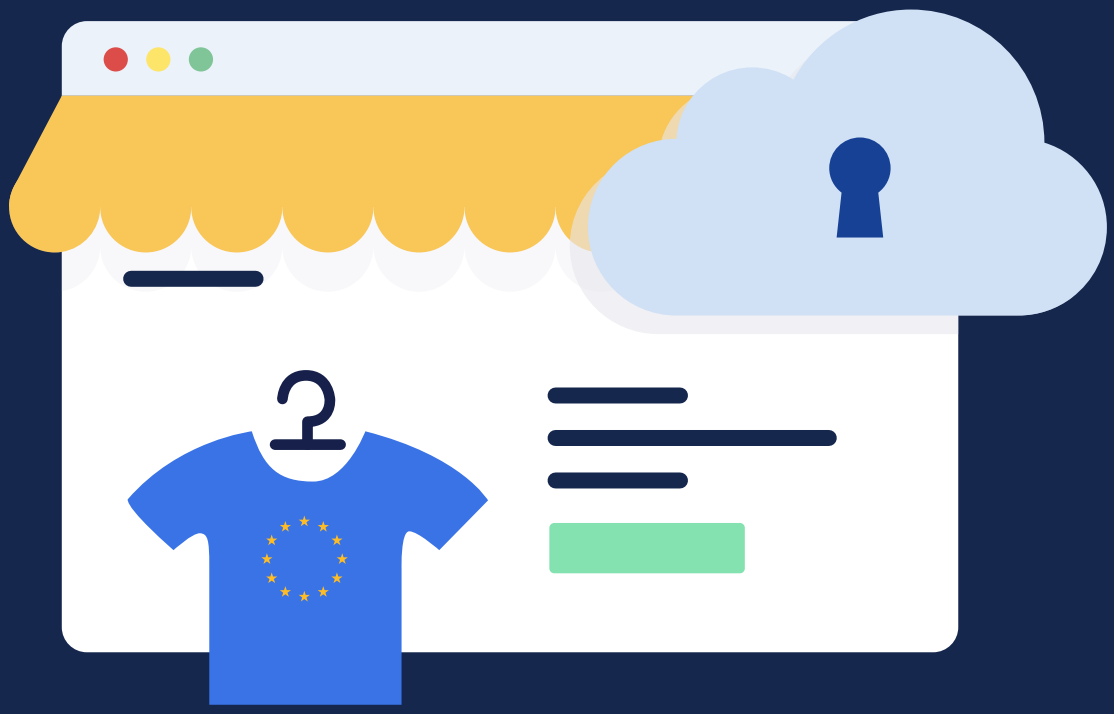
freshworks

# The **eCommerce Guide** to **GDPR**

## How to **Ensure Compliance** and a **Competitive Edge**



# Table of Contents


| | |
|---|---|
| Executive Summary | 03 |
| What is the GDPR? | 04 |
| What Does the GDPR Mean to eCommerce? | 06 |
| Challenges to Overcome | 10 |
| Harness the Cloud to Realize Opportunities | 10 |

# Executive Summary

Big changes are coming when it comes to protecting consumer data, and just about every eCommerce business will be impacted. The General Data Protection Regulation (GDPR) is a set of regulations that determine how companies and organizations throughout the European Union (EU) capture, process and store personal information. And it applies to all business regardless of size, location or where data is processed.

This white paper outlines the regulations requirements, challenges facing eCommerce companies, and the opportunities afforded to those that choose the right approach to satisfying the GDPR.

# What is the GDPR?

The GDPR – which replaces the Data Protection Directive in effect since 1995 – applies to any organization dealing with customers residing in the EU and will go into effect on May 25, 2018.

The main goals of the GDPR are to give individuals more rights and control over their personal data, and ensure this data is secure. Specifically, the GDPR regulates the collection, storage, use, and sharing of "personal data," defined as any data that relates to an identified or identifiable natural person. Note that the regulation doesn't distinguish between a person's private, public, or work roles as relates to data.

Personal data can include, but is not limited to, the following:

- Online identifiers (e.g., IP addresses and cookies)
- Employee information
- Sales-related data
- Customer service data
- Credit and debit card numbers
- Customer feedback
- Physical details
- Social media posts
- Cultural identity
- Location data
- Biometric data
- Loyalty program records
- Financial information

In fact, any information that is somehow linked and tracked back to an individual – even if through an account number, unique code, or pseudonym – is considered personal data. Moreover, you need to follow more stringent rules when it comes to processing certain "special" categories of personal data, such as that reveals a person's racial or ethnic origin, or concerns their health or sexual orientation.

Under the GDPR, individuals can demand to know exactly how their data will be used, request access to and get a copy of their stored data, and even request it be corrected or removed from a company's systems. They can also restrict or choose not to allow their personal data to be subject to automated processing, and can even demand that it be erased (i.e., they have the "right to be forgotten.") If they choose to do so, they can move their data between companies.

