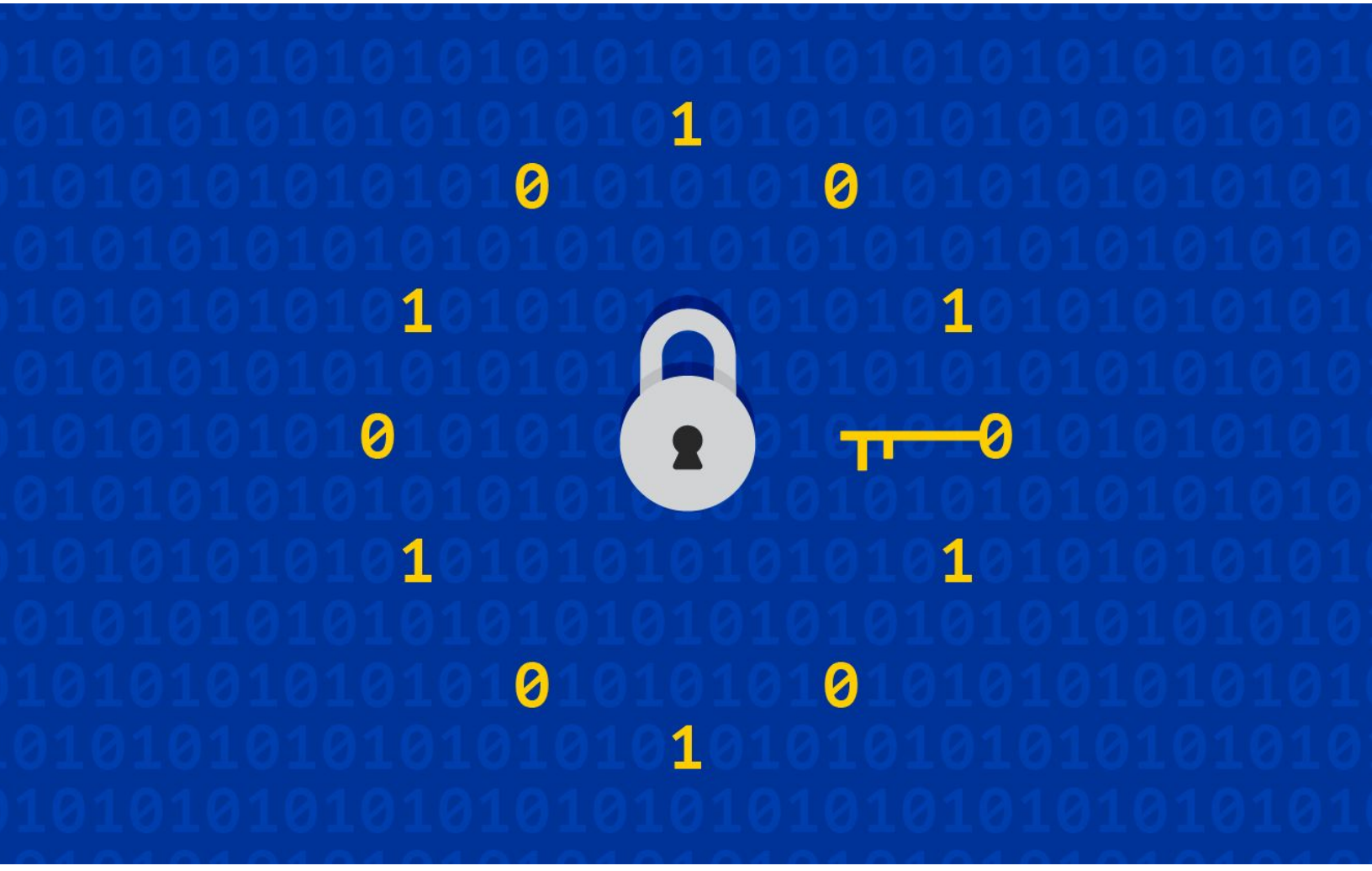

General Data Protection Regulation (GDPR)

What You Need To Know

April 2018

About This Guide

This document is an introduction to the General Data Protection Regulation (GDPR). The GDPR is a code of new privacy laws designed to protect the personal data of all European Union (EU) citizens and residents.

