European GDPR Law
Rules and Regulations

All you need to know about the **GDPR**

The steps a blogger can take to comply.

COMPILED BY LOES KNETSCH

Loes

GDPR Requirements

Content

GDPR requirements, step-by-step explanation
The GPDR (General Data Protection Regulation) law and how it impacts you

"Law GDPR May 25th 2018 in operation"

The European Union has approved a new privacy law for its citizens. The GDPR. Everyone who wants to do business inside the borders of the EU has to inform their EU visitors in what way they are placing cookies and tracking data.

The consequences of the GDPR are complex. For that reason, I have divided the steps to be taken into three different groups. Each group once again consists of areas where a company must have an answer to, to be able to live up to the demands arising from the GDPR.

Organizational measures
The GDPR requires organizations that process personal data to take measures that significantly reduce the risk of a data breach. You must also be able to show which measures you have taken. The measures include

Privacy Impact Assessments
Audits
Follow-up policy rules
Logging of activities
The appointment of a Data Protection Officer (DPO)
The GDPR requires certain organizations to appoint a Data Protection Officer.

This can be an existing employee or an external consultant who bears the responsibility.

For example, if your organization manages a large customer base, you will have to appoint a Data Protection Officer. The GDPR expects from the national authority that they provide assistance in determining the job requirements.

The designated officer is responsible for testing the GDPR how the organization deals with data, issuing advice about the measures to be taken and when and how a Privacy Impact Assessment should be carried out. In addition, the officer is the first contact person to the Data Protection Authority on behalf of the organization.

One stop-shop

The concept of a one-stop shop ensures that an organization with several branches in the EU has only one Personal Data Authority.

Processes, procedures, and policies
The GDPR defines a data leak as "a leak of security that results in unintentional or unlawful destruction, loss, modification, unauthorized release of or access to personal data that has been sent, stored or otherwise processed".

This is a more comprehensive definition than before and makes no difference whether a data leak harms the individual or not. Every organization is obliged to inform the Authority for Personal Data of the data leak within 72 hours after discovery.

Organizations are exempt from reporting the leak to data subjects, provided sufficient technical and organizational measures have been taken to protect the personal data, such as encryption.

Privacy by Design

Complying with the GDPR means implementing privacy by design in the development of new processes and products in which the collection or processing of personal data plays a role. Where this was previously a best practice, privacy by design is now a requirement.

Privacy Impact Assessment

A Privacy Impact Assessment aims to test the technical and organizational measures taken by an organization in favor of the GDPR requirements.

According to the GDPR, a PIA is a formal requirement; the controller must ensure that a PIA has been executed before it starts a process or activity with a high privacy risk.

International Data Exchange

Internationally operating organizations should, where necessary, tighten the policy and processes for exchanging data with non-EU countries. The rules for the processing or exchange of data by organizations to jurisdictions that are not recognized by the European Commission have been considerably tightened.

Awareness of data protection
Internal staff

There is still plenty of time, but start quickly creating awareness about the GDPR and the stricter guidelines throughout the organization. The transparent processing of personal data and the adjusted rights of the individual may require adjustments that can have a significant impact on the financial and IT processes. The training of staff can contribute to the awareness.

Responsibility - technical measures
Technical

The GDPR obliges the responsible person to demonstrate that the organization complies with the data security principles. It is important for an organization that it pursues a clear policy with which the required standards are met. The requirements include monitoring, reviewing and testing data processing procedures, ensuring processes and ensuring that employees are trained to handle personal data with care. An organization must at all times be able to submit the measures taken when requested by the European Data Protection Authority.

Data Leak - Technical Measures
Within 72 hours after discovering a data breach, this must be reported to the Data Protection Authority. Good preparation for a possible data leak includes drawing up clear policy measures and regularly testing procedures.

Failure to report a leak within the set term may result in a fine in addition to a possible fine for the data leak itself.

More rights for those involved - technically
The GDPR strengthens the rights of data subjects, for example by adding the right to allow a person to view, have modified, or even delete the data that is processed about himself.

Access for data subject

One of the main goals of the GDPR is to protect the rights of the individual. For an organization, this results in adapting or adding procedures for processing access requests to the personal data of data subjects.

