European Commission

The GDPR: new opportunities, new obligations

What every business needs to know about the EU's General Data Protection Regulation

Justice and Consumers

Luxembourg: Publications Office of the European Union, 2018

Print	ISBN 978-92-79-79453-7	doi:10.2838/6725	DS-01-18-082-EN-C
PDF	ISBN 978-92-79-79430-8	doi:10.2838/97649	DS-01-18-082-EN-N

TABLE OF CONTENTS

CHAPTER 1

A BUSINESS OPPORTUNITY

The GDPR regulates the way businesses process and manage personal data. Effective as of 25 May 2018 and applicable to all businesses and organisations (e.g. hospitals, public administrations, etc.), it constitutes the biggest change to the EU's data protection rules in over 20 years.

Not only does the GDPR give citizens more control over how their personal data is used, it also significantly streamlines the regulatory environment for businesses.

It does this by establishing a uniform framework for data protection legislation across the EU. In other words, instead of each country having their own data protection laws, now the entire EU is governed by a single regulation. Thus, a company operating in different countries no longer needs to comply with multiple — often differing — regulations. Instead, they only need to conform to the GDPR in order to offer their services anywhere in the EU.

How the GDPR can benefit your company

- **One Union, one law:** a single set of rules makes it simpler and cheaper for companies to do business in the EU.
- **One-stop-shop:** in most cases, companies only have to deal with one Data Protection Authority (DPA).
- **European rules on European soil:** companies based outside the EU must apply the same rules as European companies when offering their goods or services to individuals in the EU.
- **Risk-based approach:** the GDPR avoids a burdensome, one-size-fits-all obligation and instead tailors obligations to the respective risks.
- **Rules fit for innovation:** the GDPR is technology neutral.

It's all about trust

The protection of personal data is an important concern for individuals. Hence, their trust in digital environments remains low. According to a Eurobarometer survey:

- eight out of 10 people feel they do not have complete control of their personal data;
- six out of 10 say they do not trust online businesses;
- more than 90% of Europeans say they want the same data protection rights across all EU countries.

The GDPR represents a new opportunity for your business to improve consumer trust through risk-based personal data management.

"Businesses that fail to adequately protect an individual's personal data risk losing consumer trust, which is essential to encouraging people to use new products and services."

CHAPTER 2

UNDERSTANDING THE GDPR

Does the GDPR apply to me?

In summary, the GDPR applies to ***any*** business that:

processes personal data by **automated** or **manual** processing (provided the data is organised according to criteria).

Even if your business only processes data on behalf of other companies, you still need to abide by the rules.

The GDPR applies if:

- your company processes personal data and is based in the EU, regardless of where the actual data processing takes place; or
- your company is established outside the EU but offers goods or services to, or monitors the behaviour of, individuals within the EU.

What is personal data?

Personal data refers to any information that relates to an identified or identifiable, living individual. This can include:

- name
- address and phone number
- location
- health records
- income and banking information
- cultural preferences
- ... and more.

Personal data that has been de-identified, or pseudonymised, but that can still be used to re-identify a person also falls under the scope of the GDPR. However, personal data that has been rendered irreversibly anonymous in such a way that the individual is no longer identifiable is not considered to be personal data and thus not governed by the GDPR.

The GDPR is also technology neutral, meaning it protects personal data regardless of the technology used or how the personal data is stored. Regardless of whether your business processes and stores personal data using a complex IT system or via paper-based files, you will be governed by the GDPR.

"Regardless of whether your business processes and stores personal data using a complex IT system or via paper-based files, you will be governed by the GDPR."

Be extra careful with special (sensitive) categories of personal data

If the personal data you collect includes information on an individual's health, race, sexual orientation, religion, political beliefs or trade union membership, it is considered sensitive. Your company can only process this data under specific conditions and you may need to implement additional safeguards, such as encryption.

What constitutes processing personal data?

According to the GDPR, actions such as collecting, using and deleting personal data all fall within the definition of processing personal data.

Do you monitor your premises via CCTV? Consult a database containing personal data for business purposes? Send promotional emails? Delete (digital) employee files or shred documents? Or post a photo of a person on your website or social media channels?

If you answered 'yes' to any of these, then your company is certainly processing personal data.

How does the GDPR help reduce costs?