Gauge has created this guide to give eCommerce merchants a brief overview of key issues related to GDPR. In the following pages you'll find a basic summary of the rights and protections granted by the regulation, answers to common questions, and our Next Step recommendations to get you started on the road to compliance.

Gauge predicts that the GDPR will become the new global standard for data privacy. Over time, other nations are likely to adopt similar regulations to protect their own citizens. In simple terms, this will become the "PCI compliance" for personal data in the future.

The GDPR is a meaty subject. Its requirements, implementation, and mandates may seem highly technical and unpleasantly onerous for merchants. But once they understand the regulation's scope and its aims, most people—customers and merchants alike—would probably agree that it's needed. Companies have a clear obligation to safeguard their user data and a valid need to protect themselves from legal exposure. GDPR compliance will go a long way toward accomplishing both.

Our goal is always to use our eCommerce expertise to provide accurate, valuable insights for our clients. That said: ***We aren't lawyers or data auditors, and this guide does not constitute legal advice.*** It's our interpretation and overview of the most pressing points of GDPR. For critical compliance questions, always consult a GDPR-informed lawyer.

This guide is based on information from the official GDPR Portal, the GDPR Breakdown on the UK's Information Commissioner's Office, the book *Be Ready for GDPR* by Punit Bhatia, and from other sources we've consulted. You can also check out our recent article about GDPR published on our website. This guide only focuses on how GDPR impacts eCommerce merchants; however, the GDPR also affects many other industries and fields. For more information about other industries, please see the official GDPR Portal.

Gauge

2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

Executive Summary

The General Data Protection Regulation (GDPR) is a regulation passed by the European Parliament. The regulation's primary aims are:

1. To give EU citizens and residents control over their personal data, often called "personally identifiable information" (PII).
2. To create a single, unified regulatory environment for international businesses.

In practical terms, ***the GDPR applies to all eCommerce merchants around the world.*** As this guide will explain, if you sell products online you will be legally obligated to comply—even if your company doesn't sell or ship products to the EU, and even if your organization has no physical presence in the EU.

GDPR will take effect on May 25, 2018. Unlike many US regulations, there's no implementation grace period. The law is immediately enforceable.

Why Should Merchants Care About GDPR?

"But Grandmother! What big teeth you have," said Little Red Riding Hood, her voice quivering slightly.
"The better to eat you with, my dear!" roared the wolf. — Little Red Riding Hood

These regulations have teeth. If an organization is found to be noncompliant, heavy fines will be levied. Article 83 states that there are two tiers of fines. The tier assigned will depend on factors like the nature and severity of the infringement and which Articles have been violated—***not*** the size or income of the business.

- The lower tier is €10 million (~$12 million USD) or 2% of the company's annual worldwide revenue, ***whichever is greater***.
- The upper tier is either €20 million (~$24 million USD) or 4% of the company's annual worldwide revenue, ***whichever is greater***.

Ouch! You can read more specifics about the fine regime here.

Yikes! Are those Fines Actually Enforceable in the US?

Because the fines are assessed by European authorities, a common misconception is that EU authorities won't be able to recover fines from companies based in the US. We recommend reading this article to get a better understanding of the legal risks of non-compliance for US companies.

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

From that article:

> *"The bottom line: EU regulators can fine U.S. companies for violating GDPR, and they can do it with the help of U.S. authorities."*

We're not lawyers, and because the regulation is brand new, no test cases exist yet to see how enforcement will play out. But both the size of the fines and the history of legal cooperation between the US and the EU make one point very clear: ***US merchants who ignore GDPR do so at their own peril***.

As is often the case for legal compliance, your risk of investigation increases with the size of your business. However, the GDPR gives any EU citizen or resident the right to make a complaint and trigger an investigation. Even smaller companies need to be compliant, as fines could easily spell doom for businesses large and small.

If you do sell or ship products to Europe, or if you have warehouses, third-party service providers, or partners there, you ***absolutely must*** be very concerned about full compliance with GDPR.

