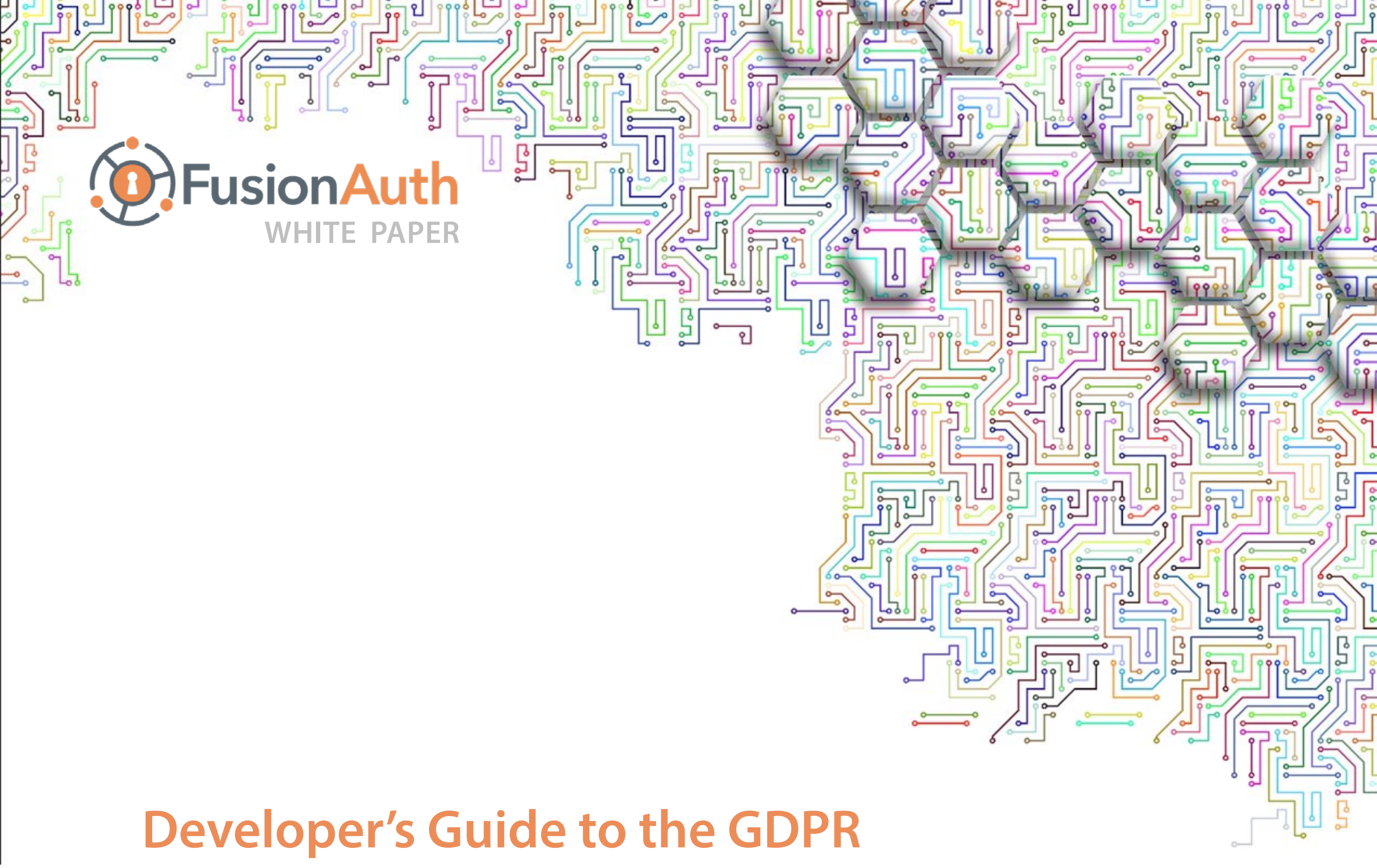


FusionAuth
WHITE PAPER

Developer’s Guide to the GDPR

The who, what, when, where, and why of the GDPR for developers.

The General Data Protection Regulation (GDPR) was adopted by the European Parliament in 2016 and is designed to address consumers’ concerns about the collection and use of their personal data. It is a binding regulation for all members of the European Union (EU) and replaces the 1995 Data Protection Directive[1]. More complete than the previous directive, the GDPR unifies the complex web of data protection regulations throughout the EU and introduces severe penalties for companies fail to comply.

