Cookie Script

GDPR Compliance Checklist

1. MAKE A GDPR-COMPLIANT PRIVACY POLICY
2. KNOW THE DATA YOU ARE HOLDING
3. SECURE YOUR WEBSITE
4. USE A COOKIE BANNER ON YOUR WEBSITE
5. REVIEW DATA PROCESSORS OR THIRD PARTY CONTRACTS
6. VERIFY THE AGE OF YOUR WEBSITE USERS
7. GET CONSENT FOR EMAILS
8. EVALUATE YOUR WEBSITE FORMS
9. EVALUATE INTERNATIONAL DATA TRANSFER
10. ANALYZE DATA BREACH
11. UPDATE YOUR CMS PLATFORMS
12. RESPOND TO USER REQUEST

The General Data Protection Regulation (GDPR) took effect on May 25, 2018.

The privacy standards of the GDPR and ePrivacy Directive aim to **protect the personal data and privacy** of all people in the European Economic Area (EEA).

The data protection law applies to all foreign companies processing the personal data of people in the EEA. The GDPR applies to your business even if you don't have any physical presence in any country of the EU.
If your website collects and processes the personal data of users from the EEA, then you should work through our GDPR compliance checklist.

Read this GDPR compliance checklist to learn more about:

- **Users' rights under the GDPR.**
- **Businesses' responsibilities under** the GDPR.
- **How to get and store valid user consent.**
- **What information your cookie banner** needs to provide.
- **What information your Privacy Policy** needs to provide.
- **How to comply with the GDPR.**
- **The benefits of using a Consent** Management Platform (CMP).

Under the GDPR, users in the EU have the following rights:

- **The right to be informed.** Individuals have the right to know how you process their personal information. The easiest way to deal with this right is to post your privacy online, easily accessible by anyone.
- **The right to access.** Individuals have the right to be informed if their personal data is processed, what data, for what purposes, and receive access to it.
- **The right to rectification.** Individuals have the right to ask that their data be updated or corrected.
- **The right to restrict processing.** Individuals have the right to block or suppress the processing of personal data. This means that you still have the right to store the data, but not the right to process it.
- **The right to object.** Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, including profiling; object to direct marketing; and object to processing for purposes of scientific or historical research and statistics.

- **The right to data portability.** Individuals can reuse their personal data across different services. People are allowed to transfer or copy personal data from one service provider to another, so businesses need to provide their data copy.

- **The right to erasure.** Individuals have the right to ask that their data be removed or deleted from your database.

- **The rights around automated decision-making and profiling.** Individuals have the right to request information about automated decision-making and likely outcomes of using it, including profiling. They can also refuse use of automated decision-making technology with regards to personal data.

N O T E: GDPR uses an **explicit consent model**, also called opt-in consent model. This means that businesses must obtain user consent before any personal data is collected.

1. Make a GDPR-compliant Privacy Policy

The main purpose of a Privacy Policy is to inform your website visitors about how you collect, process, and/ or share their personal data. It should explain the user's rights and your business obligations to the users.

Your Privacy Policy must contain the following information about personal data collection & processing practices:

- Who owns the website or mobile app.
- How do you collect the data.
- How long do you keep the data.
- Categories of personal data collected
- Purposes for which data is collected
- The third parties with which data is sold or shared, if any.
- Whether data collected is sold to or shared with third parties.
- List of User Rights. Inform website visitors of their privacy rights and how to exercise them.
- The Policy's effective date.
- Does the data include sensitive personal data?

N O T E: Your Privacy Policy must be written in a clear and easily understandable language. Avoid technical jargon or complex terminology.

N O T E: Enable individuals to exercise their rights under the GDPR, like opting out of user consent. This could be done via a cookie banner, using a Consent Management Platform (CMP).

2. Know the data you are holding

To know how users' personal data is controlled, you need to know what personal data you hold:

- What personal data do you already have?
- Does the data include sensitive personal data?
- Do you hold personal data from minors, who are below 16 years of age?
- How long do you keep personal data?
- Do you have consent to collect personal data? Where is it stored?
- Why do you collect this data?
- How is collected personal data processed?
- Where is collected personal data stored?
- Who has access to this data in your business?
- Do any third parties hold personal data you collected? If yes, how do you control their usage of this data? Do you have any agreements on this?
- Are there any third parties, holding your users' personal data, based outside the EU? If yes, are they aware of the GDPR? Do you have any agreements with them?

N O T E: GDPR Article 4 defines personal data: “Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

Personal data also includes:

- Religious views
- Ethnic origins & identities
- Genetic data
- Biometric data
- Philosophical beliefs
- Health records
- Sexual orientations
- Political opinions
- Memberships.

IP addresses are classified as personal data if they can be used to identify a person. For example, if a user's IP address is collected alongside their address, phone number, or email address, that would be considered personal data because the identity of the person could be linked to their address, phone number, or email address.

If you're not sure if the IP addresses you collect should be classified as personal data, keep on the safe side and protect them as they are personal data.

N O T E: Personally Identifiable Information (PII) is considered sensitive personal data and should be protected with the highest level of cybersecurity.

