

# GDPR: The basics

FUJITSU



shaping tomorrow with you

# What is GDPR?

The EU General Data Protection Regulation (GDPR) is the biggest European shake-up of data protection in a generation. It's the culmination of two decades of experience of a rapidly growing data economy. It replaces the Data Protection Directive 95/46 EC and is designed to harmonize data privacy laws across Europe.<sup>1</sup> It is a bold step to protect human rights in the digital age. As The Guardian put it; "Data is knowledge and knowledge is power. That is why data protection matters in a democracy."<sup>2</sup>

## What is GDPR for?

The GDPR protects the rights of individuals in the EU by controlling who can collect and process their personal data.

## Where did GDPR originate?

The Charter of Fundamental Rights of the European Union is very clear about what every EU citizen should expect: for example, the right to work, marry, receive an education, and be free from discrimination, slavery, and coercion. Fundamental to those rights is the right to a private life.

The protection of our rights as individuals is at the heart of the concept of modern democracy. The rise of digital technology has blurred the lines of what is private and what is public. It has created new streams of data that are often automatically produced and collected in entirely new ways. Our Internet usage, our smartphones and other mobile devices, our smart homes, our cars and a rapidly expanding ecosystem of sensors embedded in everyday objects, all generate data about what we think, say, want, and do.


Article 7 of the Charter says, "Everyone has the right to respect for his or her private and family life, home and communications." Article 8 focuses on data; "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."<sup>3</sup>

<sup>1</sup> <https://www.eugdpr.org/>

<sup>2</sup> Editorial: The Guardian: August 7th, 2017

<sup>3</sup> EU Charter of Fundamental Rights, 2000





# What kind of data does GDPR cover?

The personal data of each data subject, that is individuals residing within the European Union.

## What is personal data?

It relates to a person – a data subject. It includes names, addresses, emails, or date of birth. But, data is also “personal” when it connects different pieces of information to make a data subject identifiable and unique: ID-card-numbers, phone numbers, credit card numbers, IP-addresses or the GPS data of a smartphone can identify (in combination with other data) a data subject. This also means that one individual piece of information may not be seen as personal data but in combination with other information this may be defined as personal data.

## Why is personal data so important?

Because its real power is revealed when it is aggregated and then refined to yield insights. But who owns it? Who has the right to access and control it? How can we be sure that we won't be disadvantaged by the data that any organization holds about us? What happens when it is wrong? Do we have the right to be anonymous, or left alone?

GDPR delivers a very human-centric answer to all those important questions. It is more than just another law: it is a step forward in the enforcement and the protection of human rights as its aim is to give citizens back control of their personal data.

# Who does GDPR apply to?

The GDPR applies to the processing of personal data by a data controller or data processor.

## What's a data controller?

The data controller can be thought of as a natural person or legal organization being for example private, public or other bodies which collects and processes the personal data of data subjects.

## What's a data processor?

A data processor is a natural person or legal organization which is responsible for processing personal data on behalf of the data controller.

## Who does what?

The data controller determines the purposes, conditions and means of the processing of personal data, including setting in place appropriate technical and organizational controls. The processor acts on the written instructions of the controller to process the personal data as agreed between these two parties.

The controller of the personal data is liable for what the processor does with it. When a controller makes an agreement with a processor, they must ensure that the processor (and any sub-processors they may engage) complies with their written instruction in line with GDPR. If there's an infringement of the GDPR, then each may be liable for their actions.



# Is this just about data within the EU?

No, it applies to all public and private sector organizations processing the personal data of data subjects residing in the European Union, regardless of the company's location.

GDPR makes its applicability very clear - it will apply to the processing of personal data of data subjects who live in the European Union by controllers and processors, regardless of whether they are established in the Union or whether the processing takes place in the EU or not. When that personal data moves across borders outside the EU it could be at risk of 'unlawful use or disclosure', so GDPR protects it wherever it is used.

GDPR applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior.

## Does it matter how the data is collected?

Personal data that's automatically as well as manually collected is covered by GDPR. So, it doesn't matter if the data your organization holds is in a physical file or on a database – it is covered by GDPR. And even if a data record is anonymized (or pseudonymized), but there is a possibility that it can be linked to a specific individual, then that too is covered.

