iubenda

Guide GDPR

Attorney-level solutions to make your websites and apps compliant with the law across multiple countries and legislations.

Index

1

What is the GDPR and where does it apply?

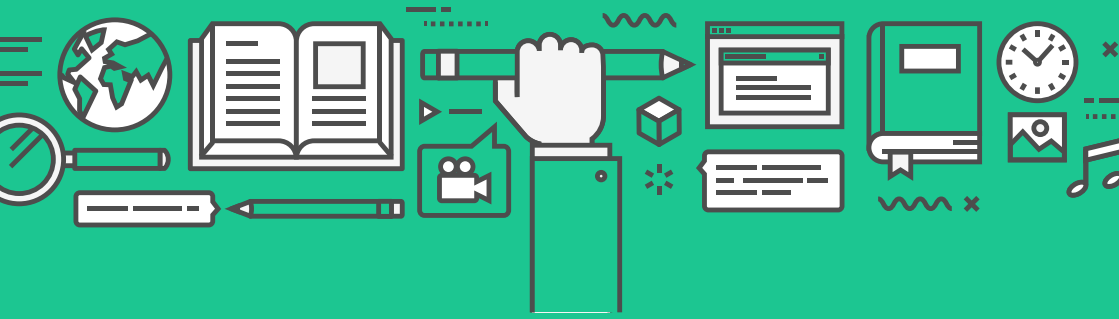
GDPR stands for General Data Protection Regulation (Regulation (EU) 2016/679) and at its most basic, it specifies how personal data should be lawfully processed (including how it's collected, used, protected or interacted with in general). It's intended to strengthen data protection for all people whose personal information fall within its scope of application, putting personal data control back into their hands.

The GDPR can apply where:

- An entity's base of operations is in the EU (this applies whether the processing takes place in the EU or not);
- An entity not established in the EU offers goods or services (even if the offer is for free) to people in the EU. The entity can be government agencies, private/ public companies, individuals and non-profits;
- 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**. As a matter of fact, this PwC survey showed that the GDPR is a top data protection priority for up to 92 percent of U.S. companies surveyed.

The GDPR becomes enforceable starting from May 2018.



2

2. Main Legal Requirements

+Special definitions used below:

**The term 'user' here means an individual whose personal data is processed by a controller or processor.*

**The term 'data controller' means any person or legal entity involved in determining the purpose and ways of processing the personal data.*

**The term 'data processor' means any person or legal entity involved in processing personal data on behalf of the controller.*

For example, an internet company may collect user information via their website and store it using a 3rd party cloud service. In this scenario, the internet company is the data controller and the organization running the cloud service is the data processor.

I. Lawful basis for processing data (Article 6)

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

The lawful bases are:

- The user has given consent for one or more specific purposes.
- The data processing is necessary for the performance of a contract in which the user is a participant or necessary in order to take steps (requested by the user) prior to entering the contract.
- The processing is necessary for fulfilling a legal obligation to which the data controller is subject.
- The processing is necessary for protecting the vital interests of the user or of another person.
- The processing is necessary for performing a task carried out in the interest of the public or as contained under the official authority given to the data controller.
- The processing is necessary for the legitimate interests of the data controller or third party, except where overridden by the interests, rights and freedoms of the user, in particular where the user is a child.

II. Consent (Articles 7&8)

Organizations must get **verifiable consent** from users.

In regards to Consent for children, organizations are required to get **verifiable consent** from a **parent or guardian** unless the service being offered is a preventative or counseling service. Organizations must make reasonable efforts (using available technology) to verify that the person giving consent actually holds parental responsibility for the child.

In general, when getting consent for data processing, organizations **may not use overly complicated or indecipherable** terms. This includes legalese and unnecessary jargon. This indicates that terms and privacy policies should be laid out legibly (see ours here) using understandable language and clauses so that users are fully aware of what they're consenting to and what the consequences of their consent are. Organizations must be transparent on the purpose of the data collection and consent must be "explicit and freely given". This means that the **mechanism for acquiring consent must be unambiguous** and involve a clear "opt-in" action (the regulation specifically forbids pre-ticked boxes and similar "opt-out" mechanisms). The regulation also gives a specific right to withdraw consent; it must, therefore, be as easy to withdraw consent as it is to give it.

