Your Step-by-Step Guide to Becoming GDPR Compliant

Posted by PDI Marketing Team

Published: July 27, 2021

There are 99 articles in the General Data Protection Regulation (GDPR) that describe the rights given to European Union citizens and the rules that businesses must follow.

that really mean?

What is the GDPR? We broke it down for you > >

If you take a look at companies who have already started GDPR compliance initiatives, you will find myriad techniques. A PwC Survey found that 77 percent of companies are leveraging Privacy Shield to become compliant, while 75 percent are utilizing binding corporate rules. Additional methods include model contracts, de-identifying European data, and centralizing data centers in Europe.

It will be easier to decide which method best fits your company if you know what steps you need to take. This will vary for each business, depending on how compliant the company already is. Some companies will only have to tweak a few processes, while others will have to build compliance from the ground up.

This checklist is meant to help companies figure out where they are on the scale of compliant to non-compliant. First discover which steps your business needs to take, and then you can guide it in the right direction.

Relevance

If your company is located outside of the European Union, your first task is to determine if the GDPR applies to you. A PwC Survey shows that 92 percent of U.S. organizations consider the European General Data Protection Regulation one of their top priorities. And over 50 percent consider GDPR compliance *the* top priority.

Do not assume your company falls outside the scope of the GDPR simply because your physical location is elsewhere. If you have customers in the European Union, you likely store their information and therefore must comply.

If this is not the case, congrats! You do not need to be compliant by May 25th, 2018. However, that does not mean you should abandon the idea of becoming compliant altogether.

Explore why some companies are becoming GDPR compliant even when not legally required to do so > >

If your business currently falls under the GDPR, there may be steps you can take to avoid being subject to these regulations. Depending on your customer base, these steps may be worth pursuing. However, this does not guarantee that you will not have to become GDPR compliant sometime in the future.

Awareness

Make sure the right people in your organization are aware of the GDPR, its importance, and the repercussions of non-compliance. Remember that becoming GDPR compliant may be a lengthy process, so you should not wait until the deadline is impending to begin the necessary changes.

Assign Responsibility

Whoever is placed in charge will need to determine who the lead supervisory authority for your company will be, figure out which member state laws modify the GDPR requirements in ways that apply to your business, and stay up-to-date on guidance published by the European Data Protection Board and the relevant supervisory authorities.

Level of Existing Compliance

A large portion of EU businesses are compliant with the Data Protection Act (DPA) of 1998. If a company is compliant with the Data Protection Act, they will already be compliant with a large chunk of the GDPR.

This does not make it any less essential to determine where your company fails to meet GDPR standards, but it does make the process of becoming compliant less strenuous.

Uncover and Protect Sensitive Data Within Your Company

Before you can secure customer information, you must know where it resides inside your company. This makes discovering all sensitive data within your organization arguably the more important step in the GDPR compliance process.

Auditors will not accept “I didn’t know we kept that information” as an excuse for non-compliance. You must know where all relevant data is, even if that information is sitting in an archive collecting dust.

This crucial step will define your entire process, so make sure you uncover every scrap of data before moving forward. You do not want to uncover additional information that is outside your project scope as the project progresses. This will force you to take time to revise your processes, and will increase the timeline of your GDPR compliance initiative.

Once all pertinent data has been uncovered, it must be protected. The majority of the General Data Protection Regulation's articles involve companies keeping data protected or proving that their data is protected.

This is the bedrock of EVERYTHING in the GDPR. There are no shortcuts or ways to sidestep this piece of the puzzle. If all customer information is not discovered and kept secure, it is not a question of *if* you will be hacked or fined. It is a question of *when*.

If you are ready to secure your sensitive data, then it's time to discover "3 Steps to Identify and Protect Sensitive Data for the GDPR" > >

Review Current Policies

Now that you know where your sensitive data resides, compare how your data and policies shape up to GDPR standards. You don't want to reinvent to wheel, so create a list of all policies and practices that meet GDPR standards, which processes could meet standards with slight modifications, and which areas need a complete overhaul.

The European General Data Protection Regulation is the first major change to the EU's data protection legislation in nearly 20 years. Take this as an opportunity to dust off your company's policies, boost your security, and bring your data protection systems into the 21st century. This is your chance to get ahead of the curve instead of scrambling to recover after a breach has occurred.

Also known as Privacy Impact Assessments, these are a way to assess the risk that customers face when their information is collected, utilized, and possibly disclosed by a business. The purpose of these appraisals is to find high risk areas that a company is expected to address and resolve.

While it is a good idea for all businesses to run privacy impact assessments and discover any potential weak links, not every company will be required to do so. This rule is mandatory for certain classes of businesses that have "high risk" processing. In fact, there are several GDPR rules that only apply if the company processes information that is thought to pose a "high risk" to the freedoms and rights of the person it pertains to.

Every company will need to examine their own processes and perhaps even consult an expert to determine if they are "high risk." Common high risk activities include data processing that could result in identify theft, financial loss, or fraud. There are other categories as well, so make sure to contact a GDPR expert if your company is unsure of its standing.

For companies in the high-risk category, mandatory privacy impact assessments may be followed with a meeting with your supervisory authority. This meeting is optional for some organizations, and mandatory for others.

Depending on backlog, the wait for this meeting can extend the deadline of your GDPR compliance project. Therefore it is a good idea to get started on this step as soon as possible.

Examine Lawful Basis

The GDPR has stricter rules than its DPA predecessor. Therefore, every organization should examine all data processing activities to determine if they still have a lawful basis, or exemption, for each.

If consent is your lawful basis, refer to the next section for details on how that is changing.