The GDPR takes into consideration the needs of businesses. For example, the regulation aims to remove administrative requirements in order to reduce costs and minimise the administrative burden:

- **No more prior notifications:** the reform scraps most prior notifications to supervisory authorities, along with their associated costs.
- **Data Protection Officers:** companies mainly need to appoint a DPO if their core activities involve processing sensitive data on a large scale or involve the large-scale, regular and systematic monitoring of individuals. Public administrations have an obligation to appoint a DPO.
- **Data Protection Impact Assessments:** companies are only obliged to carry out a Data Protection Impact Assessment if a proposed data processing activity involves a high risk to the rights and freedoms of individuals.
- **Record keeping:** companies with less than 250 employees are not required to keep records unless the data processing is not incidental or involves sensitive information.

"The regulation aims to remove administrative requirements in order to reduce costs and minimise the administrative burden."

CHAPTER 3

YOUR OBLIGATIONS UNDER THE GDPR

The GDPR places direct data processing obligations on companies at an EU-wide level. According to the GDPR, a company can *only* process personal data under certain conditions. For instance, the processing should be fair and transparent, for a specified and legitimate purpose and limited to the data necessary to fulfil this purpose. It must also be based on one of the following legal grounds.

- The **consent** of the individual concerned.
- A **contractual obligation** between you and the individual.
- To satisfy a **legal obligation**.
- To protect the **vital interests** of the individual.
- To carry out a **task that is in the public interest**.
- For your company's **legitimate interests**, but only after having checked that the fundamental rights and freedoms of the individual whose data you are processing are not seriously impacted. If the person's rights override your interests, then you cannot process the data.

In focus: getting consent to use personal data

The GDPR applies strict rules for processing data based on consent. The purpose of these rules is to ensure that the individual understands what he or she is consenting to. This means that the consent should be **freely given, specific, informed** and **unambiguous** by way of a request presented in clear and plain language. Furthermore, consent should be given by an **affirmative act**, such as checking a box online or signing a form.

If you are processing personal data pertaining to a **child** based on consent, then parental consent is required. However, as the age threshold varies between 13 and 16 amongst different countries, it is advised that you consult national law.

Remember! Where someone consents to the processing of their personal data, you can only process the data for the purposes for which consent was given. Furthermore, you must give them the opportunity to withdraw their consent.

Determine your role and responsibility

Once you have determined that the GDPR applies to your business and that there is a processing of personal data, the next step is to determine your role.

Data protection rules distinguish between the data controller and the data processor, with different obligations applying to each. Whereas the data controller determines the purpose and means of processing the personal data, the data processor only processes the personal data on behalf of the data controller. However, this does not mean the processor can simply hide behind the data controller.

The GDPR requires that a data controller only engages a data processor who offers sufficient guarantees. These guarantees should be included in a written contract between the data controller and processor. The contract must also contain a number of mandatory clauses, including, for example, a clause stipulating that the data processor will only process personal data on the documented instructions of the data controller.

Obligations that protect individual rights

The GDPR includes a number of obligations aimed at protecting an individual's right to have control over their personal data.

Your obligation: providing transparent information

Companies must provide individuals with information on who is processing what and why. At a minimum, this information must clearly state:

- who you are;
- why you are processing the data;
- what the legal basis is;
- who will receive the data (if applicable).

In some cases, the information must also state:

- contact information of the DPO;
- legitimate interest (when the legitimate interest is the legal ground for processing);
- basis for transferring the data to a country outside the EU;
- how long the data will be stored;
- the individual's data protection rights (i.e. right to access, correction, erasure, restriction, objection, portability, etc.);
- how consent can be withdrawn (when consent is the legal ground for processing);
- whether there is a statutory or contractual obligation to provide the data;
- in the case of automated decision-making, information about the logic, significance and consequences of the decision.

"Companies must provide individuals with information on who is processing what and why."

Your obligation: right to access and right to data portability

Individuals have the right to request access to their personal data, free of charge and in an accessible format. If you receive such a request, then you have to:

- tell the individual if you are processing their personal data;
- inform them about the processing (such as the purposes of the processing, categories of personal data concerned, recipients of their data, etc.);
- provide a copy of the personal data being processed.