Here are more specifics about three key areas of GDPR focus:

1. **Individual's rights.** Consumers (and your employees) have a right to know who is collecting data, for what purpose, and how long are you (and your partners and service providers) are going to keep it.

2. **Security measures.** You and your partners/service providers need to put in place appropriate security controls and satisfy new obligations. Perhaps most importantly, your company can't pass off responsibility for the security of consumer and employee data to a third party.

3. **Breach notification.** Within 72 hours of a breach occuring, your company must notify the authorities and, in cases of high risk, affected individuals as well.

## Six Key Principles

In addition to addressing the previous three main areas, your organization – and your partners/service providers – need to comply with the following six key principles if you collect or process personal data:

1.**Demonstrate transparency, fairness, and lawfulness** in how you collect, handle and use personal data. You clearly communicate to the consumer about how you are collecting or using personal data and you will need a "lawful basis" to process that data.

2. **Limit the processing of personal data to specified, explicit, and legitimate purposes.** You won't be able to reuse or disclose personal data for purposes that are not "compatible" with the purpose you originally collected the data

3. **Minimize the collection and storage of personal data.** You should only collect and store what is adequate and relevant for your intended purpose.

4. **Ensure the accuracy of personal data and enable it to be erased or rectified.** You will need to ensure that the personal data you store is accurate and can be corrected if need be.

5. **Limit the storage of personal data.** You must only retain personal data for as long as necessary to achieve whatever you intended when you collected the data.

6. **Ensure security, integrity, and confidentiality of personal data.** You must use technical and organizational security measures organization to keep personal data secure.

Fail to comply with any requirements of the GDPR and you could be fined upto €20M up to 4% of your global revenues. That's a steep price to pay, and one your business likely can't afford, as it can cost you short-term revenues and long-term customer loyalty.

### Moving Data Outside the EU

The GDPR requires that organizations transferring data outside of Europe have a lawful basis to do so and use "appropriate safeguards." The most common ways of legitimizing such transfer include:

- Entering into a standard contract -- known as a Model Clause as defined by the EU -- with its customers.
- Self-certifying for the EU-US Privacy Shield to key protections of the data (for data transfer to US).
- Adopting Binding Corporate Rules

## What Does the GDPR Mean to eCommerce?

While the GDPR will require changes within your business, the biggest change may be the fact that you can't just collect and use data as you wish. To that end, complying with the GDPR will require unprecedented levels of data management, transparency, and security.

## Data Management Requirements

Specifically, this is what you can expect:

- You need to get a consumer's active opt-in for all one-to-one communication on any channel – even Skype, Messenger, Facebook, and Instagram – even if you've previously interacted with this individual.
- If you market to children under the age of 16, you need parental consent to process their child's data.
- You will need to focus more on discarding data vs. keeping it because you can only keep data if you have a clear, ongoing use for it.

The GDPR even applies to the ways you profile individuals through automated processing. Typically, this falls into the following categories:

- **Economic situation:** Tracking user purchases, price percentiles and related calculations.
- **Personal preferences:** Whether captured explicitly or implicitly through tagging.
- **Behavior:** Affinities for products, brands or categories, whether captured explicitly or implicitly.
- **Location/movements:** Such as through IP addresses and cookies.

If you carry out large-scale behavioral targeting, you'll need a Data Protection Officer on staff to formally oversee all aspects of your data management process.

## Transparency Requirements

Whether you use algorithms, machine learning, personalization, or some other technology to process personal data, you need to first notify and give them an opportunity to opt-out of it. Simply put, you need to show each individual what you know about them, where data is sent and who is responsible for storing and processing it, how you intend to use that information, how long you will store it, and whether you will be transferring outside the EU.

A prime example is the shopping cart and checkout process. You will need to clearly state which payment gateway provider is processing payments for you and how personal data such as credit card details, email address and physical address will be processed and stored.

To collect data, you need to give consumers and employees a very clear and detailed view of all their options as relates to submitting their personal data.

If you are using consent as the ground for such processing, remember that as per the GDPR, consent must be:

- Freely given
- Informed
- Specific
- Unambiguous

The following also apply if consent is used as the basis for processing the data:

1. Even if you just want to share a person's browser history with a third-party company, you need to get consent to share that data. When asking for consent, along with providing clear "yes" and "no" options, you'll need to provide:

- Name(s) of the company/companies you'll be sharing the data with
- How the data will be used
- How long the data will be stored
- How the individual can withdraw consent and access their data

2. If you contact or interact with prospects or customers through more than one channel – e.g., phone, email, SMS – you need to provide options for individuals to give consent for each channel. You also need to give an option for the person to change their choices going forward.

3. And you will need to maintain detailed records of all consent (see records of processing activities under Article 30[1] of GDPR).