Because consent under the GDPR is such an important issue, it's **mandatory** that yo **keep clear records** and that you're able to demonstrate that the user has given consent; should problems arise, the **burden of proof lies with the data controller**, so keeping accurate records is vital. The records should include:

- When and how consent was acquired from the individual user
- Exactly what the user was told and which conditions were applicable at the time that the consent was acquired

For an **example of compliant record-keeping vs non-compliant record-keeping**, see the following

Non-compliant Record Keeping	Compliant Record Keeping
Simply keeping a spreadsheet with customer names and whether or not consent was provided	Ensuring that you keep a copy of the customer's signed and dated form which shows the action taken by the customer to provide their consent to the specific processing.
Simply keeping the time and date of consent linked to an IP address, with a web link to your current data-capture form and privacy policy.	Keeping comprehensive records that include a user ID and the data submitted together with a timestamp. You also keep a copy of the version of the data-capture form and any other relevant documents in use on that date.

A note on consent: *it is not the ONLY basis that an organization can choose to process user data; it is only one of the "Lawful Bases", therefore companies can apply other lawful (within the scope of GDPR) bases for a data processing activity. With that said, there will always be data processing activities where consent is the only or best option.*

Another EU law worth mentioning here is the **ePrivacy Directive** (also known as the Cookie Law). This law still applies as it has not been repealed by the GDPR. In future, the ePrivacy Directive will be replaced by the ePrivacy Regulation and as such, **will work alongside the GDPR**; the upcoming regulation is expected to still uphold the same values as the directive. The Cookie Law requires users' informed consent before storing cookies on a user's device and tracking them. You can read more about the Cookie Law here.

III. Users' rights

- **The right to be informed (Articles 13&14)**: Organizations must provide users with information about the data processing activities they carry out. Such information can be provided via privacy notices/policies in writing, including by electronic means. The information must be concise, transparent, intelligible, easily accessible, written in clear and plain language (especially if addressed to a child), and free of charge. If the data is collected from the actual user it relates to, then they must be provided with privacy information at the time the data is obtained, however, if the personal data is obtained from a source other than the individual user it relates to, then the user must be provided with privacy information within a "reasonable period" of the data being obtained. This period can be no later than one month in general; if you use the data to communicate with the user, at latest when the first communication occurs.

- **The right to access (Article 15)**: Users have the right to access their personal data and information about how their personal data is being processed. If the user requests it, data controllers must provide an overview of the categories of data being processed, a copy of the actual data and details about the processing. The details should include the purpose, how the data was acquired and with whom it was shared. Also, the organization must provide the person making the request with a copy of their personal data free of charge (a reasonable fee can be charged for further copies). The requested data must be provided to the individual without undue delay and at latest, within one month of receiving the request; the exact number of days the organization has to honor a request depends on the month in which the request was made. The Right to access is closely linked to the Right to data portability, but these two rights are not the same. It is therefore important that in your privacy policy, there is a clear distinction between the two rights.

- **The right to rectification (Article 16)**: Users have the right to have their personal data rectified if it is inaccurate or incomplete. This right also implies that rectification must be disclosed to any and all third-party recipients involved in the processing of the data in question – unless doing so is impossible or disproportionately difficult. If requested by the user, the organization must also inform the user about these third-party recipients. Requests can be extended by a further two months if the request is complex or if numerous requests were received from the individual. The individual must be informed within one month of receipt of the request with an explanation as to why the extension is necessary. Requests must be honored without undue delay and at latest, within one month of receiving the request. In most cases organizations must comply with a request for rectification without charging a fee, however, if a request is found to be "manifestly unfounded or excessive", a "reasonable fee" can be requested in order to carry out the request or refuse to deal with the request.

