GDPR 101

What You Need to Know

Zettaset

Table of Contents

What is the GDPR?

GDPR is short for General Data Protection Regulation. It was formally adopted in April 2016, and goes into effect on May 25, 2018.

The GDPR is a set of regulations that aim to strengthen and unify data protection rules for individuals (referred to as "data subject") within the European Union (EU), and includes protection for both citizens and residents. The GDPR applies to all companies that do business with (and use personal data from) the EU. That includes a large proportion of enterprise companies headquartered in the US, Canada, China, Japan, and other non-EU countries. Whether you're just hearing about the GDPR for the first time or you're beginning to make preparations, this guide will help you on your GDPR journey.

You can view the complete text here, but be warned — there are countless chapters, articles, recitals (used to establish context), and over 250 pages of legal jargon.

What is the GDPR's purpose?

Why was the GDPR created? For one, it's an update to existing data protection regulations that date back to the mid 1990s. Today's world is very different, and the GDPR seeks to address these technological, geopolitical, social, and cultural changes. Privacy and security are being treated as fundamental rights in Europe. The GDPR strives to ensure that the rights and freedoms of an EU citizen or resident aren't put at risk — regardless of where their data is stored. Data breaches and improper handling of information are the new normal, and we've seen, time and again, the negative impacts cyber leaks can have on individuals.

Any company regardless of its physical location must abide by these rules when dealing with EU resident data.

That being said, the GDPR has two main goals. First, the regulation will establish a single set of data protection rules across the EU. Because the GDPR is an EU regulation, it will take effect for all of the EU's 28 member countries. Individual countries may choose to enact additional regulations building upon the GDPR, but cannot alter or remove any parts of the regulation. Although it's an EU directive, any company regardless of its physical location must abide by these rules when dealing with EU resident data.

Second, the intent of the GDPR is to give individuals greater control over their personal data. This includes sensitive information such as medical records and financial data, of course, but also any information that can be used to identify an individual. If you ask customers or prospects for their

gender or dietary preferences, you're on the hook. Other examples include first and last name, email address, ID number, physical addresses, and online identifiers such as IP addresses and cookies. The GDPR applies equally across all strata of society; there is no distinction between data collected on individuals, employees, or public figures. Employees, customers, vendors, and partners are treated equally.

The regulations also establish rules enabling the free movement of personal data within the EU and across the world. The goal is to create a unified system of data protection and cooperation so that personal data "shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data." Cross-border flows of personal data have increased as EU member countries have integrated economically and socially.

The exchange of personal data between public and private organizations has also grown. It is through the GDPR, then, that authorities seek to build a strong, cohesive, cooperative framework to protect the individual in an increasingly connected world. The US Congress is receiving mounting pressure to adopt a national data security standard of its own. This would eliminate the gaps, overlaps, and contradictions with the many state laws and requirements that businesses must currently obey.

What kind of data are we talking about?

Personal data doesn't just mean sensitive information — it signifies any data that can, directly or indirectly, identify an individual. According to the law, this includes identifiers such as:

- Names
- Identification numbers
- Location data
- Online identifiers (IP addresses, cookies, etc.)
- Physical characteristics
- Physiological factors
- Genetic information
- Mental status
- Socioeconomic data
- Cultural identities

The GDPR makes no distinction between data from private, public, or work roles.

Who does the GDPR apply to?

The GDPR applies to all companies that gather any type of personal data from EU citizens and residents. There is a current misperception that the GDPR pertains only to companies with 250+ employees, but in reality the regulations apply to organizations regardless of size or physical location. If you control and/or process personal data of even one EU subject, the GDPR applies to you.

Data controllers and data processors

The GDPR's predecessor, the Data Protection Directive, holds only the data controller liable for compliance. If a data breach occurred, the controller was legally responsible for a cyber incident caused by the actions of their data processor. Now, data controllers and data processors are both obligated to comply with data protection requirements. This is a new concept. What is the difference between a controller and a processor? It comes down to how you handle the data.

Data controller

This is the person (or organization) determining the purposes and methods for processing personal data. The controller has more responsibilities than the data processor. The GDPR defines a controller as:

> *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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

Data processor

The data processor, on the other hand, performs any operation(s) on personal data. This can be done manually or it can be automated. If you record, organize, structure, store, alter, combine, retrieve, use, disclose, transmit, disseminate, erase, or destroy personal data, you're a data processor. The GDPR defines a processor as:

> *A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

The distinction between controller and processor is an important one, as each have different compliance requirements. It's true that data controllers carry greater responsibilities and liabilities, but data processors now face legal obligations, too. Processors must observe GDPR mandates or risk penalties and loss of business opportunities. Article 28 states:

> *Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*

This means that the data processor's customers (the controllers) are asked to work only with processors that comply with the GDPR, or risk penalties themselves. Experts are predicting that processors may seek independent compliance certifications in order to reassure potential customers.

