GDPR Compliance Kit

June 15, 2018

Due to the rising interest in protection of personal data, and the 2018 reform of EU data protection rules, we assembled a compliance kit that provides transparency for your website visitors and peace of mind for you and your organization.

About the GDPR

The General Data Protection Regulation (GDPR (EU) 2016/679) is a measure initiated to specify how data should be used, collected, protected and interacted with. This regulation controls how personal data is lawfully processed to protect personal information by allowing control of its application in the hands of the individual.

Enforcement in the GDPR began in May 2018.

Where does it apply?

The GDPR applies where:

- The base of operations for the entity is in the EU, regardless if the data processing takes place in the EU
- An entity not in the EU offers goods or services (free offers included) to people in the EU.
- An entity not established in the EU monitors the behavior of people who are in the EU.

*The entity can be government agencies, private/ public companies, individuals and non-profits

This regulation effective covers the majority of companies and can **apply to you regardless if your organization is based in the EU** or not. According to a PwC survey, GDPR data protection is a top priority for up to 92 percent of U.S. companies.

Legal Requirements

The world's dependence on digital services and products has resulted in an increased necessity for data privacy, resulting in many regions enforcing strict data regulations that business are expected to comply. Failure to comply with these regulations can lead to financial consequences while also contributing to damaging your organization's reputation and public trust. It is essential to ensure that your business is in compliance with legal obligations.

Regional regulations may apply to your business whether it's located in the region or not. For that reason, it's always advisable that you approach your data processing activities with the strictest applicable regulations in mind.

Major Components

The majority of legislations in place require you to make disclosures relating to your data processing activity outlined in a comprehensive privacy policy. This ensures that security measures are implemented for protecting personal data with an effective approach to gaining user consent or allowing withdrawal.

Data regulations vary based on your region, activity, type of processing, business type, and the age of your users. In addition to the points outline below, you may potentially have additional responsibility depending of your law of reference.

Disclosures

Users need to be informed of:

- Owner details of website/app
- Privacy Policy effective date
- Policy changes notification process
- Type of data being collected
- Which third parties have access to their data & what data they're collecting
- Information on their individual rights to their data

Depending on your law of reference you may also be required to employ additional disclosures to users, third-parties and supervisory authority.

Consent

Users need to be able to give consent or have the opportunity to decline or withdraw. Any method that would require the user to make a direct and verifiable affirmative action is allowed, including text fields, toggle buttons, checkboxes, and email confirmation.

It is **mandatory** to keep clear records and maintain an ability to demonstrate that users have given consent. If an issue should arise, the **responsibility to provide proof remains with the data controller** and it is important to keep accurate records. The records should include:

- How consent was acquired from an individual user
- When consent was confirmed
- What conditions were applicable and what information was told to the user at the time of consent

Non-compliant Record Keeping	Compliant Record Keeping
Maintaining a spreadsheet with customer names and whether or not consent was obtained.	Keeping a copy of the user's signed and dated form which details the action taken by the user to offer consent to specific processing.
Keeping the date and time of consent linked with an IP address and a web link to your current privacy policy and data capture process.	Maintaining comprehensive records that include a user ID and the data submitted together with a timestamp. You should keep a copy of the version of the data-capture form and other relevant documents in use on that date.

Determining your law of reference

In general, the laws of a specified region apply if:

- Your operation is based there; or
- You utilize processing services or servers in the region; or
- You target users in that region

This specification means that **regional regulations may apply to your business regardless if you are located in that region** or not. It's is heavily advised that your approach to your data processing policy and activities are drafted with the stricted applicable regulations in mind.

Lawful basis for processing data

According to the GDPR, data can only be collected if there's at least one lawful basis for processing. The lawful bases are:

- The user has given consent for a specific purpose.
- A user is a participant or necessary for the performance of a contract in which data processing is required. The user must request or consent to the terms of the contract.
- Data processing is required to fulfill a legal obligation in which the data controller is the subject
- The data processing is needed for protecting the vital interests of the user or of another person.
- The processing is needed for carrying out a task that is in the interest of the general public or obtained under official authority given to the data controller
- The data processing is essential for the legitimate interests of the organization or third party, except where overridden by the rights and freedoms of the user, in particular where the user is a minor.

Our Solutions

We realize that you've got a business to run. New regulations are hardly ever convenient. In effort to give you peace of mind, and to also provide your users with transparency in the data your website collects, we composed a few packages that suit your business.