In most cases, an organization will not be able to request compensation for providing access to the data and must be able to comply with this request within one month.

The right to be forgotten (The right to delete information)

This right gives individuals the possibility to request the controller and any processors to delete personal data without undue delay. This request must be granted in situations where there are questions about the execution of the processing or when an individual withdraws consent from processing.

Third parties who have insight or access to the personal data of data subjects must also comply with this request.

Automated profiling

The GDPR defines profiling as "any form of automated processing of personal data used to evaluate personal aspects, in particular with which it is analyzed and/or with which predictions are made that have to do with performance at work, the economic situation, health, personal preferences, interests, reliability, behavior, location, and movement within an area. "Nevertheless, there is some ambiguity about the way in which an individual can challenge the right to automatic decision-making based on profiling.

Data transferability

The GDPR introduces a new right to data transferability, which means that an individual can request the automatically processed personal data. The processor will have to provide this information in a machine-ready format.

Right of resistance

As part of strengthening the rights of the individual, the European Commission has agreed to restrict the processing of personal data for marketing purposes. This also includes limiting profiling activities with a marketing goal.

If an individual objects to an organization, it will immediately have to stop processing personal data. In addition, the contact details of the individual must be kept on an internal list.

Organizations are obliged to inform individuals about their rights to the processing of personal data.

Communicate privacy info
Permission

Obtaining approval from individuals on the processing of his or her personal data should be as simple for an individual as the withdrawal of the approval. Approval or withdrawal cannot be derived from silence, pre-ticked boxes or inactivity.

Parental permission

As part of strengthening the rights of the individual, the European Commission has agreed to restrict the processing of personal data for marketing purposes. This also includes limiting profiling activities with a marketing goal.

The GDPR requires that organizations receive permission from parents before they can process personal data of minors. If an individual objects to an organization, it will immediately have to stop processing personal data. In addition, the contact details of the individual must be kept on an internal list.

Notification of processing

The introduction of the GDPR means for many organizations that they will have to share more information with individuals where they process personal data. Information that must be shared includes, among other things, the legal basis for the processing of the data, the retention period and the right of the individual to make reports to the European Data Protection Authority, provided there are problems with the processing of personal data. The GDPR requires concise and clear language in the communication to the owners of the personal data.

Data security (integrity and confidentiality)

The GDPR uses data security principles similar to those in the current directive, such as honesty, regularity, and transparency; limiting the goal; data minimization; data quality; security, integrity, and confidentiality.

You must ensure that personal data are processed in a manner that ensures security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage: "The organization and service provider that processes personal data on behalf of the organization takes appropriate technical and organizational measures that guarantee a minimum level of security appropriate to the risks ".

The GDPR proposes a number of security measures that can be used to ensure the protection of data, including pseudonymization and encryption of personal data; ensure continuity in ensuring confidentiality, integrity, availability and resilience of systems and services with which personal data are processed; the ability to timely restore the availability of and access to data in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the proper processing of personal data.

Encryption

The GDPR specifies encryption as a solution that can help to ensure compliance with some of its obligations. The regulation says the following about this:

Article 32 - Security of processing

"1. Taking into account the implementation and implementation of the implementation of the controller and the processor. appropriate technical and organizational measures to ensure a level of security for the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data [...] "

Article 34 - Communication of a personal data leak to the data subject

"3. The communication to the data subject should be in accordance with the following conditions: (a) controller has implemented appropriate technical and organizational protection measures. the data leak, in particular, those that render the personal data unintelligible to anyone who is not authorized to access it, such as encryption [...] "

What does this mean for you?
A few questions:
Is your website accessible to European visitors?
Does your website track data?
Does your website place cookies?
That is 3x YES

The Internet doesn't stop at the border of the European Union

Your website is tracking data

Google Analytics is tracking data
Google Adsense is tracking data
Almost all plugins are tracking data
Autoresponders, like Aweber, and MailChimp are tracking data
Yes, your website is placing cookies

Wealthy Affiliate is placing cookies
Your affiliate programs are placing cookies
Your responsibility according to the GDPR Requirements
Inform your visitors of which data you are tracking, and that you are placing cookies

There are GDPR plugins you can activate to help you meat the GDPR Requirements

Privacy Policy

2. New Privacy Policy

GDPR requirements example privacy policy

The GPDR regulation (General Data Protection Regulation) and its impact on you and your online activities.