3. Secure your website

As a website owner, you must ensure your website is secure. This means that the data stored needs to be protected and that the website itself needs to be protected from outside attacks and data breaches.

Here are the basic steps to protect your website from hackers and other people with fraudulent intent:

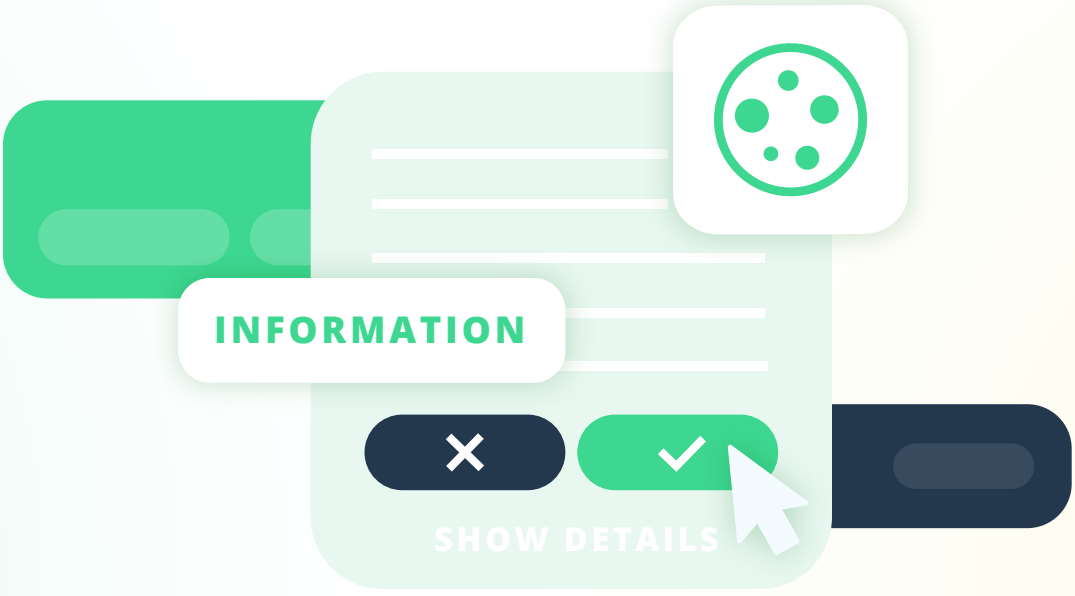
- **Install** an SSL certificate to have HTTPS website URL, that will encrypt any information sharing between your website and the server.
- **Add** extra layers of protection to your server if your users share payment information on the website.
- **Use** strong passwords for admin accounts.
- **Use** anti-virus software or services.
- **Apply** the means for protecting your website against DdoS.
- **Try** not to share personal data, especially sensitive data with third parties.
- **Anonymize** personal data before storing them to make the user anonymous.
- **Do not collect** or store personal data more than what is necessary for your website and remove it once you do not need it.

4. Use a cookie banner on your website

If your website collects data from users based in the EU and uses non-necessary cookies, then you should use a Cookie Banner to get cookie consent from users to store cookies on their devices.

The banner should inform website users that the website uses cookies and what information they collect.

It also should inform users about their **right to refuse** the usage of cookies and their personal data collection, as well as the **right to request to delete** users' personal data already collected.



Here are the basic points you should have in mind while adding a cookie banner:

- Describe **what kind** of cookies you intend to set and why.
- Explain **why** you need to set cookies.
- The banner should have **opt-in** and **opt-out** options for accepting and rejecting cookies, accordingly.
- **Do not drop** cookies BEFORE the user gave explicit consent (opt-in option).
- Give a **possibility to enable** Cookie Consent based on cookie category.
- **Include information** about your Privacy Policy and a link to it.
- Give a possibility **to withdraw or change** Cookie Consent status on every page of your website.
- Document and store all **user consents**.
- Make your **website accessible** even if the user did not allow to use cookies.
- Non-interaction with the banner or scrolling over the web page **does not mean** the user gave Cookie Consent.

5. Review data processors or third-party contracts

If data processors or third parties are performing some functions on behalf of your business, then **you should ensure they align with your Privacy Policy**. They should take all actions to be GDPR compliant as well.

You could make an agreement with third parties regarding data processing processes on behalf of you.

6. Verify the age of your website users who consent to data processing

The GDPR permits personal data processing for persons at least **16 years** of age. To lawfully collect personal data from minors younger than that age, you must receive consent from the holder of parental responsibility for the minor.

Your website must have an age verification process to verify the age of users before collecting any data.

If the website determines that the user's age is below 16 years, implement a separate parental consent process.

7. Get consent for emails

If you use email marketing services to send out newsletters or send emails for any other purpose to EU users, **you need permission from your users to send these emails**.

The users have to give an explicit (opt-in) consent to receive emails from you.

Users should also have the **possibility to opt-out of emails at any time**. Provide an unsubscribe link in your email, easily found by the user. After the user clicks on it, it should take the user to a page where he may easily unsubscribe from emails without any justification.