In addition, when the processing is based on consent or a contract, the individual can ask for their personal data to be returned or transmitted to another company. This is known as the right to data portability. The data should be provided in a commonly used and machine-readable format.

Even though these two rights are closely related, they are nonetheless two distinct rights. Thus, you must make sure that there is no confusion between the two rights and inform the individual accordingly.

Your obligation: right to erasure (right to be forgotten)

In some circumstances, an individual can request that the data controller erase their personal data, such as when the data is no longer needed to fulfil the processing purpose. However, your company is not obliged to comply with an individual request if:

- the processing is necessary to respect one's freedom of expression and information;
- you must keep the personal data to comply with a legal obligation;
- there are other reasons of public interest to keep the personal data, such as public health or scientific and historical research purposes;
- you need to keep the personal data to establish a legal claim.

Your obligation: right to correct and right to object

If an individual believes that their personal data is incorrect, incomplete or inaccurate, he or she has the right to have it rectified or completed without undue delay.

An individual may also object at any time to the processing of their personal data for a particular use when your company processes it on the basis of your legitimate interest or for the performance of a task in the public interest. Unless you have a legitimate interest that overrides the interest of the individual, you must stop processing the personal data. Likewise, an individual can ask to have the processing of their personal data restricted while it is determined whether or not your legitimate interest overrides their interest. However, in the case of direct marketing, you are always obliged to stop processing the personal data at the request of the individual.

A word of caution on automated decision-making and profiling

Individuals have the right not to be subject to a decision that is based solely on automated processing. However, there are some exceptions to this rule, such as when the individual explicitly consented to the automated decision. Except where the automated decision is based on a law, your company must:

- inform the individual about the automated decision-making;
- give the individual the right to have the automated decision reviewed by a person;
- give the individual the opportunity to contest the automated decision.

For example, if a bank automates its decision of whether or not to grant a loan to a certain individual, that individual should be informed of the automated decision and given the opportunity to contest the decision and request human intervention.

Obligations based on risk

In addition to the obligations aimed at protecting individual rights, the GDPR also contains a number of obligations whose application depends on the risk.

Your obligation: appoint a Data Protection Officer (DPO)

A DPO is responsible for monitoring your compliance with the GDPR. One of the DPO's core tasks is to inform and advise employees who carry out the actual processing of personal data about their obligations. The DPO also cooperates with the DPA, serving as a contact point towards the DPA and individuals.

Your company is required to appoint a DPO when:

- you regularly or systematically monitor individuals or process special categories of data;
- this processing is a core business activity; and
- you do it on a large scale.

For example, if you process personal data to target advertising through search engines based on people's online behaviour, then the GDPR requires that you have a DPO. If, however, you only send your clients promotional material once a year, then you will not need a DPO. Likewise, if you are a physician who collects data on patients' health, a DPO is probably not needed. But if you process personal data on genetics and health for a hospital, then a DPO will be required.

Your obligation: data protection by design and default

The GDPR introduces two new principles: data protection by design and data protection by default.

Data protection by design helps ensure that a company takes data protection into account at the early stages of planning a new way of processing personal data. In accordance with this principle, a data controller must take all necessary technical and organisational steps to implement the data protection principles and protect the rights of individuals. These steps could include, for example, using pseudonymisation.

Data protection by design minimises privacy risks and increases trust. By placing data protection at the forefront of developing new goods or services, any possible data protection issues can be avoided at an early stage. Furthermore, this practice helps raise awareness about data protection across all departments and levels of a company.

Data protection by default entails ensuring that your company always makes the most privacy friendly setting the default setting. For example, if two privacy settings are possible and one of the settings prevents personal data from being accessed by others, this should be used as the default setting.

"Data protection by design minimises privacy risks and increases trust."

"Data protection by default entails ensuring that your company always makes the most privacy friendly setting the default setting."

Your obligation: providing proper notification in the case of a data breach

A data breach occurs when the personal data for which you are responsible is disclosed, either accidentally or unlawfully, to unauthorised recipients or is made temporarily unavailable or altered.

It is vital for a business to implement appropriate technical and organisational measures to avoid data breaches. However, if a data breach does occur and the breach poses a risk to individual rights and freedoms, you should notify your DPA within 72 hours after becoming aware of the breach.

Depending on whether or not the data breach poses a *high* risk to those affected, a business may also be required to inform all individuals affected by the data breach.

