



General Data Protection Regulation (GDPR) Fast Facts

Perfecting the Art of *Active* **Cyber Defense**

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

Executive Summary

The EU General Data Protection Regulation (GDPR) was approved by the EU Parliament on April 14, 2016 after four years of preparation and debate. The GDPR is designed to strengthen and unify data protection for individuals within the EU and also addresses the export of personal data outside the EU. All EU Member States must comply with the regulations by May 25, 2018, after a two-year transition period.

The GDPR applies to all companies worldwide that process personal data of EU citizens and replaces the Data Protection Directive 95 / 46 / EC. It was designed to provide for the harmonization of data privacy laws and regulations across the EU.

What is the General Data Protection Regulation (GDPR)?

The GDPR is intended to strengthen and unify the protection of data for individuals within the EU and also addresses the export of personal data outside the EU. One of the primary objectives of the GDPR is to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect in 2018, it will replace the Data Protection Directive of 1995. The GDPR was adopted on April 27, 2016 after four years of debate. It takes full effect on May 25, 2018 after a two-year transition period.

Who Does It Impact?

The GDPR applies to data controllers and processors at organizations if data subject (individual) is resides within the EU. With similar definitions as under the Data Protection Act of 1998 (DPA), the controller says how and why personal data is processed, and the processor acts on the controller's behalf. If an individual currently is subject to the DPA, that individual likely will also be subject to the GDPR.

The GDPR places specific legal obligations on processors, requiring they maintain records of personal data and processing activities. Processors will have significantly more legal liability if responsible for a breach. These processor obligations are new under the GDPR. Controllers have the additional obligation to ensure contracts with processors comply with the GDPR.

Processes carried out by organizations operating within the EU are subject to the GDPR, as well as organizations outside the EU offering goods or services to individuals in the EU if they process personal data of EU residents. According to the European Commission "personal data" is any information relating to an individual, whether it relates to his or her private, professional or public life.

Certain activities, including processing covered by the Law Enforcement Directive, processing for national security purposes, and processing carried out by individuals purely for personal/household activities are not covered by the GDPR.

Definitions

Biometric Data

Any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows their unique identification.

Data Portability

The requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Controller

The entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor

The entity that processes data on behalf of the Data Controller.

Data Erasure

Also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Data Protection Authority

National authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Field

A section of a record, especially in a database, in which an item of data is entered.

Data Subject

A natural person whose personal data is processed by a controller or processor.

Data Masking

A method of creating a structurally similar but inauthentic version of an organization's data that can be used for software testing and user training. The main reason for applying masking to a data field is to protect data that is classified as personal identifiable data, personal sensitive data or commercially sensitive data.

EDPB

The European Data Protection Board (EDPB); it will replace the Article 29 Working Party and its functions will include ensuring consistency in the application of the GDPR, advising the EU Commission, issuing guidelines, codes of practice and recommendations, accrediting certification bodies and issuing opinions on draft decisions of supervisory authorities.

Definitions

EEA

The European Economic Area (EEA) includes all 28 EU member states, plus Iceland, Lichtenstein and Norway. It does not include Switzerland.

Personal Data

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person.

Encryption

The process of disguising a message or data in such a way as to hide its substance.

Processing

Any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

GDPR

General Data Protection Regulation (GDPR). New data privacy and protection regulations which will replace individual data protection laws in all EU countries on 25th May 2018.

Right to Access

Also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Recipient

Entity to which the personal data are disclosed.

Regulation

A binding legislative act that must be applied in its entirety across the Union.

Right to Erasure / Right to be Forgotten

The data subject's existing right to deletion of their personal data, in certain circumstances, has been extended to a new 'right of erasure' in circumstances detailed in Chapter III Section 3 GDPR.

What Information Applies?

Personal data

The GDPR applies to both automated personal data and manual filing systems where personal data are accessible according to specific criteria.

Any data that can be used to identify an individual is considered personal data according to the GDPR. It includes, for the first time, things such as genetic, mental, cultural, economic or social information.

Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data.” For example, the special categories specifically include genetic and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Key GDPR Requirements

Data Breaches

- Data Controller under legal obligation to notify Supervisory Authority within 72 hours of the discovery of a breach.
- Reporting of a data breach is not subject to any de-minimize standard.
- Affected individuals must be notified if an adverse impact is determined.

