imperva

GUIDE

The Road to Compliance: Steps for Securing Data to Comply with the GDPR

Executive summary

The European Union (EU) General Data Protection Regulation (GDPR) has replaced the Data Protection Directive 95/46/EC (Directive).

The regulation expands privacy protections and includes obligations for companies that handle personal data originating in the EU. Unlike the Directive, it extends the reach of the data protection law to companies who may have no presence in the EU **as long as** those companies process an EU resident's personal data in connection with goods or services being offered or if those companies monitor the behavior of individuals within the EU.

Even for organizations that already follow cybersecurity best practices, GDPR data security requirements could result in process and technology changes that will require substantial time and resources to implement. The potential upside for security teams is twofold: they may benefit from the increased investigative capacity and streamlined breach response plan that comes with process and technology measures **as a result of** compliance.

This guide is for CISOs who want to understand whether their companies are impacted by the new regulation, how it impacts them, and what steps their teams can take to comply with GDPR data security requirements. You'll learn:

- The basic framework, intent, and extent of the GDPR
- Which companies are affected
- What the penalties are for non-compliance
- A pragmatic approach to approaching a GDPR compliance project
- How Imperva can help

Making GDPR data security compliance a top priority

Any company that processes personal data originating in the EU (whether or not the data subject is a citizen or resident of the EU) or the data of an EU resident—whether the company has operations in the EU or not—is covered by the GDPR. Because this could affect nearly every website or app in the world, it's no wonder that GDPR compliance is a top priority for CISOs around the world.

For companies located in the EU, doing or seeking to do business with individuals in the EU, or monitoring the behavior of or collecting information from individuals in the EU, the GDPR has introduced a new level of compliance obligations around privacy and data security.

Wherever your company is on the road to GDPR compliance, this guide can help you take the right steps to get there.

GDPR ONE YEAR IN

Only 28% of firms say they are compliant with the GDPR today, with 30% "close to compliant."

SOURCE: CAP GEMINI SURVEY - SEPT 2019

About the GDPR

The Official Name

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Properties

Length of the full text 88 pages
Status Effective since May 25, 2018
Purpose Gives individuals in the EU stronger rights, empowering them with better control of their data and protecting their privacy in the digital age.

Organizations Impacted

Both data controllers (those that determine the purposes and means of processing personal data) and data processors (those that process personal data on behalf of the controller) of personal data originating in the EU or of EU residents, regardless of the location of the business.

What Is Personal Data?

Any information relating to an identified or identifiable natural person that originates in the EU. More specifically, the GDPR states: "'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, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Certification

For those that successfully meet the requirements, there is an optional certification, which may provide a competitive advantage and help build customer trust.

Does GDPR apply to your organization?

Many global organizations operating outside of the EU may still require guidance as to how the regulation applies to them. While CISOs should always consult with their legal departments about applicability, the following explanation and examples provide a starting point for understanding the reach of the regulation.

GDPR requirements apply to any organization doing business in the EU regardless of whether the processing of personal data takes place in the EU or not, and whether it's data about EU residents or EU visitors.

It is important to note that the new rules will apply to businesses established outside the EU if they process the personal data of EU residents or visitors in connection with:

- Offers of goods or services, irrespective of whether payment is required; or,
- Monitoring of behavior that takes place within the EU

While simply having a website or email accessible in the EU is not enough to bring a global business under the GDPR scope, certain factors may indicate that a business intends to offer goods or services to EU residents or visitors within the EU, which then bring the business within the scope of the new rules. These factors may include:

- The use of a language or a currency generally used in one or more EU Member States with the possibility of ordering goods and services in that language
- The mentioning of customers or users who are in the EU[1]

[1] Paragraph 23 of the Introductory Recitals to the GDPR.