The GDPR Act comes into operation on May 25, 2018 and can have consequences for your online business.

The European Union has adopted a new privacy law for its citizens. The DGPR. Anyone who wants to do business online within the borders of the EU must let EU visitors know how they place and follow cookies and trace data. The report is mapped out with a popup, for this purpose plugins have been designed called EU Cookie law or GDPR.

The consequences of the GDPR are complex. That is why I made a sample privacy policy here that you can use in whole or in part on your website. As appropriate.

Cookie and tracking policy

This is the Cookie policy for [website name], accessible via [website url]

What are cookies

As is common with almost all professional websites, this site uses cookies, small files that are downloaded to your computer to improve your experience. This page describes what information they collect, how we use them and why we sometimes have to store these cookies. We will also share how you can prevent these cookies from being stored, but this can downgrade or 'break' certain elements of the site's functionality.

For more general information about cookies, see the Wikipedia article on HTTP cookies.

How we use cookies

We use cookies for various reasons that are described below. Unfortunately, in most cases there are no industry-standard options for disabling cookies without completely disabling the functionality and functions that they add to this site. It is advisable to leave all cookies if you are unsure whether you need them or not, if they are used to provide a service that you use.

Disable cookies

You can prevent the setting of cookies by adjusting the settings in your browser (see the help of your browser for information about this). Please note that disabling cookies affects the functionality of this and many other websites that you visit. Disabling cookies usually also results in disabling certain functionality and functions of this site. Therefore it is recommended that you do not disable cookies.

The cookies that we place

Account-related cookies

When you create an account with us, we use cookies to manage the registration process and general administration. These cookies are usually deleted when you log out, but in some cases they can stay behind to remember your site preferences when you are signed out.

Login related cookies

We use cookies when you are logged in so that we can remember this fact. This prevents you having to log in every time you visit a new page. These cookies are usually deleted or deleted when you log out to ensure that you only have access to restricted features and areas when you are logged in.

E-mail and newsletters related cookies

This site offers subscription services for newsletter or e-mail and cookies can be used to remember whether you have already been registered and whether certain notifications should be displayed that may only be valid for subscribed / unsubscribed users.

Orders that process related cookies

This site offers e-commerce or payment facilities and some cookies are essential to ensure that your order is remembered between pages so that we can process it correctly.

Surveys related cookies

From time to time, we offer user surveys and questionnaires to provide you with interesting insights, useful tools or a better understanding of our user base. These surveys may use cookies to remember who has already participated in a survey or to provide you with accurate results after you have changed pages.

Cookies with forms

When you submit data via a form such as that on contact pages or note forms, cookies can be set to remember your user data for future correspondence.

Site preferences cookies

To provide you with a great experience on this site, we offer the functionality to set your preferences for how this site works when you use it. To remember your preferences, we need to set cookies so that this information can be called when you respond to a page that is affected by your preferences.

Cookies from third parties

In some special cases we also use cookies that are offered by trusted third parties. The following section describes which external cookies you may encounter through this site.

This website uses Google Analytics, one of the most widespread and trusted analytical solutions on the web, that help us understand how you use the site and ways we can improve your experience. These cookies can keep track of things like how long you spend on the site and which pages you visit, so that we can continue to produce interesting content. See the official Google Analytics page for more information about Google Analytics cookies.

Third-party analysis is used to track and measure the use of this site so that we can continue to produce compelling content. These cookies can track things such as how long you spend on the site or which pages you visit so that we can better understand how we can improve the site for you.

From time to time, we test new features and make subtle changes to the way the site is delivered. When we still test new features, these cookies can be used to ensure that you get a consistent experience while you are on the site, while ensuring that we understand which optimizations our users value the most.

Because we sell products, it is important that we understand the statistics of how many visitors to our site actually make a purchase and that is why they are the kind of data that these cookies will keep. This is important to you because it means that we can accurately make predictions that allow us to monitor our advertising and product costs to ensure the best possible price.