Sanctions

- Severe penalties may apply for non-compliance with the requirements of the GDPR. The following sanctions may be imposed:
 - A written warning in cases of first and non-intentional non-compliance.
 - Regular periodic data protection audits.
 - A fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.
 - A fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

Data Protection Officer (DPO)

The GDPR requires the appointment of a DPO if you:

- Are a public authority (except for courts acting in their judicial capacity).
- Carry out large scale systematic monitoring of individuals (for example, online behavior tracking).
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offenses.

- Organizations may appoint a single DPO to act for a group of companies or a group of public authorities, taking into account their structure and size.
- Regardless of whether the GDPR requires your organization to appoint a DPO, you need to ensure your organization has sufficient staff and skills to execute your obligations under the GDPR.

Other Key GDPR Facts

The GDPR brings additional requirements and changes to the way companies are required to protect data and ensure compliance with the regulation. The GDPR:

1. Tightens the rules for obtaining consent to use personal information, requiring organizations to ensure they use easy-to-understand language when asking for consent and clearly explain how the information will be used.
2. Requires organizations collecting personal data to prove they have consent from the individual to process the data.
3. Requires the appointment of a DPO by public authorities and other organizations who processing personal information.
4. Introduces mandatory Privacy Impact Assessments (PIAs) requiring data controllers conduct PIAs where privacy breach risks are high prior to beginning any project involving personal information.
5. Harmonizes various data breach notification laws in Europe. The regulation requires notification of a data breach to the local data protection authority within 72 hours of discovery.
6. Introduces very restrictive, enforceable data handling principles, including one requiring organizations not hold data any longer than necessary, and to not change the use of the data for purposes other than for which it was originally collected.
7. Expands liability beyond data controllers. In the past, only controllers were considered responsible for data processing activities. The GDPR extends that liability to all organizations handling personal data in any way.
8. Requires privacy by design, meaning privacy must be included in systems and processes to comply with the principles of data protection.
9. Introduces the concept of one-stop shop which allows any European data protection authority to take action against an organization regardless of where in the world the company is based. This offers the benefit of having to deal with only one supervisory authority rather than a different one for each EU Member State.

Preparing for GDPR Enforcement

Companies doing business with a Member State of the EU can start preparing for GDPR enforcement now.

- Establish and document a framework of accountability in your organization.
- Develop, publish and implement required policies and procedures, and regularly review and update them.
- Train your workforce members and ensure they understand their obligations related to privacy and security.
- Conduct a risk assessment and mitigate known vulnerabilities.

GDPR Timeline

#	Description	Date
1	Full compliance date	May 25, 2018
2	Regulation in force 20 days after publication in EU Official Journal	May 4, 2016
3	Adoption by European Parliament	April 14, 2016
4	Adoption by Council of the EU	April 8, 2016
5	European Parliament's LIBE committee vote positively on outcome of negotiations between the three parties	December 17, 2015
6	Negotiations between European Parliament, Council and Commission (Trilogue) result in a joint proposal	December 15, 2015
7	European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) orientation vote	October 21, 2013

Right to Erasure

- Right to Erasure could be the biggest burden of GDPR.
- GDPR regulations to be enforced starting in 2018, allows Europeans to request organizations delete their personal data for a variety of reasons.
- A controversial set of EU rules that allow individuals to have their names removed from search engine results.
- Multi-national organizations with hundreds of databases across their enterprise, including everything from e-commerce functions and third-party providers to audits and other operations, are scrambling to find a way to search this data to find and delete the records belonging to individual consumers.

- Organizations are examining ways to meet this compliance manually, where individual employees need to find and delete data throughout their entire company, or updating their technology to unite data in a single access point.
- Organizations say:
 - The cost of the erasure compliance obligation is far more expensive than any other requirement under GDPR.
 - This has been the poke they need to integrate their systems and actually see where their data is located.

Understanding the Requirements

- Companies must delete user's personal data when that information is no longer used for the reason it was collected, when individuals withdraw their consent.
- Individuals do not have a total right to erasure, however. Organizations can refuse erasure requests when complying would interfere with the right to expression and information, when the data is relevant to the public interest, or when the information is relevant to legal claims and other purposes.
- A dispute between an individual and the data collector will be officiated by the data protection authority in the region. Further appeals could go to the national courts, a presumably time-consuming process that would assess the interests involved.
- Companies need to consider the nature of the information and request balanced against other interests that the regulation contemplates, including the public's right to know.