In both scenarios, the decision will need to be legitimately justified. If a request is refused, the individual must be informed (along with the justification) without unnecessary delay and within one month of receiving the request.

- **The right to erasure (Article 17):** When data is no longer relevant to its original purpose or where users have withdrawn consent or where the personal data have been unlawfully processed, users have the right to request that their data be erased and all dissemination ceased. Requests must be honored without undue delay and at latest, within one month of receiving the request. Requests can be extended by a further two months if the request is complex or if numerous requests were received from the individual. The individual must be informed within one month of receipt of the request with an explanation as to why the extension is necessary. The right to erasure can be refused where the personal data is processed for archiving purposes in the public interest (for example, scientific research), where data is necessary for legal defense, or to comply with a legal obligation, or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller. The right to erasure can also be denied where the data is necessary to exercise the right of freedom of expression, or where the data is being processed for health purposes in the public interest.

- **The right to restrict processing (Article 18)**: Users have the right to restrict the processing of their personal data in cases where they've contested its accuracy; where the user has objected to the processing and the organization is considering whether it has a legitimate ground which overrides this right; where the processing is unlawful but the user requests restriction instead of erasure; or where the data is no longer needed but the user needs it to establish, exercise or defend a legal claim. The restriction must be disclosed to any and all third-party recipients involved in the processing of the data in question – unless doing so is impossible or disproportionately difficult. If requested by the user, the organization must also inform the user about these third-party recipients. Requests must be honored without undue delay and at latest, within one month of receiving the request. Requests can be extended by a further two months if the request is complex or if numerous requests were received from the individual. The individual must be informed within one month of receipt of the request with an explanation as to why the extension is necessary. In most cases organizations must comply with a request without charging a fee, however, if a request is found to be "manifestly unfounded or excessive", a "reasonable fee" can be requested in order to carry out the request or the request can be refused. In both scenarios, the decision will need to be legitimately justified. If a request is refused, the individual must be informed (along with the justification) without unnecessary delay and within one month of receiving the request.

- **The right to data portability (Article 20)**: Users have the right to obtain (in a machine readable format) their personal data for the purpose of transferring it from one controller to another, without being prevented from doing so by the data processor. Both 'provided' and 'observed' data are included under this rule. This right only applies to personal data and as such does not apply to genuinely anonymous data (data that can't be linked back to the individual). Requests must be honored without undue delay and at latest, within one month of receiving the request. Requests can be extended by a further two months if the request is complex or if numerous requests were received from the individual. The individual must be informed within one month of receipt of the request with an explanation as to why the extension is necessary. In most cases organizations must comply with a request without charging a fee, however, if a request is found to be "manifestly unfounded or excessive", a "reasonable fee" can be requested in order to carry out the request or the request can be refused. In both scenarios, the decision will need to be legitimately justified. If a request is refused, the individual must be informed (along with the justification) without unnecessary delay and within one month of receiving the request.

- **The right to object (Article 21)**: Under the GDPR, users have the right to object to certain processing activities in relation to their personal data carried out by the Controller. In a nutshell, the user can object to the processing of their data whenever the processing is based on the controller's legitimate interest, or the performance of a task in the public interest/exercise of official authority, or for purposes of scientific/historical research and statistics. The user has to state a motivation for their objection, unless the processing is carried out for direct marketing purposes, in which case no motivation is needed to exercise this right. If an objection to the processing of personal data is received and there is no grounds to refuse, the processing activity must stop. While the processing activity (including storage) must stop for the particular processing activities objected to, erasure may not be appropriate if the data is processed for other purposes (including the fulfillment of legal or contractual obligation) as the data will need to be retained for those purposes. Requests must be honored without undue delay and at latest, within one month of receiving the request. Requests can be extended by a further two months if the request is complex or if numerous requests were received from the individual. The individual must be informed within one month of receipt of the request with an explanation as to why the extension is necessary. In most cases organizations must honor an objection (where there is no grounds to refuse) without charging a fee, however, if a request is found to be "manifestly unfounded or excessive", a "reasonable fee" can be requested in order to carry out the request or the request can be refused. In both scenarios, the decision will need to be legitimately justified. If a request is refused, the individual must be informed (along with the justification) without unnecessary delay and within one month of receiving the request.