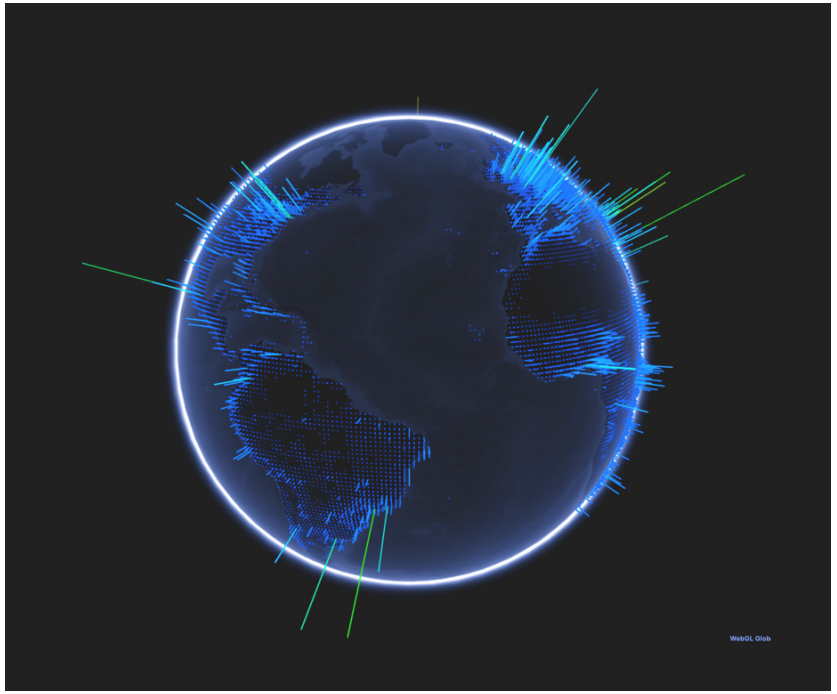
Does GDPR apply? Two examples

Example 1

A financial analyst firm is tasked with projecting a European company's revenues for the next three years. The primary analyst works out of an office in the US, but uses personal data provided by the client. Because the data was collected in the EU, it is subject to GDPR requirements, even though the analyst is based out of the US office and didn't originally collect the data.

Example 2

A mobile and online website allows people to shop for, buy, and rate products. The US-based company that owns the retail storefront collects personal data about the people that visit and make purchases. The information is subsequently used in advertising campaigns and sales reports. If a person visits the website while they are physically present in the EU, the requirements of the GDPR follow the personal data collected during that visit. That means that any website or mobile application that is accessible by and collects personal data from a person in the EU will need to comply with the GDPR.



[1] Paragraph 23 of the Introductory Recitals to the GDPR.

The price of non-compliance

If the benefits of complying with GDPR aren't incentive enough, the potential penalties for companies that do not comply should help you create a convincing business case for the investment needed. While fines are discretionary rather than mandatory, to be imposed on a case-by-case basis, in ways designed to be effective, proportionate and dissuasive, the two tiers of maximum administrative fines set out in the regulation are steep. Depending on the violation, fines may fall into one of two categories:[2]

The greater of €10 million/~$11 million or 2% of global annual turnover of the preceding financial year

For non-compliance related to consents, data protection, controller and processor obligations, written records, privacy impact assessments, breach communications, and certifications, among others. See Article 83(4).