For data processing that has a lawful basis, organizations must maintain documentation which shows they have assessed their data processing practices, correctly weighed the rights of the data subjects, and are following proper protocols.

White & Case has compiled a detailed breakdown of the topic that you can access for free here: "Lawful basis for processing –Unlocking the EU General Data Protection Regulation"

Consent and Access Requests

If consent is your company's basis for lawful processing, be aware that these rules are changing. It is imperative that your customers receive a clear, understandable explanation of how their data will be used before they provide consent.

Consent must be given voluntarily, and must be of an "opt-in" mechanism. It is no longer acceptable to automatically check the consent box or to require data subjects to "opt-out" of giving consent.

Remember that individuals under 16 years of age cannot legally provide consent without the additional authority of a guardian. Individual EU Member States have the option to lower this age to 13 years.

Individuals have the right to withdraw their consent at any time. Your company will need to figure out a standardized way to handle such events, to ensure the data subject's wishes are fulfilled in a timely manner.

The GDPR also gives individuals the right to request access to their personal data. This gives data subjects the right to see how their information is being processed and ensure that it is being processed in a lawful manner.

Access requests must be fulfilled without monitory fees. The GDPR will no longer allow the £10 subject access fee that existed under DPA. A fee can be leveraged if a request is unfounded or excessive, which may apply if a request is repetitive or if multiple copies are requested. The fee is to be based on administrative costs, not profit.

Rewrite Privacy Notices

The GDPR has expanded the requirements for privacy notices from the original DPA guidelines. A company may have to include more information than before, to be determined on a case-by-case basis. If your privacy notices have always been clear and detailed, then you may be good to go!

expectations for this last requirement are higher if the privacy notice is addressed to someone under the legal age of adulthood.

Data Protection Officers

Companies that regularly monitor EU citizens on a large scale, or who process "special categories of personal data" may be required to appoint a Data Protection Officer (DPO). Laws between member states may vary slightly, so make sure to check if your company needs to appoint a DPO based on the relevant member states.

DPO's advise organizations on how to comply with the GDPR requirements. They give advice regarding data protection impact assessments, cooperate with the organization's supervisory authority, and can be authorized to respond to data subjects on subject matters pertaining to the processing of their information.

While it is possible to assign an employee to be your organization's DPO, steps must be taken to ensure there are no conflicts of interests. Another option is to hire an external DPO.

Whoever you hire to become your DPO, they must report to the highest level of management in your company. They should be included in all data protection and security initiatives in the company. They are also protected from repercussions, such as firing, they might face for performing their duties.

Data Breach Notifications

In the case of a data breach, organizations are required to notify the appropriate authorities "without undue delay." This notification must occur within 72 hours of the time the organization discovered the breach. There are specific circumstances that may except a company from reporting a breach or extend their deadline for

A surprising number of companies lack defined processes for reporting a data breach. The last thing you want to do during a breach is search for the correct authority to notify. Document a policy that clearly lays out who to contact, both internally and externally, when a data breach occurs. Then, most importantly, follow through and ensure this policy is carried out correctly.

External Data Transfers

When transferring personal data to a country or international organization outside the EU, a commission must determine if the data recipient can provide a sufficient level of security. If the recipient's data security measures are deemed adequate, data can then and only then be transferred.

If the data recipient is not deemed to have a sufficient level of protection, there are other ways to get approval to transfer data to them. These include the use of binding corporate rules, standard contractual clauses, as well as a few other conditions.

Often companies do not even know who they are transferring external data too, let alone whether they are compliant.

If you are ready to track the movement of your sensitive data, then you need "3 Steps to Identify and Protect Sensitive Data for the GDPR" > >

Closing Notes

While these steps are by no means a comprehensive list of ways companies must comply with the GDPR, they provide guidance to start laying your foundation.

While the GDPR is meant to create a cohesive legislation that applies to the entire European Union, there are small alterations to the rules between European member states. Before you declare yourself GDPR compliant, spend some time researching the differences, if any, that your member state has made to the General Data Protection Regulation.

Posted by PDI Marketing Team

Pacific Data Integrators Offers Unique Data Solutions Leveraging AI/ML, Large Language Models (Open AI: GPT-4, Meta: Llama2, Databricks: Dolly), Cloud, Data Management and Analytics Technologies, Helping Leading Organizations Solve Their Critical Business Challenges, Drive Data Driven Insights, Improve Decision-Making, and Achieve Business Objectives.

Submit your email below to book a consultation with PDI !*

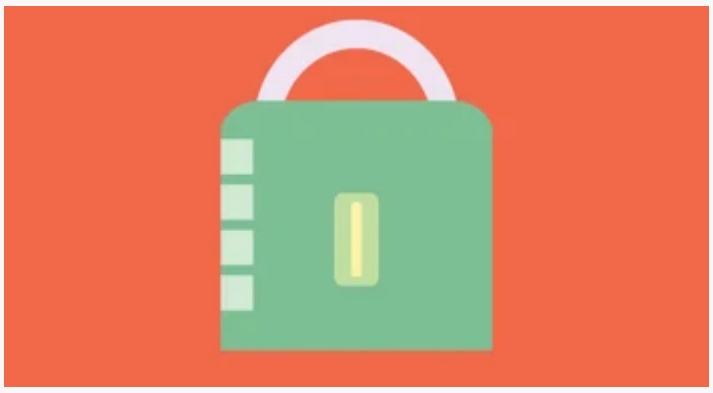
SUBMIT

Share

Share

Share

Related Articles



[Yes, GDPR Compliance is Worth the Cost]

[3 Steps to Identify and Protect Sensitive Data for the GDPR]

[Constantly Discover and Protect Sensitive Data for the GDPR]