Business Benefits

- Social media, web search, and e-commerce companies might be most dramatically affected by the right to erasure.
- Allows individuals to petition data collectors to correct information about themselves.
- Individuals often make data about themselves available manually, either by filling out forms, answering questions, checking boxes, or other benign methods.
 - When they inadvertently add incorrect information, or that information is mistakenly changed later, records and algorithms become less accurate.
 - Duplication of data (multiple files of the same photos, for instance) affects data's utility and costs storage space.
- Going to be a bigger problem for old, more so than new, data sets.
- Small businesses particularly well-suited for erasure. With less information coming into their systems and fewer old databases, administrators at smaller organizations might have less work to do.

Accidental Data Loss

- GDPR broadly defines a data breach as a security incident that leads to “destruction, loss, alteration, unauthorized disclosure of, or access to” personal data that is collected, sent or processed by a firm.”
- 57% of data breaches experienced by companies are a result of hacking or malware, according to data from the Privacy Rights Clearinghouse.
- About 22% of data breaches stem from unintended disclosure, which includes incidents such as cloud storage loss and emails sent to unintended recipients.
- 10% of breaches are due to lost smartphones, and 7% are due to lost corporate laptops and drives.
- Data-loss incidents, typically a result of an employee making a mistake, often are overlooked by executives and information-technology specialists.
- Fortunately, there are technologies and policies companies can put into place to help prevent data loss from each of these types of incidents; much in the same way firewalls and antivirus software are used to safeguard against malware.
- Fines under the GDPR can be reduced if a company shows it has taken steps to mitigate the damage caused by a breach.








Lost Devices

- A lost smartphone or laptop may sound like a few hundred dollars of headache, but data on these devices can be worth a lot more than the hardware itself.
- Computers and smartphones have built-in encryption, but most people don’t turn that on. Nearly two-thirds of companies may not turn on encryption for their devices.
- As an added measure, some invest in enterprise mobility management tools that allow IT staff to track and remove corporate data or completely wipe a device if it is lost.

Unintended Disclosure

- Several organizations have been hit hard by relatively simple scams that involve unintended email disclosure.
- The Internal Revenue Service has warned firms in recent years of schemes where employees are tricked into sending staff tax documents to cybercriminals, who then use the forms to file fraudulent tax returns.
- Scams often can be avoided by using basic scanning software that spots suspicious emails, along with training staff on how to identify phishing emails, but these solutions don’t fix the everyday issue of employees typing in the wrong recipient address.

GDPR: Fast Facts

Fact	Description
 The official name	Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (GDPR).
 Length of the full text	88 pages.
 Status	Effective May 25, 2018.
 Objective	Simplify the regulatory environment for international business by unifying the regulation within the EU.
 Purpose	<ul style="list-style-type: none"> ✦ Gives individuals in the EU stronger rights, empowering them with better control of their data and protecting their privacy in the digital age. ✦ Comprehensive reform of the European Union's 1995 data protection rules to strengthen and unify the protection of data for individuals within the European Union (EU). ✦ Addresses export of personal data outside the EU.
 Who it Impacts	<ul style="list-style-type: none"> ✦ Data controllers and processors at organizations, if the data subject resides within the EU. ✦ Individuals currently subject to the Data Protection Act (DPA) are likely subject to the GDPR.
 Information Covered	<p>Personal data – Any data that can be used to identify an individual, including things such as genetic, mental, cultural, economic, and social information.</p> <p>Sensitive personal data – Special categories of personal data including, genetic and biometric data, where processed, to uniquely identify an individual.</p>

Key Requirements



Data breaches

- ❖ Data Controller under legal obligation to notify Supervisory Authority within 72 hours of discovery of a breach.
- ❖ Reporting of breach not subject to any de-minimize standard.
- ❖ Affected individuals must be notified if adverse impact is determined.



Sanctions

- ❖ Severe financial penalties may apply for non-compliance with requirements of the GDPR.
- ❖ Written warning in cases of first and non-intentional non-compliance.
- ❖ Regular periodic data protection audits.