Important Definitions

To understand the GDPR, you need to understand a few key terms. Quotes taken directly from the GDPR are italicized:

Data Subject

This is *an identified or identifiable natural person* you collect information about. For eCommerce merchants it includes customers, site visitors, people in your email marketing database, and the like.

Personal Data, aka Personally Identifiable Information (PII)

"Personal data" is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address. We'll dive further into this definition later in this guide.

Data Controller

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In simple terms, this means you—the company or person who *collects* the personal data.

Gauge

2413 Bull Street, Savannah, GA, 31401

www.gauge.agency

(912) 228-3265

Processing

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In short, if a person, service, or company (including yours) does anything at all with the personal data you collect, it's considered "processing."

Data Processor

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This essentially includes any person, tool, or service that has access to any personal data you've collected. It includes your marketing services and third-party partners.

Other key terms are defined here.

Does GDPR Apply to My Business?

The regulation applies if any *one* of the following statements are true:

1. You are a merchant collecting data from EU residents or citizens.
2. The data subject (site visitor or customer) is based in the EU.
3. Any data processor—like a cloud service provider that provides analytics services—is based in the EU.

> Most importantly: The regulation also applies to organizations based outside the EU if they collect or process (1) personal data of individuals located inside the EU, or (2) personal data of EU citizens located anywhere in the world.

Even if your business doesn't ship or sell directly to the EU, chances are excellent that your systems **do** collect personal data on EU residents or citizens. This is because GDPR doesn't only apply to your *customers*—it applies to all *visitors* to your site. For example, if your site collects IP addresses from all visitors or if any site visitor can sign up for your email newsletter, you fall into the scope of the GDPR.

Some merchants who don't sell internationally have considered blocking all IPs from EU countries. This blanket blocking is an attempt to exempt themselves from GDPR by preventing anyone within the EU from viewing their site. We strongly recommend against that, for two reasons.

Gauge

2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

1. **Blocking EU IP addresses does NOT exempt you from GDPR.** As long as the data belongs to a EU citizen, GDPR applies—regardless of where that citizen is located geographically. If an EU citizen visits your site while on vacation in another country, GDPR still automatically applies. The increasing use of VPNs and proxies among regular web users makes this problem even more complicated.

2. **Google doesn't look kindly on blocking people from your website.** Blocking EU IP addresses isn't merely ineffective; it can actually be harmful. Doing so can negatively affect important like SEO —and therefore, negatively affect your bottom line.

To put it simply: **Because it has such a broad scope, GDPR essentially applies to all eCommerce merchants globally.**

What Do I Really Need to Know About Compliance?

The GDPR cares most about how you collect, store, and use personal data. The regulation requires you to:

1. Develop an inventory of all personal data you acquire.
2. Create plans and processes to comply when a user asks you to delete, correct, transfer, or limit their data.
3. Execute those plans when a user requests it.
4. Clearly explain to all users how you're using the data you collect and how they can submit requests about their own data.
5. Make sure any company or service that has access to user data you collect—including third-party companies and services—are GDPR-compliant.
6. Do all of the above in a timely manner (30 days).

1. What is Included in "Personal Data"?

The GDPR uses an incredibly expansive definition of "personal data," also called "personally identifiable information" or PII. Here is a short *and by no means comprehensive* list of what GDPR includes under that umbrella term:

i. IP addresses
ii. Login IDs
iii. Social media posts
iv. Digital images

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

v. Geolocation information
vi. Biometric information
vii. Behavioral user data
viii. Email addresses
ix. First & last names
x. Billing & shipping addresses

Here's the language the regulation uses:

> *"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); 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.*

The key phrase there is "directly or indirectly." The directly identifiable stuff is easy. However, there are lots of edge cases where it's possible to indirectly identify someone by what sites or pages they visit, or by which of your services they use. Many indirect cases won't be obvious. We highly recommend speaking with a qualified attorney to identify those.

What Are the Actual GDPR Mandates?

The GDPR consists of 99 articles. [You can read the full text here](#).

