responsabili e addetti, documenta le basi giuridiche e ogni altra informazione richiesta.

iubenda

www.iubenda.com - business@iubenda.com

Alcuni tra i nostri clienti:

Rai

GRUPPO MEDIASET

la Repubblica

LA STAMPA

MONDADORI

jobtome

ahrefs

ustmo

stickermule