iubenda

Introduction to GDPR

General Data Protection Regulation

WHAT IS THE **GDPR** AND WHERE DOES IT APPLY

GDPR stands for General Data Protection Regulation and, at its most basic, it specifies how personal data should be lawfully processed (including how it's collected, used, protected or interacted with in general).

WHAT IS THE **GDPR** AND WHERE DOES IT APPLY

The GDPR can apply where:

- an entity's base of operations is in the EU;
- an entity not established in the EU offers goods or services (even if the offer is for free) to people in the EU; or
- an entity is not established in the EU but it monitors the behaviour of people who are in the EU, provided that such behaviour takes place in the EU.

This scope effectively covers almost all companies and, therefore, means that the GDPR can apply to you whether your organization is based in the EU or not.

ROLES DEFINED BY THE GDPR

The GDPR defines specific roles for the subjects involved in the processing of personal data

User/data subject

An individual whose personal data is processed by a controller or processor.

Data controller

Any person or entity involved in determining the purpose and ways of processing the personal data.

Data processor

Any person or entity involved in processing personal data on behalf of the controller.

iubenda

ROLES DEFINED BY THE GDPR

DPO (Data Protection Officer)

A natural or legal person with expert knowledge of data protection law whose role includes assisting the controller or processor to monitor internal compliance with the GDPR and overseeing data protection strategy & implementation. The DPO should also be proficient in IT process management, data security and other critical issues surrounding the processing of personal and sensitive data.

Specifically, DPOs are appointed when there is large-scale systematic monitoring of users, if an organization is performing complex operations with sensitive user data or where the processing is carried out by a public authority.

ROLES DEFINED BY THE GDPR

EU-representative

A natural or legal person to be appointed when the controller is based outside of the EU, but offers goods or services (even for free) to EU-based users or monitors their behaviour as far as it's taking place within the EU.

LAWFUL BASES

Under the GDPR data can only be processed if there's at least one legal basis for doing so.

- User's **consent** for one or more specific purposes
- Performance of a **contract** or prior to entering the contract
- **Legal obligation** to which the data controller is subject
- **Legitimate interests** of the data controller or third-party except where overridden by the rights and freedoms of the user (and, in particular, minors)
- Data processing which is necessary for protecting the **vital interests** of a user or of another person
- Data processing which is in the **interest of the public** or as contained under the official authority given to the data controller

CONSENT REQUIREMENTS

When using consent as lawful basis of data processing, the data controller must collect **freely given, specific, explicit and informed consent**.

GDPR also places the **burden of proof** on the data controller which is explicitly required to demonstrate – **unambiguously** – proof that valid consent has been collected.

These consent proofs or records must contain **specific information** in order to be considered, including:

- **who** provided the consent;
- **when and how** consent was acquired from the individual user;
- the consent collection **form** they were presented with at the time of the collection;
- which **conditions and legal documents** were applicable at the time that the consent was acquired.

USER'S RIGHTS

Under the GDPR, users must have the following rights:

- The right to be **informed**
- The right to **access**
- The right to **rectification**
- The right to **object**
- The right to **data portability**
- The right to **erasure**
- The right to **restrict processing**
- Rights relating to **automated decision making and profiling**

CROSS-BORDER DATA TRANSFERS

The GDPR permits data transfers of EU resident data outside of the European Economic Area (EEA) only when in compliance with set conditions – i.e. the external country must have an “adequate” level of personal data protection by EU standards, or be transferred under the use of standard contractual clauses (SCCs), binding corporate rules (BCRs), or lastly, have explicit **informed** consent from the user.

OFFLINE COMPLIANCE DUTIES

GDPR has severe impacts on the internal company compliance level.
For instance, it requires the data controller to:

- appoint **data processors, DPOs and/or EU-representatives**;
- notify the Supervisory Authority in case of **data breach**;
- maintain **records of processing activities**;
- carry out **Data Protection Impact Assessments** (DPIAs).

RECORDS OF PROCESSING ACTIVITIES

The GDPR requires that both data controllers and data processors keep and maintain “full and extensive” up-to-date records of the particular data processing activities they are carrying out.

This requirement applies to organizations that have more than 250 employees, or organizations with fewer than 250 employees if their processing activities meet any **one** of the following conditions:

- the processing is **not occasional**;
- it involves **sensitive or special categories of data**; or
- it could result in a **risk** to the rights and freedoms of others.