Fair warning: This is ***NOT*** a quick read. The text is full of stipulations, clarifications, and exceptions. Unfortunately, the GDPR isn't a regulation you can distill down to a "gist" without losing a lot of critical information. You really must read most of the document carefully to fully understand its scope and to understand what parts do (or don't) apply to your business.

> In GDPR, the devil is in the details. Know the details.

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

We recommend paying particular attention to the following Articles:

1. **Articles 5 - 23** detail the general rights of individuals covered by the GDPR.
2. **Articles 24 - 39** explain how the Data Controller/Data Processor relationship (like the Merchant/Development Agency or Merchant/Email Platform relationship) must work. These Articles also assign legal responsibilities within that relationship.
3. **Articles 44 - 50** explain how the transfer of user data to countries outside the EU must be performed.
4. **Articles 77 - 84** cover the all-important remedies, liability, and penalties of the regulation.

A Transfer of Power

A critical focus point is the list of rights the GDPR grants to EU residents and citizens.

> The user has both the right to know what data you're collecting, and the right to control what you do with that data.

Before this regulation, collecting user data was more like harvesting. Once a merchant or organization collected it, *they* controlled what happened to it. You could do just about anything with your user data, and the individual user had little to no recourse.

The GDPR changes all that. Data collection is now more like a loan than a harvest. The regulation grants the user **the right to know** what personal information is being "loaned" to the merchant. It also affirms each user's **right to own and control** their personal data.

This is a significant transfer of power. It throws a massive wrench into the existing machinery of data collection and processing for just about every eCommerce merchant.

List of Rights Granted

Again, there's a lot of nuance in the full regulation, so it's important to read it in full. For the purposes of this guide, though, we can grossly simplify the text down to six key rights granted to EU citizens and residents:

1. **Right of access** to their personal data - "What do you know about me? What do you do with that data?"
2. **Right to correction** of personal data - "That info about me is wrong. Fix it."
3. **Right to data portability** - "Give me my data so I can move it to another provider."

Gauge

2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

4. **Right to be forgotten** - "I don't want you to know about me anymore. Delete all data you have about me."
5. **Right to be informed** of data breaches - "I need to know about data breaches within 72 hours."
6. **Right to limit use** of personal data - "I don't want to participate in your retargeting campaigns or your big data analytics, but I do want to continue getting the email newsletter."

Third-Party Services

One of the more complex parts of the GDPR is the Data Collector/Data Processor relationship. Data Processors include your third-party service providers or business partners your company or site uses. Things like Google Analytics, your email platform, tracking pixel providers, remarketing services, and even your development agency. Under GDPR, you are responsible for ensuring that your third-party partners and services are GDPR-compliant.

Chances are, you know who these companies are. But do you really know what they do with the data you submit? Do they resell it to other companies? Process it for other services of theirs? You might be surprised by some of the answers, especially for free services. Data is a big business. We could make a slight change to that old Internet adage and it still rings true:

> "If you're not paying for it, you're not the customer; [your data is] the product being sold."

GDPR requires you to know exactly what happens to every piece of personal data you submit to your third-party partners. Under the regulation, you're responsible for any information that:

1. You collect, via your website, apps, and services.
2. Your third-party services collect through your site or company, either by:
    a. Recording activity through your site (think Google Analytics, web site logs), or
    b. Receiving data you collect and then transfer to them (think a user submitting their email address to your Email Marketing System for your newsletter).

> In essence, you're responsible for all personal data that originates through your site or with your company.

No matter where that data goes afterward, it remains a part of your responsibility. Your company must make sure that data stays secure and under strict control.

To do that, you have to be aware of where all this data goes after it passes into other hands. The GDPR requires that you create what is essentially a "chain of custody" for user data that includes third parties. There's a compelling reason for this: If there's a data breach at your third-party partner, it's *your* responsibility—not the partner's—to notify the affected users within 72 hours.

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

Technical Challenges of Compliance

Because this is such a seismic shift, compliance will not be simple. A lot of technology simply hasn't caught up to the regulation.