GDPR rules around consent apply only if your organization is relying on consent as the basis for processing personal data. In other words, Consent is one way to comply with the GDPR, but not the only way.

## Security Requirements

Moreover, your company is now liable for any violation of the GDPR when it comes to how your business handles, processes, and stores data associated with your prospects, customers, and employees. Even if you outsource some of those tasks to a third party – such as to process payments, send emails, or to store data – your company is ultimately responsible. That means you need to ensure that any partners and third parties also comply with the GDPR. Moreover, you need to share third-party details and contact information when you collect personal data.

**Controllers vs Processors**
A data controller is who determines the "purposes and means of processing the personal data." A data processor is any entity that processes data on behalf of the controller, which can include storing the data, such as in the cloud.

Your company will also need to promptly notify individuals of any data breaches, and maintain qualified data protection officers on staff. It's also wise to train your employees on the GDPR. In particular, your customer service team should know how to respond to consumer requests for insight into how their data is being used and for access to their data.

You and your partners need to be able to detect any security breach within 72 hours of it occurring, and notify a "supervisory authority" within your business as soon as it's detected. If a data is "likely to result in a high risk to the rights and freedoms of natural persons," you also need to notify those affected "without undue delay" after becoming aware of the breach. Along with the notification, you need to explain the consequences of the breach and what you have done to date to address it. Here again it's essential that you train all employees on what constitutes a data breach.

Note that the ePrivacy Regulation is a standard intended as a complementary regulation to GDPR, which actually covers some areas more specifically, notably cookies and direct e-marketing. Users will now be able to change cookie tracking within their browser so they no longer need to deal with pop-ups asking for consent for use of cookies on individual sites. Online communications providers -- such as Gmail, Facebook, and Skype -- must now satisfy the same customer data safety requirements as traditional telecommunications providers.

## Challenges to Overcome

Handling individual requests to access, correct, erase, or restrict the processing of their data could quickly overwhelm your customer service group and other departments. After all, when someone makes one of these requests, the GDPR states you need to respond within a month. It's easy to envision that the general public will become more aware of the GDPR as May 2018 draws near. That knowledge will likely lead to more requests about their data.

Depending on the person's request, you may need to explain all the ways the data is being used, provide the reason you are storing the data, or immediately make changes to it or even delete it from all systems. If someone does request to "be forgotten," you will need to first confirm that no legislation outweighing the GDPR requires you to maintain that personal data. If you are not required to keep the data, you must remove it from your systems (and ensure you notify your partners to remove it from their systems). Imagine making sure this happens across all systems – even each employee's hard drive where this data might be stored.

In addition to protecting each individual's rights, giving them more control over their data, and protecting that data, your organization will need to be able to detect and assess security threats and breaches to meet the GDPR's breach notification obligations. Your company must also be able to prove that it is addressing all GDPR requirements.

## Harness the Cloud to Realize Opportunities

It may seem daunting to comply with the GDPR, but doing so is well worth it. In fact, compliance will ultimately translate into a benefit for your company. Your prospects, customers, and employees will appreciate your commitment to giving them more control over their data. In fact, the regulation might even open doors for you to better your customers, and drive more business from them. Consider that "50% of consumers abandon their online purchases"[2] because the customer journey does not reassure them regarding what will happen to the personal information they provide. Take a proactive approach to addressing the GDPR requirements and you can gain a huge boost in consumer confidence and loyalty.

One way to do this without overburdening your business is to take advantage of cloud-based options for essential customer-facing operations such as customer service and sales. Compliance cloud solutions help:

1. Alleviate the load of meeting compliance
2. Address changing and new regulations and standards
3. Ensure flexibility to easily change suppliers/vendors
4. More easily respond to and meet data requests from subjects customers

By partnering with a trusted cloud-based provider who is taking the required steps to comply with the regulation, your company can much more easily satisfy the GDPR and future compliance requirements.

## Conclusion:
## Make Your Business the eCommerce Vendor of Choice

Data collection has grown exponentially over the years, and your eCommerce business likely calls upon various means to collect, mine and use this data. So, it stands to reason that you are being called upon to take more responsibility in protecting this data and respecting the rights of consumers to control their own data. Taking advantage of cloud-based solutions can ease the process of complying with the GDPR and its many facets. In fact, such solutions can give your business a competitive edge, making it easier to comply with new and changing regulations with little effort on your part.

Freshworks -- the leading provider of cloud-based customer engagement software -- will be compliant by end of May 2018. Our compliance means you can be confident we are committed to ensuring the Freshworks platform satisfies the standards and regulations that matter.

For more on the GDPR and what can you do about it, check out our Resources.

**References**

[1] http://www.privacy-regulation.eu/en/article-30-records-of-processing-activities-GDPR.htm
[2] http://www.extens-consulting.com/en/behind-gdpr-compliance-opportunities/