The greater of €20 million/~$22 million or 4% global annual turnover

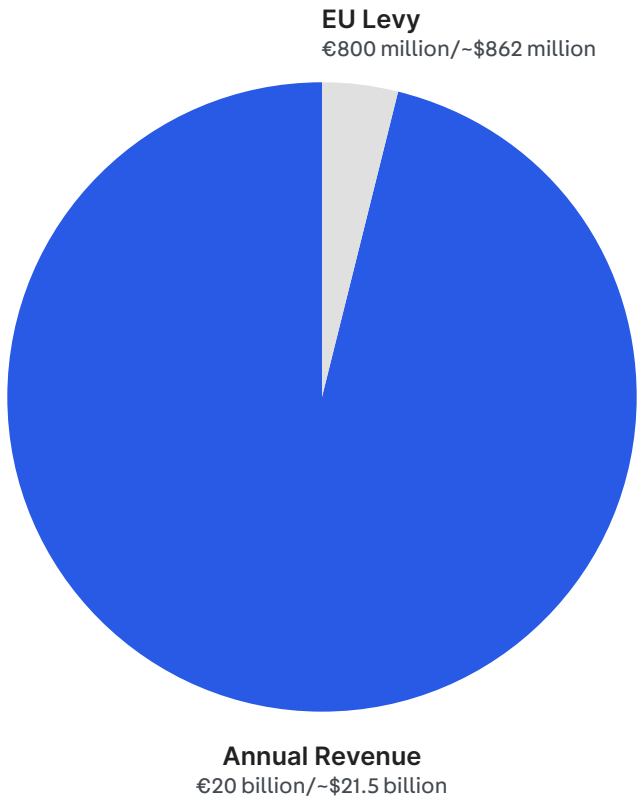
For failure to adhere to the core principles of data processing, infringement of personal rights, or the transfer of personal data to other countries or international organizations that do not ensure an adequate level of data protection, among others. See Article 83(5).

[2] Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council.

What large organizations could face

Consider this example. Acme, Inc. generates €20 billion/~$21.5 billion in revenue in 2017 and is found to have transferred personal data to the United States (a country that the European Commission has determined does not have an adequate level of protection for personal data) without implementing appropriate safeguards to protect the data and without ensuring that the data subjects have enforceable data privacy rights and effective legal remedies.

EU regulators (i.e., the relevant data protection authority) have the power to levy a fine of €800 million/$862 million (4% of €20 billion), which is far more than the €20 million minimum. With typical operating margins in single digits, a fine of this magnitude could easily consume most of the profit for a large company for an entire year.



A checklist for approaching GDPR

To help your organization get started with your GDPR compliance project, the data security experts at Imperva recommend following this checklist:

GDPR CHECKLIST	EXPLANATION
☐ **Data privacy impact assessment (DPIA)**	A DPIA helps identify and minimize privacy risks. Working with stakeholders within the business and partner organizations, you document how personal data processing complies with the GDPR. A DPIA is required by the GDPR in high-risk situations.
☐ **Personal data inventory**	Assess what personal data you have and where it is stored. By conducting a personal data inventory, you gain a clear understanding of the personal data used in your organization.
☐ **Data flow analysis**	Identify all systems which touch data that is within the scope of the GDPR. Map the flows of data from point of entry all the way through to destruction, including third-party processes. Data mapping helps you ensure that all risks are uncovered appropriately as you gain a solid understanding of your organization's complete data life cycle. See Figure 1.