Transferring personal data outside the EU?

The GDPR applies to the European Economic Area (EEA), which includes all EU countries plus Iceland, Liechtenstein and Norway. When personal data is transferred outside the EEA, the protections offered by the GDPR should travel with the data. This means that to export data abroad, companies must ensure that certain safeguards are in place.

The GDPR offers a diversified toolkit of mechanisms to transfer data to third countries. According to the GDPR, such transfers are allowed when:

1. the country's protections are deemed adequate by the EU; or
2. your company, for instance, takes the necessary measures to provide appropriate safeguards, such as by including specific clauses in the contract concluded with the non-European importer of the personal data; or
3. your company, for instance, relies on specific grounds for the transfer (called 'derogations') such as the consent of the individual.

For more information on the rules applying to international data transfers, consult the European Commission's Communication on Exchanging and Protecting Personal Data in a Globalised World: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0007&from=EN

Do you need to conduct a Data Protection Impact Assessment (DPIA)?

Conducting a DPIA is mandatory whenever the intended processing would pose a high risk to the rights and freedoms of individuals. This may be the case, for example, when new technologies are used.

According to the GDPR, there is at least such a high risk when:

- automated processing and profiling mechanisms are used to systematically and extensively evaluate individuals;
- a publicly accessible area is systematically monitored on a large scale (e.g. CCTV);
- sensitive data is processed on a large scale (e.g. health data).

The purpose of the DPIA is to identify potential risks to the rights and freedoms of individuals before the processing of personal data begins and before the risk materialises. By mitigating the risk up front, damage can be avoided and costs minimised.

If the measures indicated in the DPIA fail to remove all the identified high risks, the DPA must be consulted before the intended data processing takes place.

"Conducting a DPIA is mandatory whenever the intended processing would pose a high risk to the rights and freedoms of individuals."

What you need to do

Responding to requests

If your company receives a request from an individual who wants to exercise their rights, you should respond to this request without undue delay and in any case within 1 month of receiving the request. However, this response time may be extended by 2 months for complex or multiple requests, so long as the individual is informed about the extension. Furthermore, requests should be dealt with **free of charge**. If a request is rejected, then you must inform the individual of the reasons for doing so and of their right to file a complaint with the DPA.

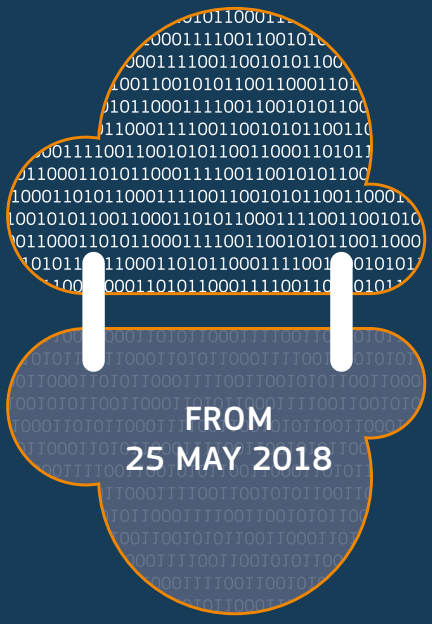
Demonstrate compliance and keep records!

One of the core principles underlying the GDPR is to ensure that companies can demonstrate compliance. This means you must be able to prove that your company acts in accordance with the GDPR and fulfils all applicable obligations — particularly upon request or inspection from the DPA.

One way to do this is to keep detailed records on such things as:

- name and contact details of your business involved in data processing;
- reason(s) for processing personal data;
- description of the categories of individuals providing personal data;
- categories of organisations receiving the personal data;
- transfer of personal data to another country or organisation;
- storage period of the personal data;
- description of security measures used when processing personal data.

In addition, your company should also maintain — and regularly update — written procedures and guidelines and make them known to your employees.



CHAPTER 4

READY TO COMPLY?

When it comes to the processing of personal data, the GDPR puts the ball in your court. The first step is to map out your current data processing activities and re-evaluate your internal business processes. In particular, you must:

- identify which data you hold and for what purpose and on what legal basis you hold it;
- assess all contracts in place, in particular those between controllers and processors;
- evaluate all available avenues for international transfers; and
- review your company's overall governance (i.e. what IT and organisational measures you have in place), including whether or not you have to or want to appoint a Data Protection Officer.