- **Rights relating to automated decision making and profiling (Article 22)**: Users have the right to not be subjected to a decision when it is based on automated processing or profiling, and it produces a legal or a similarly significant effect on the user. Organizations can only carry out automated decision-making if it is needed for the performance of a contract; authorized by EU state law applicable to the data controller; does not have a legal or similarly significant effect on the user; or is based on the individual's explicit consent. You can only make automated decisions based on special category data without the explicit consent of the user or reasons of substantial public interest.

IV. Privacy by design & default (Article 25)

Data protection should be included from the onset of design and development of the business processes and infrastructure. This means that privacy settings should be set to 'high' by default and measures put into place to make sure that the processing life cycle of the data falls within the GDPR requirements.

V. Maintaining records of processing activities (Article 30)

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

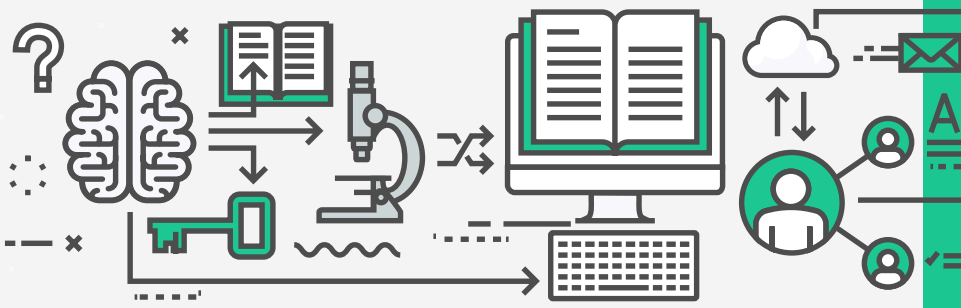
Generally, this requirement only applies to organizations that have **more than 250 employees**, however, it can **still apply** to organizations with fewer than 250 employees if their processing activities:

- Are not occasional; or
- Involves sensitive or special categories of data; or
- Could result in a risk to the rights and freedoms of others

The records of processing activities **must be in writing**. While both paper and electronic forms are acceptable, it is best practice to use an electronic method of record-keeping so as to facilitate easy amendments.

Records of the **data controller** should include:

- The name and contact details of the controller, and where applicable, the controller's representative and DPO
- The purpose of the processing activities
- Description of the various categories of users and data
- The categories of data recipients including third country (not a member of the EU) recipients or international organizations
- Transfers of personal data to a third country and the identification of that third country or international organization, including documentation of suitable safeguards (where applicable)
- Anticipated time limits for erasure of the various categories of data (where possible)
- A general description of technical and organizational security measures (where possible)



Records of the **data processor** should include:

- The name and contact details of the controller and the processor acting on their behalf, and where applicable, the processor or controller's representative and DPO
- The categories of processing carried out on behalf of each controller
- Transfers of personal data to a third country and the identification of that third country or international organization, including documentation of suitable safeguards (where applicable)
- Anticipated time limits for erasure of the various categories of data (where possible)
- A general description of technical and organizational security measures (where possible)

In regards to record keeping, you may find it **useful** to do **regular information audits** on what data your organization holds. Not only does this practice help you to readily meet your record-keeping obligations, but it also makes it easier for you to review and optimize your data processing procedures.

VI. Breach notification (Articles 33&34)

The data controller must notify the Supervisory Authority **within 72 hours of becoming aware** of the breach. If the processing is carried out by a processor on behalf of the controller, the data processor will have to notify the controller immediately after becoming aware of it. Under this rule, users must also be informed of the breach (within the same time frame) unless the data breached was protected by encryption (data rendered unreadable for the intruder), or, in general, the breach is unlikely to result in a risk to individuals' rights and freedoms. In any case, the data controller should keep records of the breaches occurred in order to be able to demonstrate to the supervising authority compliance with these provisions.