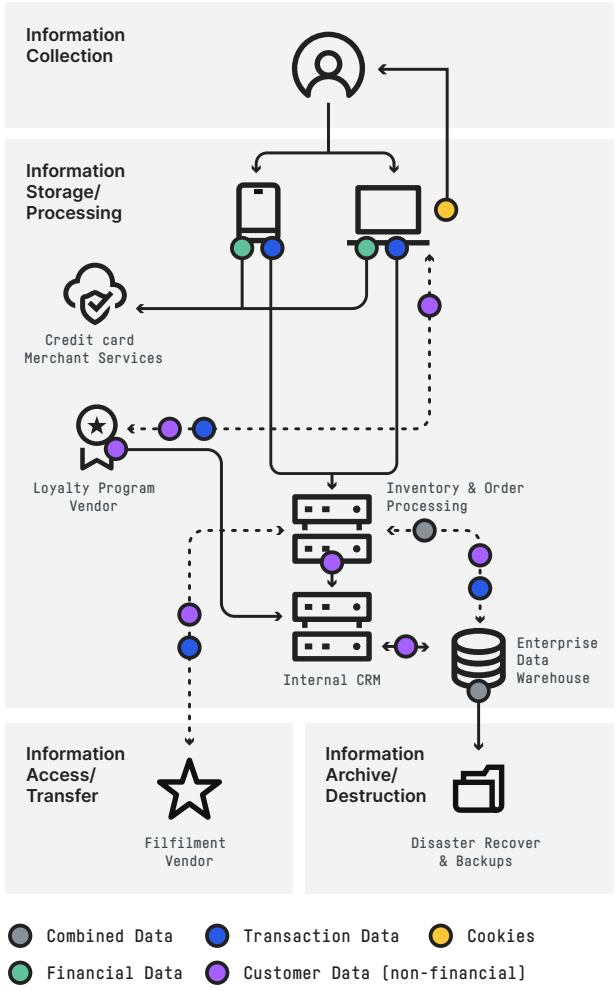


Figure 1: Data Flow Analysis

☐ **Risk assessment(s)**	Follow the touch points for the data (including databases, file systems, and people) and perform a risk assessment against each of them. You'll be evaluating current data protection policies and processes as well as the technology controls that enforce those policies and procedures. For example, do you have controls in place to enforce cross-border data transfer requirements of the GDPR? Identify areas of higher risk and what needs to happen to mitigate that risk.
☐ **Data breach procedures review**	Evaluate your procedures and controls to detect, report and investigate a data breach. The GDPR imposes breach notification requirements for data controllers and processors. For example, data controllers must report data breaches to supervisory authorities within 72 hours of becoming aware of a breach unless the breach is unlikely to result in a risk to the rights and freedoms of a natural person.
☐ **Identification of gaps and remediation plans**	Identify how you'll remediate any compliance gaps detected in your risk assessments. Prioritize which gaps are higher risk and should be addressed first. Remediation plans can include: training or hiring staff, process or policy changes, legal contracts, and implementing new technology controls.

HELP WANTED: 28,000 DPOS NEEDED

The GDPR requires public authorities processing personal information to appoint a data protection officer (DPO) when core activities require "regular and systematic monitoring of data subjects on a large scale" or consist of "processing special categories of data" on a large scale or if required to do so by local law.

As written in the GDPR, the DPO's tasks include: informing and advising on compliance obligations, monitoring compliance, advising with regard to data protection impact assessments, working and cooperating with the designated supervisory authority, and being available for inquiries from data subjects.

According to a study by the International Association of Privacy Professionals (IAPP), in Europe alone, 28,000 DPOs were expected to have been appointed by May 25, 2018.

Source: Rita Heimes and Sam Pfeifle, "Study: At least 28,000 DPOs needed to meet GDPR requirements," International Association of Privacy Professionals, April 19, 2016.

☐ **Sign off on outcomes (benefits)**	Present the results of your analysis along with the recommended solutions to get support and budget for the project. You should get executive sign off on the expected outcomes of the project.
☐ **Implement improvements/ remediation plan**	Execute the project using a proven implementation methodology that includes definition, design, and implementation phases.
☐ **Governance (ongoing accountability and DPIAs)**	Put processes in place to conduct ongoing DPIAs and ensure continuous compliance through testing.

Imperva can help

More than 5,000 customers worldwide, including financial services firms, healthcare companies, and government agencies rely on Imperva to protect their critical data and applications. When it comes to complying with GDPR, Imperva offers expert services and award-winning technology that combine to create best-of-breed solutions. These solutions can assist your company in implementing risk-reduction measures and improving your organization's compliance with data security requirements under the GDPR.

Imperva Data Security

Imperva Data Security protects sensitive data from potential data breaches and can help you implement adequate data safeguards, which are a core component of GDPR compliance. Imperva Data Security includes:

Data Discovery and Classification:

Imperva Data Security provides a proven methodology to discover and classify data, which is a critical aspect of GDPR compliance. It provides visibility into what personal data your organization holds and processes. Key deliverables include: identification of database assets, data owners and data custodians; risk classification of data; and control recommendations.