For example, a payroll management company is a data processor under the GDPR, since it processes personal data for a specific purpose. A market research agency that takes clients' aggregated data and determines how best to use that personal information is a controller. As an organization, it's possible for you to be a processor of some data and a controller of other data. You're categorized based on your actions with respect to personal data. If you're unsure about where you stand, consult your legal advisor.

Why the GDPR matters to you

There are numerous reasons why the GDPR matters to your organization. Here are a few to consider:

- **It likely applies to you**
  Even if your business is based in the US, the GDPR probably applies to you. Any organization doing business with (and using personal data from) EU citizens and residents is required to comply.
- **Penalties for non-compliance are steep**
  Organizations face fines that start at 20 million euros (roughly $25 million) or up to 4 percent of global revenue — whichever is greater.

  These penalties have the potential to be particularly harsh for massive multinational corporations. Amazon, for example, had 2017 revenue of $177 billion, which would potentially equate to a fine exceeding $7 billion. Other major tech companies could similarly be liable to pay sky-high amounts in GDPR fines. Going by the maximum 4 percent revenue penalty, Google would have to pay up to $4.4 billion, Facebook up to $1.6 billion, and Netflix "only" up to $467 million. Meanwhile, management consulting firm Oliver Wyman predicts that the FTSE 100 companies, which are the top 100 companies on the London Stock Exchange, could face annual fines as high as £5 billion ($6.9 billion) for failure to comply with the GDPR.
- **Penalties aren't only for inadequate data security measures**
  You can have top-of-the-line security and still face devastating fines if, for example, you experience a data breach and fail to report it within the 72-hour breach notification timeframe.
- **It represents a shift in mentality**
  The GDPR puts the power in the hands of the data subjects and the responsibility on organizations to protect and respect that information. Data privacy is now a fundamental right in the EU, and organizations that fail to acknowledge this will suffer.
- **It can give you a competitive advantage**
  EU customers have evolving expectations. Similarly, your partners, vendors, and competitors care that you comply with the GDPR and will be asking you directly if you're compliant. Getting your GDPR compliance in order will give you a head start over your competitors and may create a more favorable public perception of your company. Over 50 percent of US employees have never even heard of the GDPR. You're reading this guide, which means you're already more informed than the majority of your peers.

What action is required?

Great(er) Expectations

There are four main principles of the GDPR. Although it's a complex regulation, the main thrust can be summarized in a few core ideals:

- **Obtain and process personal data fairly:** The GDPR requires data to be "processed lawfully, fairly and in a transparent manner."
- **Store data for a specific purpose:** Organizations must have a justifiable reason for collecting and storing data.
- **Keep data secure and up-to-date:** Individuals must be able to trust that companies will store their data professionally and responsibly.
- **Delete data when it's no longer needed:** People, not companies, have ultimate ownership of their data. Companies may only keep data for as long as they can justify the need for it.

Obtaining data

Companies acquiring personal data are now expected to provide notice and obtain consent from the data subject. This means that when you collect data, you must explain three things:

1. The purpose behind the acquisition (why you want their data)
2. The data subject's rights to access their information
3. The expected data retention duration (i.e. how long you want to keep their data in your system)

Supervisory authorities now require that you receive affirmative consent (or legitimate interest) from a data subject in order to possess or process that individual's data. Organizations must also keep track of how and when consent is obtained, as regulators may ask for documentation. Lastly, data subjects need the ability to withdraw their consent at any time.

Storing data

The whole point of the GDPR is to minimize risk to the individual. Personal data must be stored in a secure environment to prevent data breaches and unauthorized access or use. Organizations that treat personal data irresponsibly will be targeted by supervisory authorities. The best practices for storing data and ensuring GDPR compliance are as follows:

- **Update and maintain data in a secure environment**
  A data subject can ask an organization to provide access to his/her personal data. The individual must be granted the ability to modify any inaccurate data, see what the company is doing with it, and delete any personal data.
- **Delete data once you're done with it**
  Limit your data retention. In addition to having to adhere to deletion requests or withdrawals of consent, organizations cannot keep personal data forever. You must delete

or anonymize the information if no appropriate business use case remains for storing or processing. Data subjects have a "right to be forgotten" clause (with "undue delay") in the GDPR.

If you receive a deletion request, do you have a process in place to find the data and erase it? Do you know which data you legally need to keep? Here's where you need clear communication and understanding between data controllers and data processors.

- **Maintain data portability**
  The right to data portability allows subjects to obtain and reuse their personal data for their own purposes across different services. If a data subject requests to have their collected data moved to a different controller, for example, you're required to move it in a timely manner. You'll need the technical capability and necessary business processes to do this. It's enough to convert the personal data into a "structured, commonly used and machine-readable format" (like a CSV file, for example).

72-hour breach notification requirement

One of the most demanding GDPR rules is the breach notification requirement. Data breaches must be declared within 72 hours after they have been discovered, and proper authorities (and affected data subjects) must be notified. Luckily, there is an easy workaround. If an organization secures its data in such a way that renders it unreadable and unusable, this breach announcement rule is waived. The safest way to ensure compliance here is to encrypt your sensitive data. The GDPR mentions encryption repeatedly throughout the 261-page document.