For developers, the GDPR provides a framework of requirements that will impact the business processes and architectural roadmaps for any application. In short, it codifies a set of “user’s digital rights” and will have a dramatic impact how applications collect, store and utilize information they obtain about their audience. In the following pages we will outline the basic tenets of the GDPR and clarify how they will impact a developer’s role in application development.

Introduction

Although the GDPR was approved and adopted on April 27, 2016, it included a two-year transition period and becomes enforceable on May 25, 2018. After that date, companies who are found in violation will face severe penalties as high as $24 million or four percent of their annual global revenue, whichever is greater. Clearly, this is a regulation that can have a dramatic impact on a company's revenue.

Far more than a set of reporting requirements, the GDPR defines a set of functional specifications companies need to build into their applications. System architecture and development teams will be at the forefront of making sure their applications, sites, and systems are compliant. It's essential for developers to understand these specifications and how they will impact the business processes in their applications.

There are many resources[2] that examine the details of each section of the GDPR, so we won't go through them point by point. We do want to outline how developers will be impacted by the regulations, and how they should make GDPR considerations part of their workflow.

We'll cover:

Who does it impact?

The GDPR applies to all companies that offer goods or services to, and/or monitor the behavior of EU data subjects, regardless if they have a physical presence in the EU. It will impact any company building an application that collects personal information on a data subject (a person). For this paper we will focus on software development, but in reality the requirements of the GDPR apply to any type of business or program that collects and controls personally identifiable data in any way, whether manual, electronic, observational, or even telepathic if you want to look deep into the future. If you collect data that is connected to a person, it impacts you. There is a notable qualifier that the data subjects be "in the Union" but this is already being interpreted in a variety of ways. Some say it only applies to citizens of the EU, while other sources state that any data generating event that occurs within the boundaries of the EU are included. It's also not clear how the regulations will apply to customers who move to the EU after engaging with a company[3].

What is clear is the GDPR doesn't just apply to companies based within the EU, it applies to all companies who have interactions with people connected to the EU in some capacity, whether physically or virtually. With a population of over 500 million, third largest after China and India[4], and some of the world's most well-traveled citizens,[5,6] there's always a good chance that you'll be interacting with someone who's covered.

What developers need to know

Developers should expect that the GDPR will apply to their projects and that they need to consider how to comply with these regulations sooner rather than later. Much like car manufacturers and California emission standards, it's better to build for stricter standards that will be compliant anywhere than to aim low and risk legal fines in addition to the costs and time required to rebuild non-compliant systems.

Developers should also be ready to accept the role of "data protection officer"[7], serving as the gatekeeper for appropriate data management policies. Similar to a compliance officer, the data protection officer (DPO) has a comprehensive understanding of data management requirements and how they are implemented in each project. It may not be cost-effective for many companies to assign a single person as a DPO, so developers that are prepared to learn and understand the requirements will be more valueable to their team.

What data are we talking about?

Next, let's cover the specific data the GDPR applies to. With thousands of possible data points that can be collected, what data is included and excluded? Traditionally, companies built security around explicit user data like name, address, phone number, and credit card numbers. The GDPR defines a much wider scope encompassing any information related to a natural person (a 'data subject') that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, social network identities or posts, bank details, medical information, or a computer IP address. If you can connect it back to a person, it's covered.

Obviously this creates challenges—the first reason to collect data is to tailor a user's experience based on their preferences and behavior. In modern applications it is common practice to create a marketing profile based on viewing, interaction and purchase history. It is less common to ensure that all that collected data can be completely disconnected from their real-life identity. In fact, the over-zealous collection and overuse of personal data is what prompted privacy concerns with consumers worldwide.

What developers need to know

One of the basic concepts of the GDPR is this: Data privacy must be designed into the development of business processes for products and services. This means data privacy needs to be incorporated into the requirements and scope of all business processes in an application. This report[8] by the European Union Agency for Network and Information Security provides an effective introduction to developing privacy-friendly systems and services. Developers should be familiar with these concepts, and be able to identify business processes that ignore data privacy concerns.

Conceptually, this should be a relief to developers—it's easier to build functionality into an application from the start than it is to add it right before launch. (That would never happen, right? #sarcasm) In reality, it will take effort to ingrain data privacy throughout the product development pipeline. If no one else is doing it, find a way to bring attention to privacy concerns and make sure they are addressed.

Another important concept in the GDPR relates to WHY data is collected. It's not uncommon to hear a product manager say "Just collect all the data you can and we'll figure out a way to use it later." Under the GDPR, that's no longer allowed—any data collected needs to be for a specific purpose. You can still collect the data that you want, but it has to be for a defined purpose, the user needs to be informed, and they need to explicitly agree to it. This isn't so different from CAN-SPAM regulations, but it covers a wider scope of data that has not been protected in the past.