- ❖ Appointment of Data Protection Officer (DPO).
- ❖ Tightens rules for obtaining consent to use personal information.
- ❖ Requires organizations collecting personal data to prove they have consent from the individual to process the data.
- ❖ Mandatory Privacy Impact Assessments (PIAs), requiring Data Controllers conduct PIAs where privacy breach risks are high, prior to beginning any project involving personal information.
- ❖ Expands liability beyond data controllers to all organizations handling personal data in any way.

Administrative Fines

- ❖ 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.
- ❖ 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.

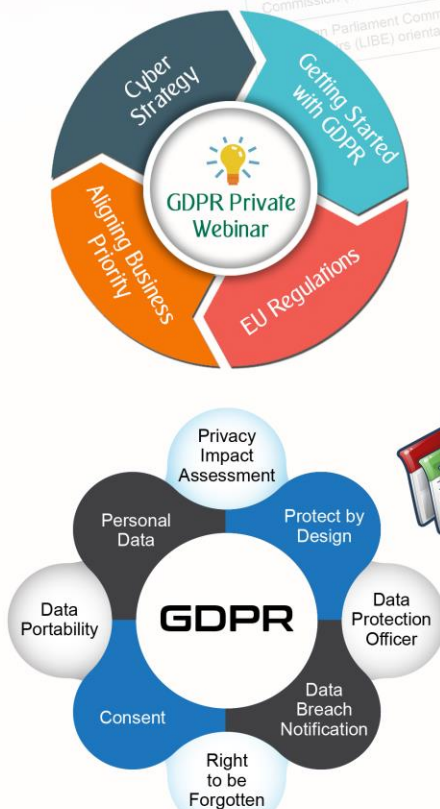
GDPR Services



The General Data Protection Regulation (GDPR) unifies the regulations within the European Union (EU). Discuss GDPR with ecfirst. ecfirst offers a complete range of GDPR compliance solutions, including:

- 🔗 Addressing GDPR mandates
- 🔗 Comprehensive risk assessment to identify GDPR compliance gaps
- 🔗 Cybersecurity vulnerability assessment to determine security vulnerabilities
- 🔗 GDPR cybersecurity strategy workshop (1-day program, delivered at your site)
- 🔗 Policy review and update to address GDPR requirements
- 🔗 Development of tailored GDPR security procedures
- 🔗 On-Demand Consulting (ODC) Advisory Services to establish a credible GDPR compliance program
- 🔗 Managed Cybersecurity Services Program (MCSP) to monitor and maintain a GDPR compliance program

GDPR Private Webinar: Complimentary!



GDPR Policy & Procedure

Update your policies to align with GDPR. Talk to ecfirst about creating customized procedures.

Act Now for GDPR Compliance!

Schedule a complimentary, private GDPR Webinar now!



Robert Acosta

Bob.Acosta@ecfirst.com

+1.949.793.5700

Perfecting the Art of Active Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents



Perfecting the Art of Active Cyber Defense



Client Reference

"I just wanted to take a moment and say thank you. Thank you and the **excellent team** at ecfirst for **hard work**, late hours and **diligence** during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an **exceptional partner** that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I continue to recommend ecfirst highly and often!"



Chip Goodman | Vice President of Information Technology

"The ecfirst team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an **integral part** of our business strategy and have been **extremely satisfied** with the **quality and value** of the services that ecfirst has rendered."



DerShung Yang | Founder & President

"Provant Health partnered with ecfirst to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were **flexible, collaborative** and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I'd recommend ecfirst to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification."



Tom Basillere | Chief Information Officer



Robert Acosta

Bob.Acosta@ecfirst.com

+1.949.793.5700

Perfecting the Art of Active Cyber Defense

1000s of Clients | Clients in all 50 States | Clients on 5 Continents



Corporate Office

295 NE Venture Drive

Waukee, IA 50263

United States

Kris Laidley

Inside Sales Support Coordinator

ecfirst/HIPAA Academy

Phone: +1.515.987.4044 ext 25

Email: Kristen.Laidley@ecfirst.com

Robert Acosta

National Sales Director

ecfirst/HIPAA Academy

Phone: +1.949.793.5700

Email: Bob.Acosta@ecfirst.com

www.ecfirst.com

© 2019 All Rights Reserved | ecfirst