Article 34 reads: "The communication [and announcement of a data breach] shall not be required if any of the following conditions are met: the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that **render the personal data unintelligible to any person who is not authorised to access it, such as encryption**."

Article 32 reads: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures **to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and **encryption of personal data**"

Recital 83 states, "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and **implement measures to mitigate those risks, such as encryption**. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected."

Preparing for GDPR

Determine if you're affected

The GDPR applies to all organizations that control or possess EU citizens' and residents' personal data, regardless of location. You can't just close your Frankfurt office and be exempt. Does your company market products to EU citizens or monitor their behavior? If so, proceed to the next step.

Hire a data protection officer (DPO)

Included in the GDPR is the requirement that certain companies elect a data protection officer (DPO) by the time the regulations go into effect. Per the GDPR, the title of "Data Protection Officer" is its own unofficial description. A DPO acts as an assistant to the controller or processor to monitor internal compliance, ensuring that an organization complies with all data protection regulations. The DPO can be appointed in-house, or the position can be filled by a contractor. Apart from certain conflicts of interest (such as CEO, CFO, CMO, HR, or IT) DPOs are not prevented from holding another position.

Not every organization needs a data protection officer, however. The GDPR initially limited the DPO requirement to organizations that have over 250 employees, but the final regulation ultimately did away with size restrictions. Now it applies to small businesses and global powerhouses alike. The GDPR asserts that DPOs are required for companies that fit any of the following descriptions:

- The processing is carried out by **a public authority or body** (excluding courts)

  -or-

- The **core activities** of the controller or the processor consist of processing operations, which require **regular and systematic monitoring** of data subjects on a large scale *[for example: collecting, combining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, transmitting, disclosing, restricting, erasing, or destroying personal information — whether or not by automated means]*

  -or-

- The core activities of the controller or the processor consist of processing on a **large scale** of special categories of data or personal data relating to criminal convictions and offences.

We've put together a useful guide that explores the data protection officer guidelines in greater detail.

Assess your database

What personal data is stored in your contacts database? How do you collect personal data and how do you justify storing and processing it? What data do you have, where is it stored and accessed, and who has access to it? If you didn't have policies in place, now's the time to make sure you do. Get a handle on your data and policies by mapping out your processes, all of which must be done before the GDPR goes into effect.

Make an effort

The EU's ODPC (Office of the Data Protection Commissioner) is charged with enforcing the GDPR. Even if you aren't compliant by the May 25 deadline, companies that make honest efforts toward compliance will be treated differently than those that ignore the law, according to the ODPC. In an interview with Irish news outlet *The Independent*, Data Protection Commissioner Helen Dixon said, "There's not going to be any amnesty or first or second chances. On the other hand, the GDPR does set out criteria when we go to look at the quantum of fine we might impose. We are obliged to take into account the level of cooperation between [the ODPC] and the regulated entity, the number of data subjects, the level of effect on the data subjects and any previous contraventions."

Don't panic

GDPR will fundamentally change how organizations collect, manage, and store personal information. Organizations that use inbound marketing will have an easier time with the GDPR. This is because they've already established opt-in consent, making compliance easier. Now it's time to work on improving your processes for capturing and preserving users' consent.

Leverage proven data protection solutions (like encryption)

Security measures and safeguards are required under the GDPR. Encryption itself is not mandatory under the GDPR, but encryption is called out in Article 32 as an "appropriate technical and organizational measure" of security.

In the event of a data breach, encryption renders personal data unreadable and unusable. Here's where encryption makes your job easy. Under the GDPR, organizations face hefty fines if they fail to announce a data breach within 72 hours. If, however, you encrypt your data, you aren't required to notify data subjects, since they are not at personal risk.

Achieving GDPR data security compliance

Companies that are preparing for the GDPR typically struggle with the same four problems:

1. Being under-informed about the subject
2. Identifying resources (people, budgets, etc.)
3. Conducting a readiness assessment
4. Launching a data inventory project

Since you've found your way to this guide, you're well on your way to possessing the necessary knowledge to engage with the GDPR. As you work toward GDPR compliance, consider us for your data encryption needs. To address data security requirements, you will need to employ encryption methods on your servers, in storage areas, with media, and throughout your networks. In addition, strong key management is necessary to protect your data, but also to comply with the data subject's "right to be forgotten."

Additional resources

- Data Protection Officer (DPO) Guide
- See encryption in action — Request a demo
- Full GDPR text

Zettaset XCrypt data encryption solutions are designed for today's complex, demanding distributed computing architectures. Enterprise customers rely on Zettaset to deliver advanced data encryption solutions that deliver performance and scalability while easily fitting within existing enterprise IT frameworks.

465 Fairchild Drive, Suite 234, Mountain View, CA 94043
www.zettaset.com // +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.