8. Evaluate your website forms

If your website has any kind of forms, such as **contact**, or **subscriptions**, that collect personal data, you must ensure the data is collected and processed according to the GDPR.

Use this checklist to ensure that the usage of website forms is GDPR compliant:

- **Provide a checkbox with a link** to your Privacy Policy page, with a text like “I have read and accept the Privacy Policy of the website”.
- Inform the user **how the collected data will be used**.
- Inform the user that **he can request to delete his collected data at any time**.
- Inform the user how **he can request to download his own data** stored on the website.
- **Use simple language** that your messaging should be clear and concise.
- **Explain why** you’re asking for their data.
- **Pre-ticked consent boxes are not allowed**, use an opt-in option to get user consent to collect data.
- **Give an option**, such as a checkbox, for users to choose whether they want to receive correspondence from you.

9. Evaluate international data transfer

If you are transferring personal data from EU to non-EU countries, then you should take care to **use international data transfer according to the law**.

Use this simple checklist to comply with the GDPR:

- **Ensure** that the privacy policy of your data processors or third parties, based in non-EU countries, corresponds to your privacy policy.
- **Make sure** that the recipient country or service provider has an adequate level of data protection system in place.
- **Do** the necessary risk assessments before transferring the data to any non-EU country.
- **Review** agreements with processors or third parties, that are based in non-EU countries.

10. Analyze data breach

In your GDPR compliance checklist, you must be prepared in the event of a data breach, so prepare a procedure for it.

Check these key points to take adequate actions in the case of a data breach:

- **Inform the appropriate supervisory authority about the data breach within 72 hours.** Immediate data breach notification is a mandatory GDPR requirement according to article 33 of the GDPR.

> ❗ **Both personal data controllers and processors need to report data breaches within 72 hours.**

Processors need to report data breaches to controllers, and controllers need to report to a supervisory authority. You must inform when it occurred, the data categories and the approximate number of users affected, the approximate number of personal data records affected, any action taken or planned to be taken, and the measures to mitigate its possible adverse effects.
A supervisory authority is Data Protection Association (DPA), which is responsible for monitoring and enforcing GDPR compliance. Supervisor authorities are usually located in the EU state the business is based.

- **Notify the affected users** if there is a pronounced risk to users' privacy as a result of the breach, including what actions they could take to protect their data.
- **Update your processes to prevent future data breaches** on your website.
- **Prepare an action plan for handling future data breaches.**

11. Update your CMS platforms

Make sure your CMS, such as WordPress, Shopify, Weebly, etc. is **updated and is GDPR compliant**.

Cookie Script

With CookieScript, we automatically generate a code for each platform, which you simply copy and insert into your CMS.

You can also update the CMS manually and add your custom code or style.

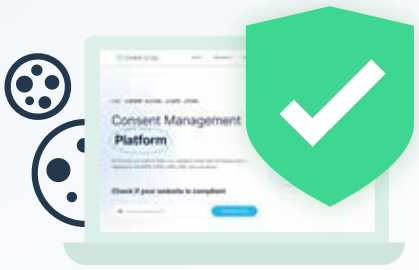
12. Respond to user request

If you received a user request regarding their personal data, be prepared to:

Answer it no later than in **2 days**.

Delete or update the user data no later than **30 days after the request**.

Prepare a process when someone requests their personal data in a **portable transferable format**.



CookieScript CMP - Your Solution for GDPR compliance

Use CookieScript CMP to ensure GDPR compliance and mitigate risks associated with data processing activities.

CookieScript is trusted by top-level brands as well as startups and small companies.

It has the following functionalities:

- **Google-certified CMP.** CookieScript is a Google-certified CMP partner and comes with a full IAB TCF v2.2 integration.
- **Supports Google Consent Mode v2.** If you want to use Google services (GA4, Google Ads, gtag, and Google Tag Manager) in the EU or EEA, you need to use a Google-certified CMP.
- **Local Storage and Session Storage scanning and blocking.** GDPR and other privacy laws require blocking of cookies, Local Storage and Session Storage until user consent is given. However, majority of CMPs do not offer this functionality. CookieScript blocks both Local Storage and Session Storage.
- **Fully customizable.** CookieScript CMP allows Cookie Banner behavior adjustments, and design customization, and has a self-hosted code option.

- **Multiple integrations.** CookieScript CMP integrates easily with Google services automatically via Google Tag Manager, so you could use Google advertisement products easily. The CookieScript CMP is also integrated with other platforms, including content management systems such as Drupal, Magento, Shopify, WordPress, PrestaShop, etc., and analytics platforms, including Google Analytics 4.
- **Language and jurisdiction support.** CookieScript Cookie Banner and cookie declaration report is translated into 40+ languages and has geo-targeting.
- **Easy to set up.** CookieScript CMP could be easily implemented in just a few steps in a privacy laws-compliant way using banner settings hints for different jurisdictions.
- **Full compliance solution.** CookieScript CMP comes with the Cookie Scanner, Privacy Policy Generator, script manager, and user consent manager. It blocks cookies, Third-Party Cookies, Local Storage and Session Storage, so you can be sure your website is compliant with the GDPR and other privacy regulations 100%!