This effectively covers almost all data controllers and processors

DATA PROCESSING IMPACT ASSESSMENT

A DPIA is a process used to help organizations comply effectively with the GDPR and ensure that the principles of accountability, privacy by design and privacy by default are put in practice.

The DPIA is mandatory in cases where data processing activity is likely to result in a high risk for users (this is particularly applicable when introducing new processing technologies).

ABOUT IUBENDA

iubenda is the most simple, complete and professional way to comply with international regulations & privacy laws

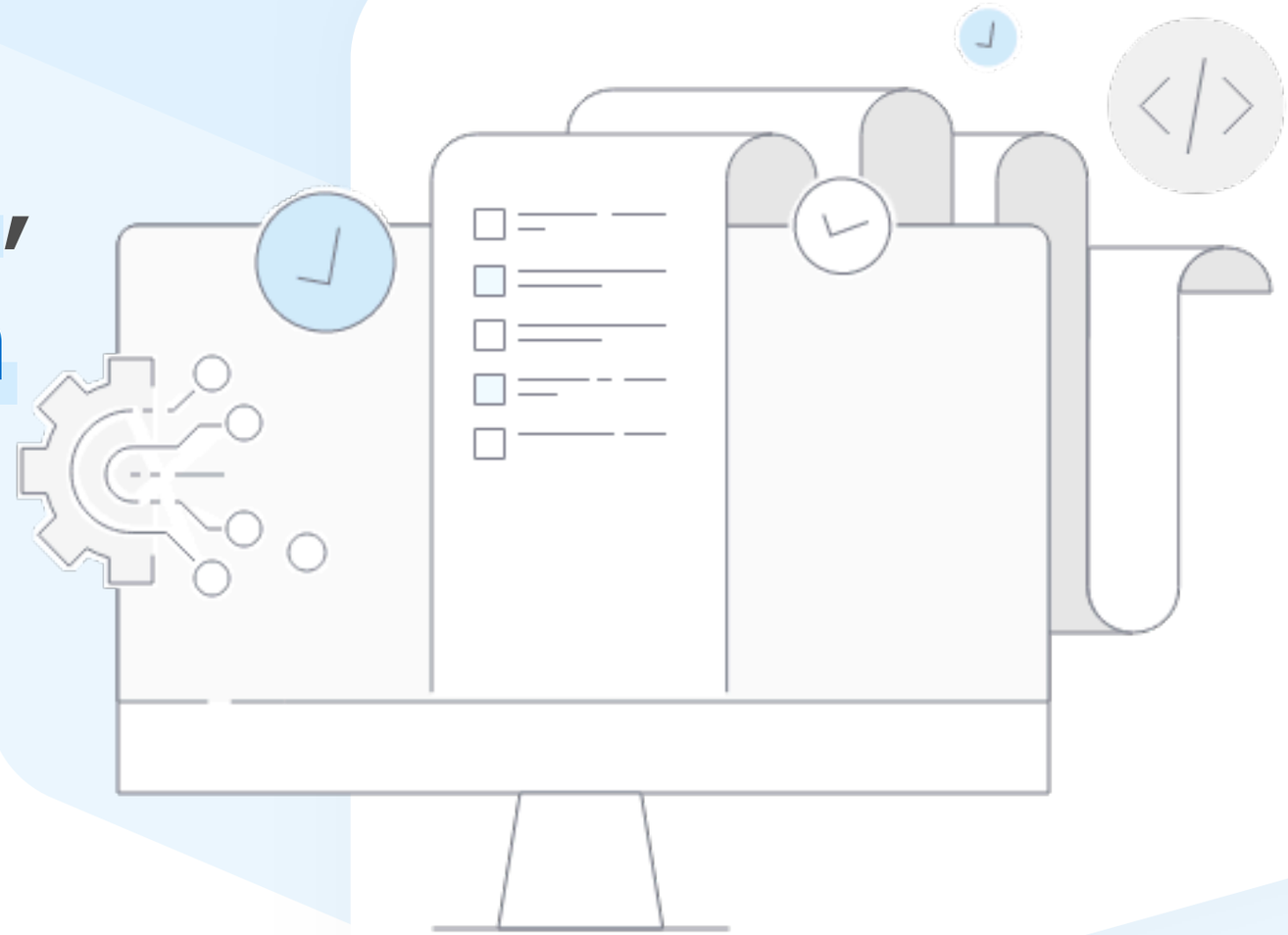
iubenda adopts a comprehensive approach to legal compliance.