Developers also need to start structuring their data processes with effective pseudonymization strategies. You'll avoid a lot of privacy issues if you associate user data with an efficient pseudonym instead of personal data like an email or phone number. Different from anonymization which destroys user identifiable information, pseudonymization is a step that ensures collected data cannot be connected to a specific person without and additional key. User IDs, tokens, and session IDs are common ways to abstract data from a unique individual.

The GDPR does not restrict the types of applications and experiences developers can build, but it does place the need for user privacy ahead of the business needs of the company. You can still build your app, you just need to make sure you build privacy controls into it from the start.

When does it apply?

The GDPR becomes fully enforceable May 25, 2018, so if you haven't already, it's time to start incorporating its principles. In existing applications, many of the requirements should be easy to implement. A good first step is to review your terms of service and registration process. Make sure you inform your users what data you will be collecting and how it will be used. Other provisions of the GDPR may require a more detailed review of business processes, and take additional development time to bring them into compliance. Any new applications should already be incorporating the GDPR to be compliant at release.

What developers need to know

We mentioned this in the previous section but it's important enough to clarify here as well. Any application needs to obtain the user's explicit consent before collecting any data, and it must be clear from the very beginning how it will be used. Burying a data use policy deep in paragraph 23.r3.A of the terms and conditions will no longer be sufficient. All data policies must be explained in clear language and easily accessible for users to review and withdraw from at their discretion.

The GDRP also specifies a user's right of access to their data. This means the user should be able to obtain:

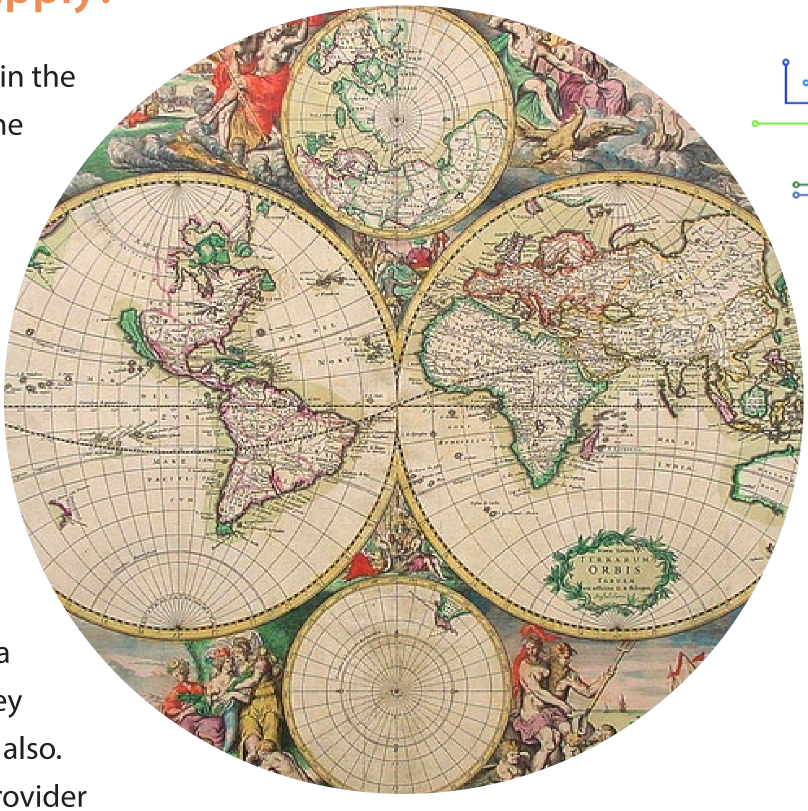
- A copy of their actual data
- A description of how it is being used
- An explanation of how algorithmically formulated data points were calculated.

The last point will be the subject of much debate due to the use of advanced machine learning systems. It may be difficult to clearly define how specific data points were derived from a data set. As those details are being resolved, developers should at minimum be prepared to provide access to existing data in a timely manner when requested.

Related to a user's right of access is their right to request the erasure of their data. Developers should know how to erase or disconnect all of a user's data from their identity. There are restrictions on why a user can request this, but it is important to be aware of the possibility.

In case of a data breach, the GDPR states that a company has a maximum of 72-hours to notify the user once the company becomes aware of unauthorized access. As a developer, it will be essential to have a notification plan in place and ready to execute in case a breach occurs. This should at minimum be a written protocol, but could also be a programmatic solution.

