CONSENT MANAGEMENT CHECKLIST FOR GDPR COMPLIANCE

USERCENTRICS

DISCLAIMER

Usercentrics does not provide legal advice, and information is provided for educational purposes only. We always recommend engaging qualified legal counsel or privacy specialists regarding data privacy and protection issues and operations.

This checklist outlines companies' responsibilities and users' rights under the European Union's General Data Protection Regulation (GDPR) and ePrivacy Directive, with steps to take to achieve compliance. It also includes the benefits of using a Consent Management Platform (CMP) and how to implement one to achieve GDPR compliance.

Read on to learn about:

- if your company needs to comply with the GDPR
- how to obtain and store valid consent
- what information your cookie banner and privacy policy need to contain
- what cookie banner design elements are user-friendly and compliant
- and more!

1 Determine if your company is required to comply

If your organization wants to collect and process (store, analyze, aggregate, share, sell, etc.) the personal data of residents in the EU:

- whether your organization is located the EU or not
- whether the data will be processed inside or outside of the EU
- whether a transaction takes place (e.g. payment for goods or services) or not

your organization is obligated to comply with the GDPR.

IMPORTANT TO KNOW

The GDPR came into force on May 25, 2018. It uses a prior consent ("opt in") model. This requires customer or user consent to be obtained before personal data is collected.

2 Create a comprehensive Privacy Policy

Purpose: Inform consumers at or before the point of data collection:

- how data is collected
- how long collected data is retained
- categories of personal data collected
- purposes for which data is collected
- whether data collected is sold to or shared with third parties
- the third parties with which data is sold or shared

Rights: Inform website visitors of their privacy rights and how to exercise them.

Language: Ensure the Privacy Policy and cookie banner are clear and easy to understand. For best user experience enable geolocation features (e.g. in a CMP) that can customize language displayed for users in different regions.

Implementation: Implement a privacy notice with information about data use, consumers' rights and user options, like consent opt out. Enable consumers to exercise rights, like opting out, via a banner or pop-up when visiting your site, e.g. with a CMP.

IMPORTANT TO KNOW
You must have a valid legal basis for data processing.
Consent is one legal basis.

3 Inform users about their rights

Consumers' rights under the GDPR:

- **Right of Access:** to be informed if personal data is processed, what data, and receive access to it, as well as information about processing purposes
- **Right to Rectification:** timely updates or corrections to inaccuracies in personal data collected, and notification from the processor when complete
- **Right to Erasure:** aka "right to be forgotten", timely deletion of personal data that has been collected (with exceptions), and notification from the processor when complete

- **Right to Restriction of Processing:** the processor must stop processing personal data temporarily or permanently
- **Right to Data Portability:** copy of personal data must be provided in a portable and readily useable format
- **Right to Object:** to processing of personal data (including sharing, sale, or profiling)
- **Right to Know about Automated Decision-making:** request information about automated decision-making and likely outcomes of using it, including profiling
- **Right to Opt Out of Automated Decision-making:** refuse use of automated decision-making technology with regards to personal data, including profiling
- **Right to Non-discrimination:** for exercising privacy rights

IMPORTANT TO KNOW

Consent choices must be displayed equally. Do not use nudging or dark patterns. It must be as easy to decline or change consent preferences as it is to accept.

4 Obtain valid consent from users

- **Explicit:** Active acceptance required, e.g. ticking a box or clickin a link. Informed: Who, what, why, how long?
- **Documented:** You have the burden of proof in the case of an audit.
- **In advance:** No data can be collected before consent is obtained, e.g cookies cannot be set on your website before the user has consented to them.
- **Granular:** Individual consent for individual purpose, i.e. consent cannot be bundled with other purposes or activities. The second layer of a CMP can display all cookies/tracking technologies in use and their purposes to enable highly granular consent choices.
- **Freely given:** Equally accessible and easy to use “Accept” and “Deny options, e.g. buttons all on the first layer of the CMP.
- **Easy to withdraw:** Changing consent or opting out is as easy to do as opting in, e.g. available on the same layer of the CMP.

IMPORTANT TO KNOW
Nonessential cookies and other tracking technologies on websites, apps, or other services cannot be triggered or loaded until valid user consent has been obtained.

5 Ensure user access even if they decline consent

- If a user refuses data processing, no nonessential cookies can be set. Essential cookies (e.g. that make the website work correctly) can be set without requiring user consent.
- Ensure users can still access your site, app, or service even if they refuse to allow the use of nonessential cookies or other tracking technologies.
- Nonconsenting users cannot be blocked entirely, but can be notified that without consent for certain technologies, some functions or services may not work correctly and may affect user experience.

IMPORTANT TO KNOW
If the purposes for which you want to collect and process personal data change, or the parties that will have access to the personal data change, e.g. you are working with a new vendor, you must request consent again for the new purpose(s) and/or third parties.

6 Stop data collection or processing as soon as the user opts out

- Data collection and processing must stop as soon as the user opts out, whether that is the first time they visit your website or access your service, or if they update consent preferences later.
- Once the user has declined or withdrawn consent, data also can no longer be forwarded or shared with third parties.

7 Securely document and store consent received from users and be able tp provide information when required

- You have an obligation to take reasonable measures to securely record and store all user data received, including consent preferences.
- In the event of an audit by data protection authorities (DPA), you must be able to verify users' consent for all data collected and the processing purposes.
- In the event of a data subject access request (DSAR) you must be able to provide the user with the data specified by the GDPR's "Rights of the data subject" in a timely fashion, e.g. their consent preferences.

8 Stop data collection or processing as soon as the user opts out

- **Review your operations** and potential changes in the law every 12 months. Update your Privacy Policy information and its effective date. Effective date should be updated even if you don't make any other changes to the Policy.
- **Transparency:** Ensure that the information that users must be notified about is clear, comprehensive and up to date. Ensure that the date of the last update is clearly visible.
- **Data sold:** List all the categories of personal information that your business has sold in the past 12 months.

9 Re-offer opt-in consent every 12 months

- If the consumer has opted out, you can present the option to opt-in again after 12 months.

Learn more about how we can help you achieve GDPR compliance with our Consent Management Platform

GET IN TOUCH