More than 65,000 companies worldwide trust our solutions for compliance with the GDPR, EU Cookie Law, California's CCPA and other global privacy laws.

We offer a complete set of SaaS solutions which allows you to easily manage cookies, create consent records and generate customized Privacy Policies, Cookie Policies and Terms and Conditions.

IUBENDA PRIVACY & COOKIE POLICY GENERATOR

The solution to draft, update and maintain your Privacy and Cookie Policy



√ FOR GDPR √ FOR CCPA

Easily generate and manage a Privacy and Cookie Policy that is professional, self-updating and customizable from 1,000+ clauses, available in 8 languages, drafted by an international legal team and up to date with the main international legislations.

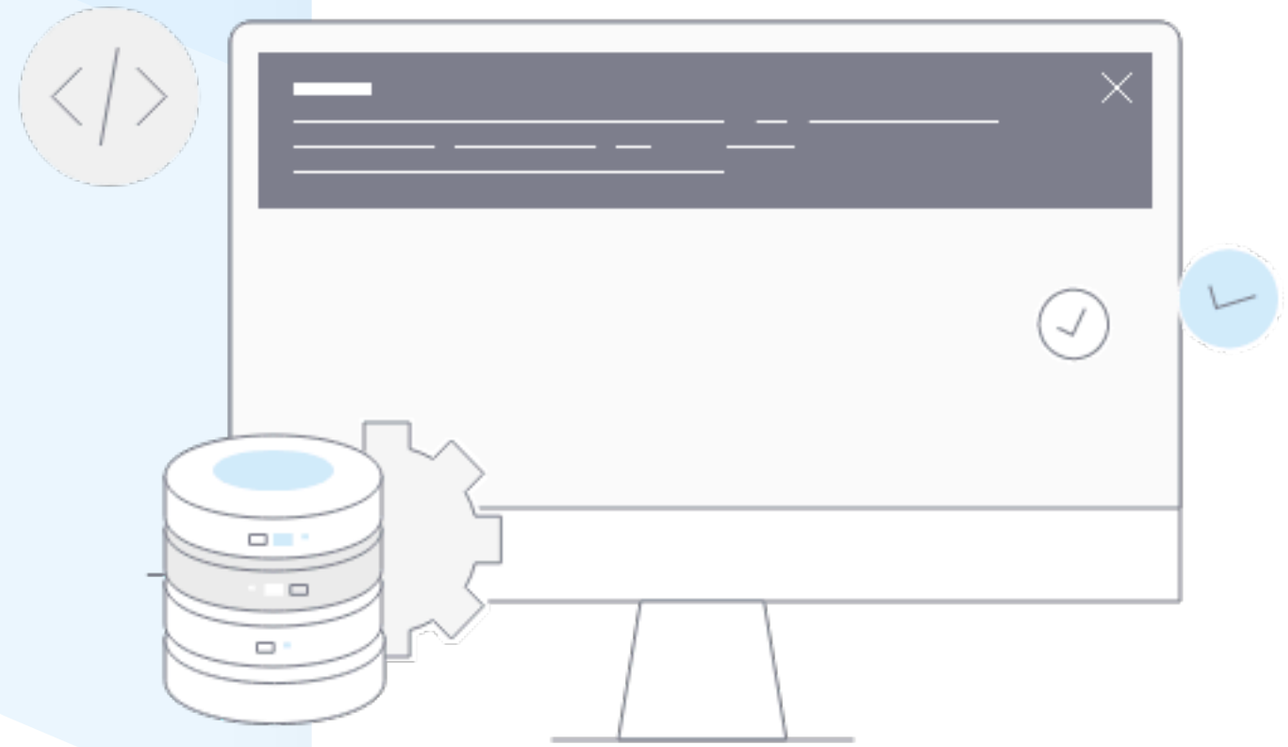
iubenda

www.iubenda.com - business@iubenda.com

IUBENDA COOKIE SOLUTION

Cookie consent management for ePrivacy, GDPR and CCPA

√ FOR GDPR √ FOR CCPA

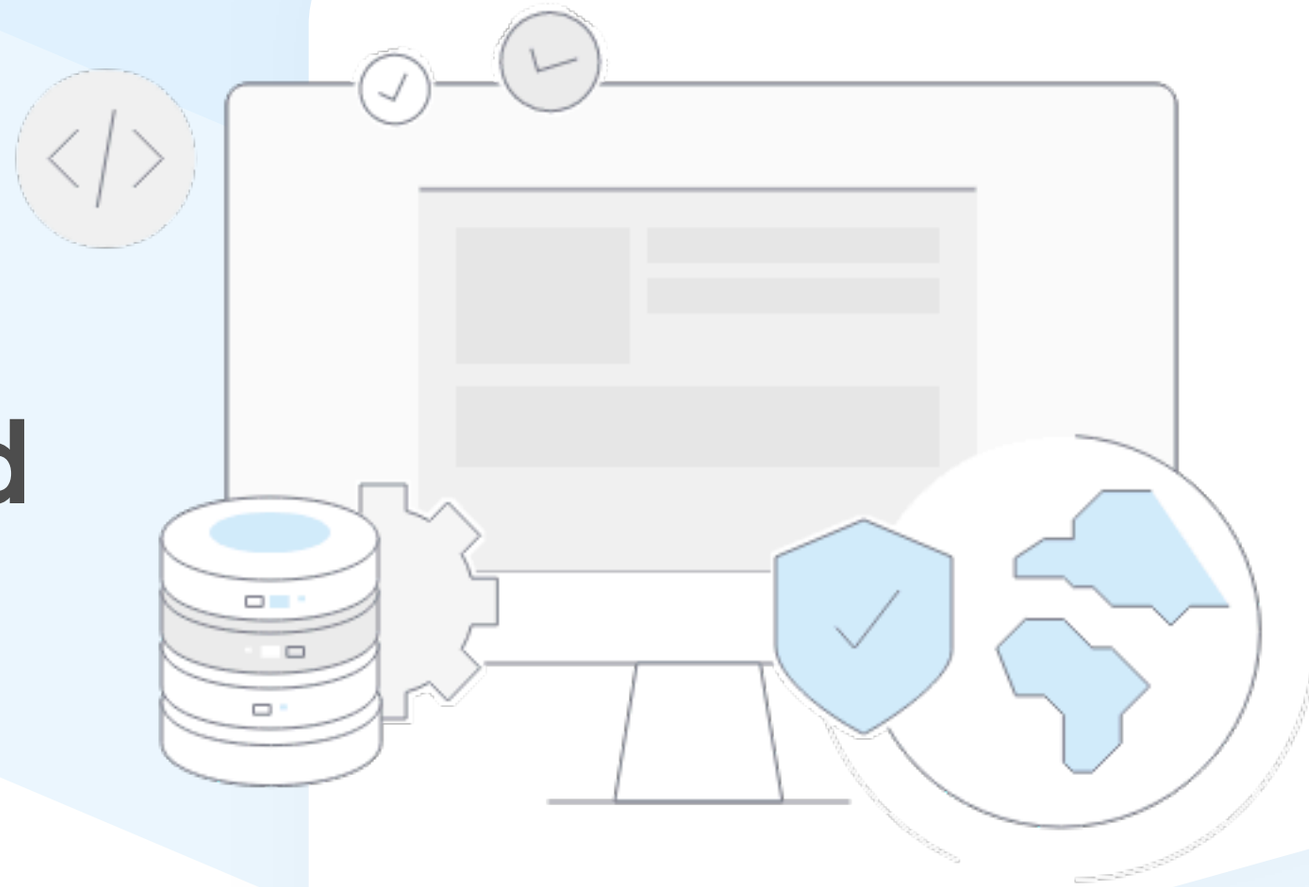


Easily generate a fully customizable cookie banner or a CCPA notice of collection, seamlessly collect consent, implement prior blocking with asynchronous re-activation and support opt-out from sale via a “Do Not Sell My Personal Information” link.