Data Masking or Pseudonymization:

The GDPR requires organizations practice data minimization, which means they collect and use data limited to only what is necessary for a specific purpose. Imperva Data Security includes Data masking capability that replaces real data with realistic fictional data that is functionally and statistically accurate. It facilitates processing of personal data beyond original collection purposes and also limits the spread of personal data beyond "need-to-know".

Data Activity Monitoring:

The GDPR requires organizations maintain a secure environment for data processing, making data activity monitoring critical. To comply with GDPR, you need to be able to answer WHO is accessing WHAT data, WHEN, and HOW that data is being used. Imperva Data Security provides complete visibility into data activity. It continuously monitors and analyzes all database activity, including local privileged user access and service accounts, in real time.

Breach Detection and Incident Response:

In the event of a personal data breach, the GDPR dictates that data controllers must notify the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." Imperva utilizes machine learning and data risk analytics to pinpoint and prioritize high-risk incidents, filtering out the noise and allowing security team to accelerate threat investigation and response.

Professional Services

In addition to Imperva Data Security, Imperva provides professional services to help organizations accelerate GDPR:

Imperva Data Discovery and Analysis Service:

Imperva Data Discovery and Analysis Service: Imperva Database Discovery and Analysis (dDnA) service provides a proven methodology to discover and classify data, which is a critical aspect of GDPR compliance. Key deliverables include: identification of database assets, data owners and data custodians; risk classification of data; and control recommendations.

Imperva Project Discovery and Analysis Service:

Imperva Project Discovery and Analysis (pDnA) service evaluates current database security controls to identify control gaps. Key deliverables include: identification of key stakeholders, risk assessment, and recommendations of solutions and plans to address identified gaps.

Table: Mapping key GDPR requirements to Imperva Data Security

ARTICLE	WHAT IT MEANS	REQUIREMENTS FOR DATA SECURITY
25: Data protection by design and by default	Implement technical and organizational measures to show consideration and implementation of Data Protection Principles and appropriate safeguards	• Data minimization • User access limits • Limit period of storage and accessibility
32: Security of processing	Implement appropriate technical and organizational security controls to protect personal data against accidental or unlawful loss, destruction, alteration, access or disclosure	• Pseudonymization and encryption • Ongoing protection • Regular testing and verification
33 and 34: Data breach notification	72 hour notification to Data Protection Authority following discovery of data breach, and notification to affected individuals	Breach report that includes: • what happened • numbers of affected individual • what data was breached
35: Data protection impact assessment	Assessment of the purpose, scope and risk associated with processing personal data	Inventory of personal data across organization, access rights to data, and risk associated with that access
44: Data transfers to third country or international organization	Permit transfers only to entities in compliance with GDPR regulation	Monitor and block access to entities or regions that do not meet requirements

Learn more

Find out more about how to comply with the data protection regulations within GDPR:

- Read the full text of the General Data Protection Regulation (GDPR)
- Check out the white paper GDPR: New Data Protection Rules in the EU
- Learn more about Five Ways Imperva Helps You with GDPR Compliance

About Imperva

Recognized by industry analysts as a cybersecurity leader, Imperva champions the fight to secure data and applications wherever they reside. In today's fast moving cybersecurity landscape, your assets require continuous protection, but analyzing every emerging threat taxes your time and resources. For security to work, it has to work for you. By accurately detecting and effectively blocking incoming threats, we empower you to manage critical risks, so you never have to choose between innovating for your customers and protecting what matters most.

At Imperva, we tirelessly defend your business as it grows, giving you clarity for today and confidence for tomorrow. **Imperva - protect the pulse of your business.**

Learn more: imperva.com, LinkedIn and Twitter

imperva.com
+1.866.926.4678