Here's a practical example: Say a user asks you to delete all of their personal data. The GDPR requires that you do so quickly—within one month—and also demonstrate to the user that you've done so. Many systems have no way to comprehensively delete the data of one specific user.

Consider how many systems you use to "process" data: marketing services, site logs, email databases, order and account records, customer service information, analytics, and so on. You're also responsible for informing any third-party services of the request, and then verifying that they've deleted that user's data too.

Now consider all of the backups, archives, and other databases you keep internally… and all of the backups, archives, and databases your third-party services keep. Under GDPR, the personal data must be completely erased from all of these systems.

As you can see, compliance with the right to be forgotten can be a very steep technical challenge. This is just one of the many logistical issues that the regulations can create.

This Is Making My Brain Hurt…

We know, it makes our brains hurt too! But it *is* possible to be GDPR compliant, so take a second to shake it off. Go get some fresh air, grab a coffee (or something stronger), or play with your dog. Once you've worked out the brain cramp, let's talk about Next Steps on your road to compliance.

Gauge

2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

Next Steps: Gauge Recommendations

Here's how you can get started.

1. Speak with a GDPR-knowledgeable lawyer

Every merchant's data collection, retention, and compliance strategy will be unique. Speaking with a lawyer about the specifics of your case is a must. It's not just a good idea, it's not just a recommendation, it's a must.

a. **Ask your lawyer** whether they're qualified to help you address GDPR-related challenges. If they aren't, find one who is.
b. **Don't wait** until after a GDPR issue comes up for you. At that point, it might be too late. An ounce of prevention is worth a pound of cure, especially when it comes to GDPR.
c. **Please Note:** The partnership between your company and Gauge is a Data Controller - Data Processor relationship. We aren't experts on GDPR, and we aren't qualified to conduct data audits, ensure compliance, or give compliance advice. Your best course of action is to work with a GDPR-knowledgeable lawyer. We're business owners too, and we don't like legal bills any more than you do. But for this issue, the stakes are very high indeed. Getting and following solid legal advice is the best way to prevent a difficult situation (getting GDPR-compliant) from becoming a potentially catastrophic one (owing millions in fines).

2. Perform a Data Audit.

a. **Conduct a thorough audit** of all the personal data you currently collect, share, process, and store via your company's website, apps, and services. Include:
    i. Data that's created when users interact with your site (like viewing a web page and generating a log file).
    ii. Data that's created when users perform any action that records information (like signing up for an email newsletter, placing an order, or talking to Live Chat customer service).

b. As you audit what data you collect, **document it thoroughly**. Once you start this process, you'll realize just how much data you collect for each visitor. It's a mind-boggling amount. This document will be long and complicated. Don't get discouraged as it grows.

Gauge

2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

GDPR compliance is very much like eating an elephant—the best way to finish it is one bite at a time. This documentation is part of the first few bites.

c. **Create a flowchart.** Use it to chart the types of personal data you collect and how it flows between your internal systems (site logs, CRMs, account records, etc.) and between your external third-party services (Google Analytics, your email platform, tracking pixel providers, remarketing systems, etc.) This flowchart will help you visualize that user data "chain of custody" discussed earlier.

d. **Determine what your personal data retention policy will be.** Unless you have a very compelling reason, GDPR severely frowns upon keeping user data forever. Determine:
    i. How long you actually need to keep each kind of personal data.
    ii. How you'll delete data once it's past your threshold of usefulness. Whenever possible, automate the data deletion process.

3. Identify your third-party partners and confirm their GDPR compliance.

a. **Make a comprehensive list** of all third-party partners and services who collect or receive personal user data.

b. **Reach out** to each one. **Create a GDPR-compliant Data Controller - Data Processor agreement** with all of them.
    i. Many third-party partners are now GDPR-compliant. They will be able to quickly draft a compliance agreement with you.
    ii. Other third-party partners may be drafting this type of agreement with your company for the very first time. It could take awhile for them to execute the agreement. Take this into consideration when planning your timeline to achieve compliance.
    iii. Some third-party services may not be able or willing to create a compliance agreement. In this case, consider switching providers or talk to a lawyer about your options.