VII. Data Protection Impact Assessment (Article 35)

A data protection impact assessment (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 by the organization. The DPIA process should be **recorded in writing**. While publishing the DPIA is not a legal requirement of the GDPR, it is suggested that data controllers consider publishing all or part of their DPIA as a gesture of transparency and accountability, especially in cases where members of the public are affected (for example, where a public authority carries out the DPIA).

An effective DPIA is useful in meeting the requirement of "Privacy by design" as it makes it possible for organizations to find and fix issues at an early stage, thus mitigating both data security risks for users, and the risk of fines, sanctions and reputation damage that might otherwise occur to the organization. **Generally speaking, the DPIA is only 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 technology). However, if unsure as to whether or not your processing activity falls within what is considered "high risk", it is recommended that a DPIA be carried out nonetheless as it is a useful tool for ensuring that the law is complied with.

"High risk" data processing activities include:

- Large-scale processing of sensitive data
- Systematic monitoring of a publicly accessible area (e.g. CCTV)
- Situations where there are extensive automated evaluations of personal data that is intended to influence decisions that can affect the user's life significantly

DPIAs can also be required in other circumstances (based on a by case evaluation) including but not limited to processing data concerning vulnerable persons (e.g. children, the elderly), data transfer across borders outside the EU and data that is being used in profiling (e.g. credit scores). You can read more about the criteria here [PDF].

The DPIA should include:

- Full descriptions of the data processed
- The purpose of the processing activity (and where applicable, information on the legitimate interests of the data controller)
- An evaluation of the scope and necessity of the processing activity in relation to the purpose
- An assessment of the risk posed to users
- Measures in place to address that risk

VIII. Data Protection Officers (Article 37)

The Data Protection Officer (DPO) is a person with expert knowledge of data protection law whose role includes assisting the controller or processor in monitoring internal compliance with GDPR regulations and overseeing data protection strategy and 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.

GDPR requires designation of a DPO specifically in the following cases:

- Where there is large-scale regular and systematic monitoring of users
- Where the processing is carried out by a public authority (except for courts or independent judicial authorities)
- Where the organization is performing complex operations with user data (in particular sensitive user data)

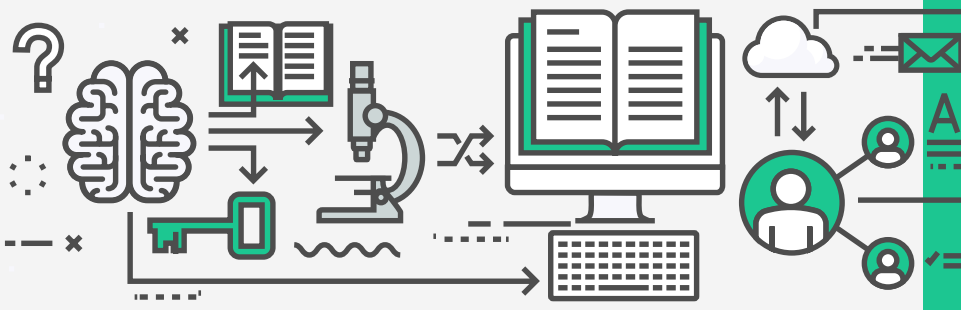
The appointment of a DPO is therefore not just based on the actual number of employees but on the essence of the data processing activity. **If your organization falls outside of these categories, then it is not mandatory that you appoint a DPO**.