IUBENDA CONSENT SOLUTION

Easily collect GDPR consent, document opt-ins and CCPA opt-outs

√ FOR GDPR √ FOR CCPA

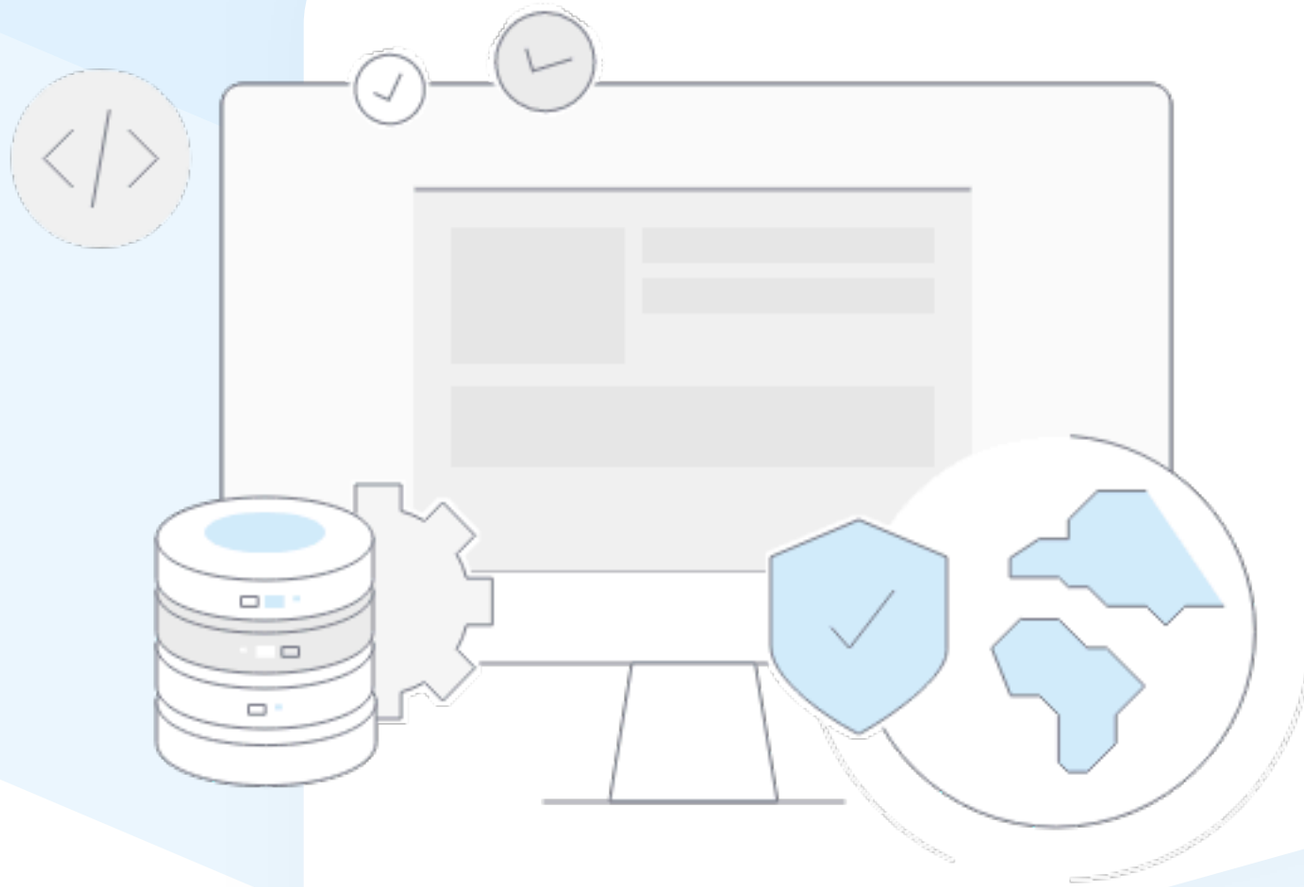


Record and manage GDPR consent, document opt-ins and CCPA opt-outs for each of your users. It smoothly integrates with your consent collection forms, syncs with your legal documents and includes a user-friendly dashboard for reviewing consent records of your activities.

INTERNAL PRIVACY MANAGEMENT

Easily document all the data processing activity within your organization

√ FOR GDPR



Create your record of processing activity: add processing activities from 1300+ pre-made options, divide them by area, assign processors and members, document legal bases and other GDPR-required records.

iubenda

www.iubenda.com - business@iubenda.com

A selection of our clients:

jobtome ahrefs ustwo stickermule

HONDA The Power of Dreams MaxMara BOGGI MILANO CASA FONDATA NEL 1939 Portland Press Herald