4. Rewrite your privacy policy to detail your data collection practices.

Gauge

2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

a. **Draft a GDPR-compliant privacy policy**, and **consult a lawyer** to help you. This is one of the main elements of GDPR compliance, and it's the most public-facing. Because of this, a lot of care needs to be taken while drafting this document. Make sure you:
    i. Explain how users can opt out of certain data processes you perform.
    ii. Detail how users can submit a request to have their data deleted entirely.
    iii. Establish a way to record the user's consent to your privacy policy.

b. **Post your privacy policy prominently** on your website.

c. **Keep it up to date.** This will not be a one-and-done task. Your privacy policy will need to be a living document. Update it whenever there's a change to the data collection methods, tools, and processes you use. Ditto for your third parties.

5. Create and follow business rules for data collection and processing changes.

We predict that this will be one of the biggest business challenges of the new GDPR-centric world. Your entire team will need to build an organizational muscle memory. Whenever there's a discussion about about adding, removing, or changing technologies, you must ask yourselves, "Does this technology or process touch personal user data? How will this change affect our GDPR posture and compliance? Who will update our privacy policies?"

a. **Codify and formally document business rules and procedures** for changes that affect personal data processing.

b. **Distribute these rules** to all internal and external teams that handle personal data and data processing technologies. Teams like Marketing, Accounting, DevOps, Development, and any others that access personal data will need to have written procedures for maintaining GDPR compliance.

c. **Example:** Marketing wants to add a new referral or affiliate tracking system to the site. As you assess your technology options, your team will need to identify what personal data is being recorded by or transferred to the provider. Consider questions like:
    i. When you receive a "right of deletion" request from a user, how will you pass that request to the provider? Who will do it, and does the service have a documented request procedure?
    ii. How will you verify that they've complied with user requests?
    iii. How will your privacy policy need to change, and who will update it?

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

iv. Are they already GDPR-compliant? Can they easily create a Data Controller - Data Processor agreement?
v. What's their procedure if they have a data breach?

6. Hire a third party auditor to confirm full compliance.

GDPR compliance is complicated. It requires a massive shift in organizational thought, and it's technically complex. Chances are, you won't get it 100% right the first time you roll out your compliance plan.

a. **Hire a third-party auditor** to examine your GDPR compliance setup. Fresh eyes can more easily see any gaps and edge cases you may have missed. Again, we're business owners too, and we know what it's like to have to choose your financial investments wisely. But hiring a third party expert is an investment worth making. It's the best way to confirm your compliance so you can sleep well at night—and avoid nightmares of hefty fines and protracted legal battles.

b. **Have your in-house GDPR expert work with this auditor**. Speaking of that...

7. Assign a team member to become your in-house GDPR Guru.

GDPR compliance is an ongoing business process. Keeping lawyers and third-party experts on retainer to maintain your GDPR compliance is expensive and impractical. Remember, there are strict timelines for responding to requests. You need an informed team member to be your point person for all things GDPR-related.

a. **Designate a Data Protection Officer (DPO).** Assign someone in your organization to be responsible for:
    i. Responding to requests
    ii. Keeping documentation up to date
    iii. Liaising with third parties
    iv. Addressing any compliance questions or issues as they arise

b. **Train them** in GDPR compliance.

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265

i. We highly recommend the book *Be Ready for GDPR* by Punit Bhatia. It's a comprehensive guide on executing GDPR compliance for organizations of all sizes.
ii. Consider a DPO certification. Many are available. Look for courses that bundle training, certification, and access to resources after certification.

c. **Read Articles 37 - 43** for more information about Data Protection Officers.

I still have questions about GDPR. Can we talk?

Absolutely! Because this is a new regulation, we're offering you a free consultation as a part of our partnership relationship. In this meeting, we can discuss the information covered within this guide and answer questions about it. Reach out to your Gauge Project or Account Manager to schedule this consultation.

Please keep in mind: we aren't experts on GDPR, and we do not conduct or offer GDPR data audits, compliance verification services, or give legal advice.

Gauge
2413 Bull Street, Savannah, GA, 31401
www.gauge.agency
(912) 228-3265