Where do the regulations apply?



We touched on geographic requirements in the section above. Now we'll address where the regulations apply within your application flow. This is explicitly defined—all of the GDPR regulations apply every step of the way between a company and a user. Data privacy must be consistently protected from the first touch-point on your website through the final follow up survey and every server, database, and reporting dashboard in between. This also means that if your company uses a third-party processor for a component of your product or service, they are required to protect your users' privacy also. Both your company and the third-party provider could be fined for any violations. Read below for specific questions you should ask your third-party providers to help assess if they are GDPR compliant. Don't rely on the word of your sales or account representative.

What developers need to know

We'll say it again: User data privacy must be protected every step of the way from first touch-point to final log out. No excuses. Whether you build it or use someone else's tools, you are responsible.

As a developer, it's essential for you to have detailed discussions with third-party providers about how they are GDPR compliant. Take the time to talk with developers who are familiar with the code and architecture of their systems. Make sure you understand how they process, store and manipulate your data. Also consider if the integration between your systems exposes data unnecessarily.

Coordinate with any third-parties to make sure you are able to provide users with their data if requested. The GDPR allows users the right to request any data that can be linked back to them. This includes provided data (emails, phone number) and observed data (behaviors, usage patterns). Application developers should be prepared to coordinate with third-party providers to fulfill requests in a timely manner.

Why does this matter?

This paper covers the basic tenets of the GDPR. Take the time to become familiar with the all the details. Every day, advances in machine learning and AI are revealing additional opportunities to extract business value from user data. At the same time, users are becoming more concerned about data privacy and want to have control of how their data is used and managed. It's clear that these conflicting trends will continue to evolve together. It will be essential for companies to maintain their users' trust to able to collect and utilize their valuable data. Developers who understand data privacy and how to maintain it while meeting business requirements will be a valuable asset to their firm.

The bottom line is that developers should understand user privacy issues will not be going away, and most likely will become more detailed and restrictive in the coming years. Get comfortable with the evolving best practices of data privacy, and be sure to view data collection and storage from both business and user perspectives.

The GDPR is a Specification Roadmap

Will all the regulations, requirements and restrictions contained in the GDPR, it would be easy to consider it a massive headache on the path to system development. This isn't the case at all. In fact, the GDPR saves developers from even more headaches by laying out a comprehensive user data management plan. Think of it as an architecture roadmap that isolates data management into a discrete component of your application. Use it to create a data management strategy that serves your business plan and respects your users' privacy.

What Developers Should Do Next

The next steps for any developer are straightforward.

- **Research:** Take advantage of the information below to understand the details and implications of the GDPR.
- **Evaluate:** Review your existing applications, in-progress projects, and third-party partners to determine where you stand.
- **Get Organized:** Prepare your team to apply these data management principles to all your future projects.
- **Follow Us:** If you are interested in the GDPR, identity and access management, or data security in general please contact us or sign up for our newsletter. We'll be hosting sessions and events throughout the year and would love to have you join us.

Contact us through Email

Follow us on LinkedIn

Follow us @FusionAuth

Follow us on Github

What to Ask Third-Party Providers

If your application takes advantage of third-party tools and components to add functionality or track user information, they should be considered part of your data management strategy. Take the time to ask what processes they have in place to ensure GDPR compliance, including their security framework and how they manage data. If they do not have a clearly defined, documented strategy you could be exposing your company to additional risk. Here are a few questions to get your discussion started:

Q: Where are their servers and computers physically located? Can you choose a location?
Even if a service is cloud-based, the physical location of the servers could impact how the GDPR applies to you.

Q: How does their platform pseudonymize user data as it integrates with external systems?
A: When user data is integrated with their system, is new data personally identifiable, or connected to an alias? The more disconnected, the safer it will be.

Q: What is their protocol for notification in case of a data breach?
This is vital since your company will need to notify your users within 72 hours. Your provider should be able to notify you so you can comply.

Q: How do they comply with your users' right of access and erasure?
How will your company coordinate efforts so users can view their data and request data erasure?

Questions for Identity and Access Management Providers

If you are considering an identity and access management solution, here are additional questions that will provide deeper insights into how they address security and data privacy.

Q: What are their default password constraints, and are they adjustable?
This is a basic question to begin. They should have a diverse set of requirements and be able to adjust them if needed.

Q: What password hash do they use, and do they use unique salts and/or peppers?
Modern standard hash algorithms like SHA-3, Bcrypt, PBKDF2 and Scrypt are designed to make brute force attacks much more difficult. If they are using standard MD5, run.