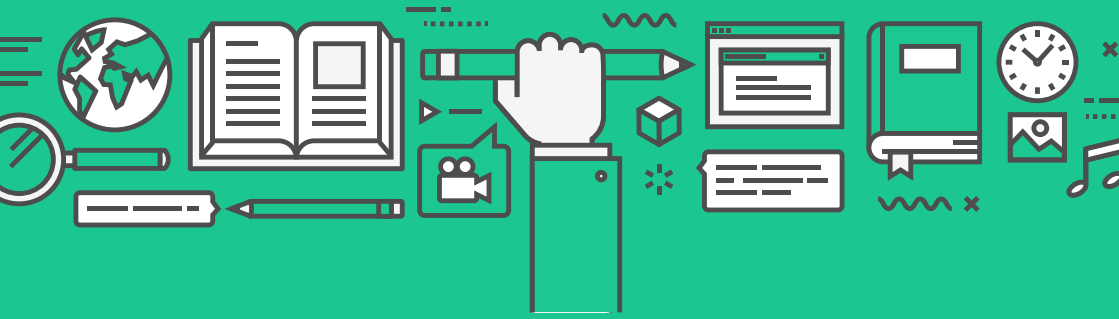
IX. Cross-border data transfers (Articles 44-50)

The GDPR permits data transfers of EU resident data outside of the European Economic Area (EEA) only when in compliance with set conditions. Under these conditions, the country or region the data is being transferred to must have an "adequate" level of personal data protection by EU standards, or where not considered adequate, transfers may still be allowed under the use of standard contractual clauses (SCCs) or binding corporate rules (BCRs).

In regards to data transfer to the US, all transfers either require that the data processor adhere to the **EU-US Privacy Shield** or that **informed consent** is received from the user (in which case the consent must be given on the basis of sufficiently precise information, including information on the lack of protection in the third country).

The Privacy Shield is a binding legal framework which was put in place to help protect EU users rights while allowing US companies to handle EU users data without prior consent. You can read more about the EU-US Privacy Shield here.





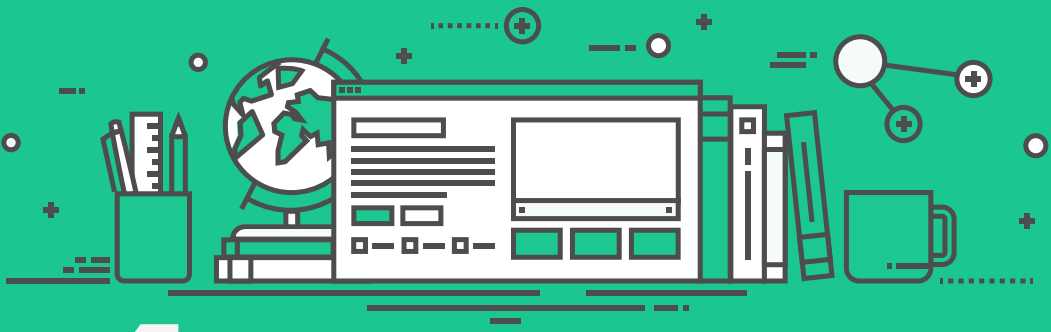
3

Consequences of Non-Compliance

The legal consequences for non-compliance can include **fines up to EUR 20 million (€20m)** or 4% of the annual worldwide turnover (whichever is greater), but perhaps equally as concerning are the other potential sanctions that may be implemented against organizations found to be in violation. These sanctions include **official reprimands** (for first-time violations), **periodic data protection audits** and **liability damages**.

The GDPR gives users the explicit **right to file a complaint** with a supervisory authority if they feel that any processing of their personal data was done in violation of GDPR regulations. So for example, if a report is made to the authority about an instance of regulatory violation, the authority may choose to perform an audit of the organization's data processing operations. If it's found that some processing activity was done unlawfully, not only is a fine imposed, but the organization may be forbidden from making further use of both the data of the inquiry and data acquired using similar mechanisms. This means that if the improper use was in regards to email address collection, the organization risks being barred from using the entire associated email list.

The GDPR also gives users the right to **compensation for any damages** resulting from an organization's non-compliance with regulations, hereby leaving violators open to potential litigation.