An essential element in this process is ensuring that your company's highest level of management is involved in such reviews, providing input and being regularly updated and consulted on changes to the data policy.

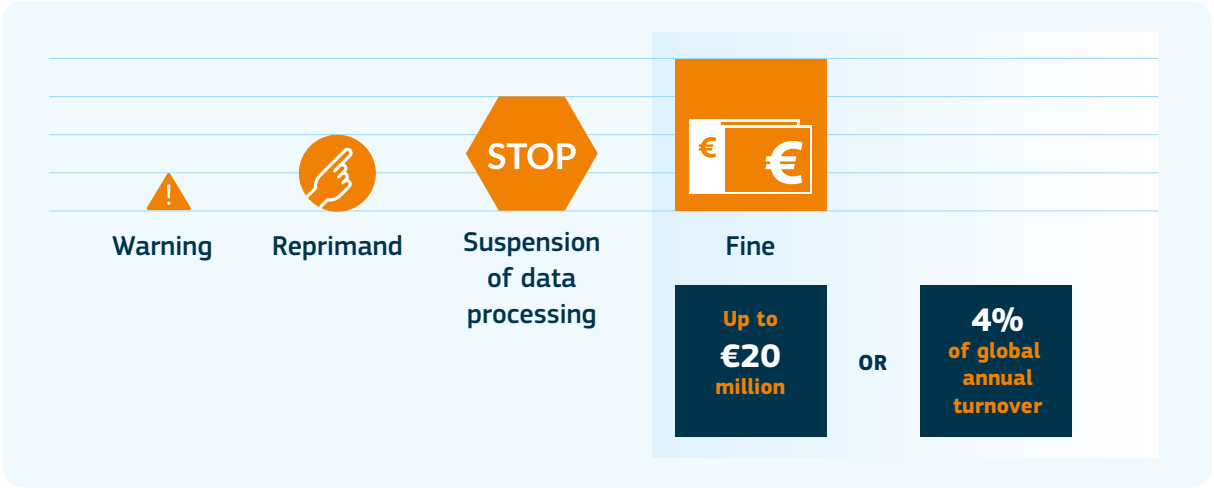
Processing data in more than one country?

For cross-border processing, a supervisory authority of another country, and not your national DPA, may be the competent authority. Typically, this is the DPA of the country that hosts your company's main establishment (where decisions about the means and purposes of processing are made) within the EU.

The risks of non-compliance

Failure to comply with the GDPR may result in significant fines — of up to EUR 20 million or 4% of your company's global turnover for certain breaches. The DPA may impose additional corrective measures, such as ordering the cessation of the processing of personal data. You should also consider the reputational damage that non-compliance could cause.

Clearly, the costs of not complying with the GDPR are far greater than any investment made to comply with it.



Questions? Concerns? Please consult your national DPA.

Find your national Data Protection Authority online

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

IMPORTANT NOTICE

The information and guidance in this brochure are intended to contribute to a better understanding of EU data protection rules.

This is intended purely as a guidance tool — only the text of the General Data Protection Regulation (GDPR) has legal force. As a consequence, only the GDPR is liable to create rights and obligations for individuals. This guidance does not create any enforceable right or expectation.

The binding interpretation of EU legislation is the exclusive competence of the Court of Justice of the European Union. The views expressed in this guidance are without prejudice to the position that the Commission might take before the Court of Justice.

Neither the European Commission nor any person acting on behalf of the European Commission is responsible for the use which might be made of the information in the brochure.

This brochure reflects the state of the art at the time of its drafting, it should be regarded as a 'living document' open for improvement and its content may be subject to modifications without notice.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres.
You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: https://europa.eu/european-union/contact_en

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/bookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU.
Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

DS-01-18-082-EN-N

The General Data Protection Regulation (GDPR) regulates the way businesses process and manage personal data. With a single European law for the protection of personal data, your company now needs to conform primarily to one data protection law while offering goods and services anywhere in the EU.

By simplifying the regulatory environment for businesses, the GDPR represents a new opportunity for your business to improve personal data management and subsequently increase consumer trust in your business.

This brochure highlights the obligations your company has under the GDPR.

europa.eu/dataprotection

Publications Office