GDPR Concept

General Data Protection Regulation

Effective on EU from May 25th, 2018

It applies to everyone handling the personal data of EU citizens, even if they are not based in the EU.

Failing to comply with GDPR are subject to fines for up to 20 million euros or 4% of your yearly turnover,

whichever is higher.

A person’s personal data is always owned by that person. This means that they must have control over it (with

some exceptions).

Obligation to give information (GDPR Art. 13 & Art. 14)

You have the obligation to provide the following information to the data subjects:

1. Controller’s contact (e.g. identity; name, address).
2. Data Protection Officer’s contact (if you have one).
3. Purpose of processing data.
4. Legal basis for processing (e.g. consent, legitimate interest, law – see art 6(1)).
5. Recipients of personal data (who you are sharing the data with or who has access to it).
6. How long data is stored.
7. Information about data subject’s rights (right to rectification, erasure, access, portability; right to withdraw consent any time; right to submit a complaint to a supervisory authority including the contact information of that supervisory authority).
8. If data is gathered for contractual obligation or other statutory reason, then information about the obligation and whether the data subject is obliged to give personal data and what are the consequences of failing to do so.
9. If any automated decision making or profiling is used, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
10. Information about personal data being transferred to third countries (outside the European Economic Area), the legal grounds for doing that and safety measures taken.

Definitions

Data subject

a human-being (user, customer, employee, etc.) whose personal information you are processing.

Processing

Any activity or set of activities performed on personal data, e.g. viewing, collecting, storing, transferring,

modifying, erasing data

Personal data

It is almost any data about a person

1) name

2) email

3) age

4) personal identification number

5) location info

6) appearance description

7) information about hobbies

8) income

9) cultural preferences

10) analytics

11) comments

12) reviews/posts

13) etc.

Sensitive data

1) racial or ethnic origin

2) political opinions

3) religious or philosophical beliefs

4) trade union membership

5) health

6) sex life or sexual orientation

7) genetic data

8) biometric data

Anonymous data

Data after removing everything that ties to a person that it belongs to.

You can’t identify the user from the data itself

After anonymized, data is not personal data anymore

Controller

It can be a natural or legal person, public authority, agency or other body

It is someone who controls personal data of others. This person determines the purpose (the why) and

means (the how) of processing personal data

If you own a website that does anything with its visitors’ personal data, you are the controller.

Processor

It processes personal data on behalf of someone else.

It is any other natural or legal person who processes or stores data on behalf of the Controller.

It can be the web hosting company, a mail service company, etc.

""""There has to be a written contract between the Controller and the data processor""""

User's rights under GDPR

1) Users can request a copy of all their data you are storing, both in human- and machine-readable format

The controller must comply within 30 days.

2) Users can request you to delete all their data. The controller must comply within 30 days.

3) Users must provide you consent for each use of their data that you perform.

Users must be able to withdraw the consent they’ve given at any time

4) User must be informed of everything you do (like sharing) with their data

Business' responsibilities with data subject under GDPR

1) You need to keep a registry of all data processing activities.

2) You might need to appoint a Data Protection Officer.

3) You need to have contracts with everyone you share customer data with

4) You are not allowed to process sensitive data without an explicit consent from the data subject

you are obliged to have a legal ground for each data processing activity and purpose.

One of these legal grounds is consent.

Not all data gathering forms require a consent (I.E. contact forms). For the ones that do, a simple checkbox

will suffice.

5) Sensitive data also requires more strict safety and security measures

6) You cannot transfer customer data to someone who does not comply with GDPR.

7) If a data breach occurs, you need to notify your local supervisory authority and possibly your customers

8) If you store a lot of data or work with sensitive data, you might be obliged to make a Data Protection Impact

Assessment.

And you are responsible for demonstrating that you’re GDPR-compliant to your supervisory authority

9) Portability. By request of the Data Subject to transfer his/her data to another company, you must provide the

data to the other company in a machine-readable format or alternatively, transfer it directly to another

company or service.

10) Privacy policy: provide data subjects detailed information about their rights related to their data as well as

how exactly their personal data is used. This policy must contain:

* What data is gathered
* Why is it gathered
* For how long it is stored
* On what legal grounds are you gathering the data
* Who to contact in case of problems, etc.

Business’ responsibilities to GDPR

1. Accountability

The controller is also responsible for demonstrating that it is following the rules of GDPR.

1. Choosing data processors

The controller should only use the services of data processors who also follow the rules of GDPR and through a written contract.

1. Technical and organizational measures to support following data protection rules

The controller must implement “appropriate technical and organizational measures” to ensure compliance.

1. Privacy by design
2. Records of processing activities

The controller needs to keep current records of all the activities performed with personal data.

This is excepted If the controller has left than 250 employees and unless:

* the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects,
* the processing is not occasional, or
* the processing includes special categories of data (i.e. sensitive data).