The Google Adsense service we use for advertising uses a DoubleClick cookie to display more relevant ads on the web and to limit the number of times that a particular ad is shown to you. Check the official Google AdSense privacy FAQs for more information about Google AdSense.

We use advertisements to offset the costs of running this site and provide funding for further development. The behavioral advertising cookies used by this site are designed to ensure that we offer you the most relevant ads where possible by following your interests anonymously and presenting similar items that may be of interest.

Several partners advertise on our behalf and affiliate-tracking cookies make it easy for us to see if our customers have come to the site through one of our partner sites so that we can credit them correctly and where possible allow our affiliate partners Each bonus offer you provide for making a purchase.

We also use buttons and/or social media plug-ins on this site that allow you to connect to your social network in different ways. For this to work on the following social media sites including; {Make a list of the social networks whose functions you have integrated with your site} will place cookies on our site that can be used to improve your profile on their site or to contribute to the data they for various purposes that are set out in their respective privacy policies.

More information
Hopefully this has clarified things for you and as previously mentioned if there is something you are not sure whether you need it or not, it is usually safer to have cookies turned on in case it interacts with one of the functions that you use on our site. However, if you are still looking for more information, please contact us using one of our preferred contact methods:

E-mail: [your e-mail address]
By visiting this link: [your website contact page]
Telephone: [your phone number]
Address: [your store address]

[Add at least 1 of these 4)

Note: WordPress has a GDPR guide in Settings>Privacy

Comply to the GDPR

3. Comply to the GDPR requirement plugin

WP GDPR Compliance plugin
1. Go to plugins

2. Add new

3. Search: WP GDPR Compliance

4. Click on install Now

5. Activate

6. Go to plugins

7. Click on settings

8. If you have contact form 7 - check activate

[When you don't have contact form 7, it will not show up, you'll only see comment form]

9. Enable WordPress comments

10. Checklist, check the boxes you use

711. Choose privacy policy

12. activate page

13 Data access request

14. Copy the short code

15. Access the page

16. Add some text
When you send a data request we show you all the data stored by [your website name] You will receive an email notification and on the base of the found data,. You can send in a request to anonymize your data.

17. Setting: No-index

18. Set from private to public and update

19. Remove from your top menu and place it into the menu with the privacy policy

20. You can choose to place a link to your Data Request page or put the code in a sidebar or footer widget. For the record, you only need one, the link to the page OR the widget.

21. The plugin is placing a box under the comment area

22. People get an error message when they don't click the box

EU Cookie Law Plugin

4. EU Cookie law Plugin Settings

There are raising some questions about the GDPR and how to install a popup warning. I use the

EU COOKIE LAW plugin for that matter

1. Go to plugins
2. Add new
3. EU Cookie law
4. Install
5. Activate

It will appear in WP Setting

Popup code for the EU Cookie law plugin or widget

The cookie settings on this website are set to “allow cookies” to give you the best browsing experience possible. If you continue to use this website without changing your cookie settings or you click “Accept” below then you are consenting to this. For more information, I refer you to <a href=”https://yourlinktoyourprivacypolicy.com” target=”_blank” rel=”noopener”>GDPR requirements cookie and tracking law</a>.
When you don’t want cookies placed, you are free to leave this website.
<a href=”https://www.google.com/” target=”_top” rel=”noopener”>DECLINE COOKIES</a>

Replace the website link for your own link.

Inform subscribers

4. Newsletter to your subscribers

Example text:

Changes to our privacy policy

We have adapted the text of our privacy policy to make it easier for you to understand how we handle your personal information.

In addition, the text has been made more
detailed and specific.
You can view our updated privacy policy here. The changes take effect on 25 May 2018.

If for some reason you do not agree with our privacy policy and you want to delete your data, you can.
In the sidebar of [yourwebsite URL] you will find a form from where you can send in a GDPR Data Request

The most important changes:

We now explain exactly what information we collect and when we do this. You will now also state in detail which purposes your personal data will be used for.
It is explained when others can perceive your identity.

We clearly state in which situations we pass on your personal information to someone else - including information about the third-parties that process personal data on our behalf.

We have mentioned what personal information we have about you, how long this data is kept and how you can download and modify this information yourself.

Loes

Please note that I do not have a legal background so you should contact a law firm for rock solid legal advice.