4

How iubenda can help

In terms of compliance, one of the first logical steps is making sure that your documents are up to regulation. At iubenda, we take a comprehensive approach to data law compliance. We build solutions with the strictest regulations in mind, giving you full options to customize as needed. This way, we'll assist you with meeting your legal obligations, reduce your risk of litigation and protect your customers —building trust and credibility.

Here's what you need to get started with full compliance:

Privacy policy

This legal document should state the ways in which your website or app collects, processes, stores, shares and protects user data, the purposes for doing so and the rights of the users in that regard.

With our Privacy and Cookie Policy Generator you can create a beautiful, lawyer-crafted, precise privacy policy and seamlessly integrate it with your website or app. You can simply add any of several pre-created clauses at the click of a button or easily write your own custom clauses using the built-in form. The privacy policy also comes with the option to include a cookie policy (it's necessary to include it if your website or app is using cookies). The policies are customizable to your needs and remotely maintained by an international legal team. See how it works here.

Cookie Solution

Because using cookies can mean both processing user data and installing files on the user devices, they are a major point of concern when it comes to user data privacy rights. For this reason, it's vital that your website or app complies with the EU's ePrivacy directive (Cookie Law). In response to this need, we've created our comprehensive Cookie Solution which simplifies compliance with provisions of the European Cookie Law. It's an easy to run cookie policy and cookie consent solution (including banner management), that's fast and does not require heavy investments. See how it works here.

Please note that from time to time, laws are amended and updated. It's therefore important to ensure that your policies meet the latest requirements. For this reason, we use embedding options and NOT copy & paste. With this method, you can rest assured that your policy is up to date and being maintained remotely by our legal team.

Internal Privacy Management

Meeting GDPR regulations can be a technical challenge to implement in practical terms. This is especially true for internal privacy management. In order to be compliant, you must be able keep track of and to describe:

- which data you collect;
- for which purposes it was collected;
- the legal basis for processing;
- data retention policy for each processing activity;
- the parties involved (both inside and outside your organization);
- security measures;
- data transfer outside of the EU, if any; and
- other related details which may apply company-wide, including data of employees.

Our solution helps you to easily record and manage all the data processing activity within your organization so that you can easily comply with requirements and meet your legal obligations. It allows you to create records of processing activity: add processing activities from 600+ pre-made options, divide them by area (sub-divisions within which data processing activities are the same), assign processors and other member roles, and to document legal bases and other GDPR-required records.
Please note: As mentioned in this e-book, full and extensive records of processing are typically required for organizations that handle "special categories of data" or have more than 250 employees, however there are some record-keeping requirements — such as which data you collect, it's purpose, all parties involved in its processing and the data retention period — which are mandatory for everyone. Additionally, even though the GDPR is a common reason to put more effort into internal privacy management, our tool is not exclusively made for application under the GDPR. It can also be used for internal privacy management in general, even by companies who do not have any users/customers within the EU.

For a list of the full features of the Internal Privacy Management tool click here or read the guide here.

Managing consent and maintaining detailed records related to it

GDPR, companies need to store proof of consent so that they can demonstrate that consent was collected. These records must show:

- when consent was provided;
- who provided the consent;
- what their preferences were at the time of the collection;
- which legal or privacy notice they were presented with at the time of the consent collection; and
- which consent collection form they were presented with at the time of the collection.

Our Consent Solution simplifies this process by helping you to easily store proof of consent and manage consent and privacy preferences for each of your users. It allows you to track every aspect of consent (including the legal or privacy notice and the consent form that the user was presented with at the time of consent collection) and the related preferences expressed by the user.
To use, simply activate the Consent Solution and get the API key, then install via HTTP API or JS widget and you're done; you'll be able to retrieve consents at any time and keep them updated.

For a list of the full features of the Consent Solution click here or read the guide here.

iubenda

Attorney-level solutions to make your websites and apps compliant with the law across multiple countries and legislations.

Get your documents and make your site or app compliant in minutes on www.iubenda.com