1. Cooperation with supervisory authorities
2. Secure processing
3. Data breach notification

The controller must inform your supervisory authority within 72 hours from the time you became aware of the

breach.

So, unless you are completely sure that the risk doesn’t qualify as “high,” we recommend informing your data

subjects of a breach.

1. Data protection impact assessment (DIPA)

If your processing activities might influence or pose a high risk to the data subject’s rights and freedoms, you

must conduct an assessment of these processing activities and find a way to mitigate risks.

1. Appointing a data protection officer (DPO)

If you monitor data subjects on a large scale, process data systematically and regularly or process sensitive data

on a large scale (art 9) you must appoint a data protection officer.

1. Age control – offering services to a child

You must try to verify either the age of your data subjects or authorization by their parent if they are underage.

You probably don’t need to worry unless are offering a product or service aimed towards children.

1. Your employees

If you are a company, all these rules apply to your employees as well. GDPR regulates the processing of everyone’s personal data, whether they are a customer or an employee.

When an explicit consent is required

An explicit consent from the data subject is required is there are not implicit legal ground (reasonable reasons) to

process personal data.

Common legal grounds

1. Fulfilling a contract

When the data processing is necessary for the performance of a contract to which the data subject is party or by

the data subject request.

1. Law

if processing is necessary for compliance with a legal obligation to which the controller is subject.

1. Legitimate interest

We don’t recommend using it without the help of a lawyer.

When should you publish the changes you’ve made?

GDPR also works retroactively. This means that it also applies to any data you have gathered before May 25th.

To ensure that you comply with GDPR, check that all your forms (including plugins and custom-built features) comply

with GDPR before publishing the Privacy Policy page. Because the data deletion functionality may not delete data on

plugins

Data Minimization

It is one of the principals of gathering personal data under GDP.

you may gather only the data you specifically need for a specific processing purpose.

So, the first thing to do is review all the forms on your website and remove any fields that are not strictly necessary.

Tracking consent

If you’re gathering any personal data on the grounds of consent, the next important thing is tracking these consents

This tracking will depend on the forms and the plugins (I.E. Contact Form 7) you use .

Features of the WordPress GDPR Framework by Data443

1) It provides various tools and features to help you make your website properly compliant.

All the base requirements of GDPR are covered.

2) It guides you through the maze of rules, regulations and requirements of GDPR.

3) it aims to provide solutions for various complex corner cases regarding data privacy and customer rights.

4) it’s a framework for developers. It is opensource

5) It provides a page where visitors can authenticate via email or login. This page allows visitors themselves to

view, export or delete their personal data automatically

- Request to view their personal data,

- Request to export their personal data in a machine-readable format,

- Request to delete their personal data,

- View and withdraw consents they have given (more on that later).

- Anonymize their data

Limitations of the WordPress GDPR Framework by Data443

1. Most existing plugins are not GDPR compliant

You may need to know which data your plugins gather and why, then also add that information.

2) It is well suited for simple WordPress websites

3) It is compatible with WooCommerce and Contact Form7

Configuring the plugin

Admin dashboard via Tools > Data443 GDPR

1. Enabling Privacy Tools:

> **General** tab > Check “**Enable Privacy Tools**”

Enable the Privacy Tools page on front-end and dashboard. This allows visitors to request viewing and

deleting their personal data and withdraw consents.

1. Selecting the Privacy Tools page

> **General** tab > Drop down menu “**Privacy Tools Page**\*”

It allows you to select which page contains the Privacy Tools controls.

This dropdown only controls where various links on your website point to

The actual contents of the page are displayed by adding the [ gdpr\_privacy\_tools] shortcode (without

spaces) inside the page content.

1. Configuring options: View / Export data

> **General** tab > **Export action**

Configures what should happen when a visitor requests to download their data

This setting applies to both human-readable and machine-readable data download

1. Exporting customer data manually

> **Data Subject** tab > **Find data subject by email** box

you can search for data subjects by email (even those who don’t have accounts on your website) and

download, anonymize or delete their personal data.

1. Deleting data

> **General** tab > **Delete data**

Configures what should happen when a visitor requests to delete their data.

You can set it to delete or anonymize the data

The notification emails contain the data subject’s email address, which also counts as personal data.

You should delete them once you no longer need them (and within 30 days).

If you configure the GDPR Framework to automatically delete personal data, you also have the option to select

whether any content (e.g. pages, posts) created by the deleted user account is also deleted or assigned to

another user instead.

1. Deleting customer data manually

> **Data Subject** > **Find data subject by email** box

search for data subjects by email (even those who don’t have accounts on your website) and download,

anonymize or delete their personal data.

1. Configuring the Privacy Policy page

> **Privacy Policy** tab

It allows you to fill in some fields and generate a Privacy Policy template.

The Representative Contact is needed for companies outside the EU. It has to be somebody on the EU that will

represent you on GDPR issues.

The generated template contains multiple places marked with [TODO] – edit these as you see fit.