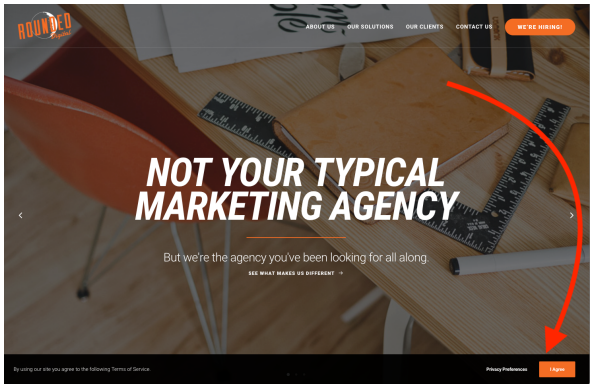
Privacy and Cookie Policy Kit
Privacy policies are legally required worldwide and cookie policies are a direct requirement under the existing ePrivacy Directive (Cookie Law). The policy we provide allows you to seamlessly integrate these new requirements into your existing website.
Privacy Policy (with regulation update protection)
Cookie Policy (with regulation update protection)
Website Optimization (compliant videos)
Display a cookie banner
Consent Storage

Fully-hosted and managed Privacy and Cookie Policy Kit with Consent Storage - $350.00

Privacy policies are legally required worldwide and cookie policies are a direct requirement under the existing ePrivacy Directive (Cookie Law). The policy we provide to your organization allows you to seamlessly integrate these new requirements into your existing website platform.

Your policy must describe what personal data your organization collects and the purpose of the collection in order to be compliant with the new regulations. You must also inform users of their data rights and list all third parties that the data is shared with.

We'll create your privacy and cookie policy that is compliant with GDPR regulations that includes customized text or incorporate your own custom legal text.



Best for sites using popular software like:

- Google Analytics
- Facebook Pixels
- Newsletters (like Mailchimp and Constant Contact)

Integration- We'll integrate your new policy with your site by using one of our widgets or integrating the data processing requirements directly into the

body of Javascript. The policy is hosted on an international server so that it can be stored and updated as needed.

Legal Quality- Our policy was drafted by a team of expert international lawyers with over 600+ clauses to keep your organization compliant.

Up-to-date policies- We track hundreds of third-party services to ensure that the details of your policy are current to comply with their requirements, policies and opt-out links.

Updated documents- Legal regulations has the potential to change periodically. We monitor major regulations revisions and update our policies to meet changing requirements.

Fully Compliant Cookie Banner

If your organization operates in the EU or has potential users from the EU, then compliance with the Cookie Law is vital. Our fully compliant cookie banner complies with the current provisions of the Cookie Law and allows an opportunity to easily inform users, collect their consent and provide an option to block any actions that could install cookies without their consent.

Maximize Collection: We offer several options for gaining consent from your users so that you can optimize your data collection by choosing the solution that works best for your demographic.

Consent via Scrolling: Make the consent process more convenient for users by utilizing consent via scrolling.

Integrated with the Privacy and Cookie Policy Generator: Our Cookie Solution integrates with your existing cookie and privacy policies automatically so there is no need to manually enter details.

Consent Save: Be in compliance with legal obligations without annoying or overwhelming your users. Our solution can track and save consent setting from users for 12 months since their last visit. This allows your users to navigate their experience on your site without interruption during subsequent visits after giving initial consent.

Consent Storage

Organizations must be clear on the purpose of collecting data and the consent acquired from the user must be “explicit and freely given”. This states that the option for retrieving consent must be unambiguous and allow for a clear “opt-in” option (pre-ticked boxes are forbidden). Users also have a specific right to withdraw consent and this process must be as easy to opt-out as it is to opt-in.

We can help you store proof of consent and retrieve this information at a later date, while also storing all user preferences. It is essential for organizations to comply with the GDPR and EU laws, but also to securely store proof of consent and the relation to the privacy policy or online contract.

Consequences of Non-Compliance

Failure to comply can result in legal consequence with **fines up to 23 million (€20m)** or 4% of the annual worldwide turnover. Potential sanctions like official reprimands, periodic data protection audits, and liability damages can be implemented against organizations in violation of regulations.

Users have the explicit right to **file a complaint** if they feel that their personal data was processed in violation of GDPR violations. If a complaint is made then authorities have the right to audit an organization's data processing operations. If there is an unlawful action, organizations are subject not only to a fine, but also could be forbidden from collecting data and making further user of previously

collected data. Users also have the right to seek compensation for damages resulted in an organization's non-compliance with the regulations.