There are special categories that cover children's personal data, genetic and biometric data, as well as racial or ethnic origin, political opinion, religious or philosophical beliefs amongst others. GDPR does not cover personal data relating to criminal convictions, but it does protect how that data can be processed. So personal data covers quite a number of attributes.

## What is the principle of lawful processing?

GDPR is, ultimately, all about accountability. It requires that personal data is 'processed lawfully, fairly and in a transparent manner in relation to individuals, and is collected for specific, explicit and legitimate purposes' and not 'further processed in a manner that is incompatible with those purposes.' Simply, your organization needs to be accountable for how it collects and processes data.

To be accountable you must keep records of what data you have collected and what processing has been applied to it. You must ensure that it is accurate, up-to-date, and rectified or erased 'without undue delay'. You must also ensure that you do not keep data for longer than necessary unless there are public interest or other reasons for it to be retained.

## How does GDPR change the rules on consent?

GDPR strengthens the conditions for consent. It will no longer be possible for companies to create long terms and conditions full of legal language that's hard for the ordinary person to read, let alone understand. When data controller is reliant on a data subject giving their consent for their data to be processed it must be in an 'intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.'<sup>4</sup>

<sup>4</sup> <https://www.eugdpr.org/key-changes.html>



# What important new rights do individuals have?

At the heart of GDPR are a key set of rights and freedoms.

- » **The right to fair processing of information:** The data subject must be told what personal data is being collected and what it will be used for. The information must be easy to understand, concise and intelligible. That is, don't hide behind legal complexity.
- » **The right of access:** Data subjects can request access to what personal data is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.
- » **The right to rectification:** If a record is incorrect or incomplete, then the data subject has the right to request that the data is rectified. And you must give notice that the rectification has taken place.
- » **The right to be forgotten:** Also known as Data Erasure. Under certain circumstances, the data subject can request that their data is erased or can stop it being processed or shared.
- » **The right to restrict processing:** Under certain circumstances, the data subject can request a restriction of the processing of their data for specific purposes.
- » **The right to data portability:** Under certain circumstances, the data subject can obtain and reuse their personal data for their own purposes across different services. They can request a move, copy or transfer of personal data easily from one IT environment without hindrance to usability, and in a machine-readable format.
- » **The right to object:** Data subjects can object to their data being used for things like profiling, direct marketing, or historical, scientific research or even statistical analysis.
- » **The right to be informed about data breach:** Under the GDPR, breach notification will become mandatory where a data breach is likely to "result in a high risk for the rights and freedoms of individuals".



### What about automated processing and decision making?

As the rise of Artificial Intelligence (AI) transforms the way data is processed, it's no surprise that GDPR also provides protection for individuals in the era of automation. It protects the data subject from 'automated decisions' (including profiling) based on their personal data.



### What if there's a personal data breach?

There is a requirement for the controller to notify the relevant statutory authorities within 72 hours of a personal data breach if it has a high risk of affecting the data subjects - which is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".



### What are the potential penalties for infringing the GDPR?

Most of the headlines about GDPR have focused on the potential penalties, but there are two tiers of fines: Some breaches will be subject to administrative fines of up to €10,000,000 or, 2% of global turnover, whichever is the higher. Others will be subject to administrative fines of up to €20,000,000 or, 4% of global turnover, whichever is the higher.



### Why does Fujitsu think the GDPR is important?

At Fujitsu, we believe in human centric technology. Digital transformation must be about enhancing our lives as well as the way we do business. We believe that the best way to approach GDPR is to think about it as an enhancement of our individual rights, and a means by which we can achieve fairness and transparency for each one of us in the digital age.



## It's all about trust, transparency and good governance

The bottom line is that your organization needs to create a culture of privacy that's focused on the rights of the individual. It must be all about the individual and be seen as a positive step forward for effective data management and governance. Your organization will be more efficient, transparent and better able to make use of data in a legitimate and human-centric way.



## FUJITSU

22 Baker Street, London W1U 3BW, United Kingdom

Tel: +44 (0) 123 579 771

Email: [askfujitsu@uk.fujitsu.com](mailto:askfujitsu@uk.fujitsu.com)

[fujitsu.com/global](http://fujitsu.com/global)

Reference: 3827

© FUJITSU 2018. Unclassified. All rights reserved. FUJITSU and FUJITSU logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.