Q: How difficult is it to increase their hash's intensity for new users? Existing users?
Hackers will always develop more sophisticated techniques, and computer processing power is always increasing. Will their system be able to adjust to protect against evolving attacks?

Q: Is their database directly accessible from outside your system?
Limiting direct access to the database is a first line of defense against exploits and attacks.

Q: Are requests within their system secure? How robust is your authentication for internal API requests?
Using a variety of authentication credentials within the system creates an added layer of security and limits what can be done if a hacker gains access.

FusionAuth and the GDPR

Is FusionAuth GDPR-compliant? Of course. We've been preparing our clients for the GDPR to go into effect since it was first adopted. Fortunately, we developed FusionAuth from the beginning with even stricter regulations in mind, so we didn't have to go far to comply. We fully agree with these regulations and feel they provide the basic guidelines that any application or system should follow with their users' personal data.

Data protection: When clients have us host FusionAuth for them, it is always protected by strict server security, firewalls, and encryption.

Data isolation: FusionAuth is single-tenant. This provides two main benefits. First, it means that your user data is not commingled with other companies. Second, we can host FusionAuth anywhere on nearly any server. This allows us to isolate your user data in Germany for example.

Data retrieval: FusionAuth provides an easy API to collect any data it contains for a user. This includes any custom data you might have provided to FusionAuth.

Data deletion: In addition to retrieving user data, FusionAuth provides an API to quickly delete all user data, including behavior data such as IP addresses and login timestamps.

User data abstractions: FusionAuth provides the ability to pseudonymize user data through the use of opaque tokens and complex user ids. Without access to the FusionAuth database, these ids would be impossible to determine who the user is.

Password constraints: FusionAuth provides a complete set of password constraints that comply with the latest NIST regulations. Additionally, FusionAuth provides a method of configuring the password hashing algorithm including a method of upgrading the algorithm used when users log in.

Breach notification: FusionAuth has a strict breach notification policy that allows any company to quickly notify users and comply with the GDPR. We make every effort to notify our customers of any breach (or even a suspected breach) within 24 hours.

FusionAuth

Learn More About FusionAuth

For any application, CIAM is a necessary component, but it's not the core value of your application. It's much like the front door to a brick and mortar store. It doesn't make money, but if weak and insecure it increases your risk of losing everything you've built. You don't build the locks for your front door, so why ask your team to focus on user management?

Our identity and access experts deal with user CIAM every day so we understand the complexities and subtleties that modern user management demands. We are focused on staying ahead of current best practices so we can provide the most secure and flexible solution on the market. We even build in additional flexibility that allows FusionAuth to increase it's security as threats become more sophisticated.

Find out more about FusionAuth, and how it allows your team to focus on your application's core value proposition.

Links and Resources

General Data Protection Regulation Text

1. **Official Text of the General Data Protection Regulation**

   Eur-lex.europa.eu - view >>

- **GDPR Text - Neatly Arranged**

  Gdpr-info.eu - view >>

- **Wikipedia Summary of the GDPR**

  Wikipedia.org - view >>

2. **Basic Web Search for GDPR**

   Google.com - view >>

References

3. **Are We Covered by the EU GDPR? A Warning for U.S.-Only Businesses**

   LockeLord.com - view >>

4. **Size of European Union Population**

   Europa.eu - view >>

5. **These Countries Have the Most Well Traveled Citizens**

   CNTraveler.com - view >>

6. **Countries Whose Citizens Travel the Most**

   WorldAtlas.com - view >>

7. **Role of Data Protection Officer**

   GDPR-info.eu - view >>

8. **Introduction to Developing Privacy-friendly Systems and Services**

   Enisa.europa.eu - view >>

Additional Information

- **General Data Protection Regulation (GDPR) requirements, deadlines and facts**
  CSOOnline.com - view >>

- **What is GDPR? The need-to-know guide**
  Wired.co.uk - view >>

- **What is GDPR? Everything you need to know about the new general data protection regulations**
  Zdnet.com - view >>

- **Yes, The GDPR Will Affect Your U.S.-Based Business**
  Forbes.com - view >>

- **What You Need to Start Doing Now to Be Ready for GDPR**
  AdWeek.com - view >>

- **How Will the GDPR Impact Third-Party Lead Generation?**
  CMSwire - view >>

- **The Media Agency's Guide To GDPR And EPrivacy**
  Ad Exchanger - view >>

- **MarTech Today's Guide to GDPR — The General Data Protection Regulation**
  Martech Today - view >>