The General Data Protection Regulation in Plain Language

Bart van der Sloot

Amsterdam University Press

Cover illustration: Defense Advanced Research Project Agency (DARPA)

Cover design: Gijs Mathijs Ontwerpers
Lay-out: Crius Group, Hulshout

ISBN 978 94 6372 651 1
e-ISBN 978 90 4854 466 0
NUR 740

Table of Contents

Who is who?

- *Europe* is a continent of about 50 officially recognised sovereign states.
- The *Council of Europe* is a European supra-national organisation of which most European countries – 47 in total – are members. The Council of Europe focuses almost exclusively on the protection of human rights.
- The *European Convention on Human Rights* is the main legal instrument of the Council of Europe, covering essential civil and political human rights, such as the right to a fair trial, the right to privacy, freedom of expression and the principle of non-discrimination.
- The *European Court of Human Rights* is the highest court of the Council of Europe and deals with the interpretation of the European Convention on Human Rights.
- The *European Union* is a supra-national organisation of which 28 European countries are members (27 after Brexit has been finalised). Originally, the European Union (EU) was mainly concerned with socio-economic issues and the creation of a single European market, but more recently it has also adopted legal instruments that concern the protection of fundamental rights.
- A *Member State* is the term used for a sovereign country that is a member of the European Union, such as France, Germany and Italy.
- The *European Commission* can be compared to the government (executive power) of the EU; each Member State can nominate one Commissioner (to be compared with a minister). The head of the European Commission is elected by the European Parliament. The Commission drafts most of the legislative proposals, although it is itself not formally part of the legislative power.
- The *European Parliament* is the parliament of the EU; its members are elected through EU-wide elections. Together

with the Council of the European Union, the Parliament forms the legislative power of the EU. It also controls and critically assesses the functioning of the EU's executive power.

- The *Council of the European Union* consists of the heads of state of each EU Member State. When legislative proposals by the Commission are discussed with the Parliament and the Council, this is typically called the trialogue.
- The European *Court of Justice* is the highest court in the European Union and deals with the interpretation of the Charter of Fundamental Rights, the General Data Protection Regulation and other legal instruments of the European Union.
- The *Charter of Fundamental Rights* can be compared to the constitution of the European Union, containing the fundamental rights and rules related to the organisation and functioning of the EU.
- The *General Data Protection Regulation* (GDPR) lays down the general data protection framework within the European Union. Adopted in 2016, it replaces its 1995 predecessor, the Data Protection Directive. The GDPR is applicable as of May 2018.
- Also adopted in 2016 and applicable as of May 2018, the *Law Enforcement Directive* provides the data protection framework for processing personal data in the law enforcement context. These rules are in essence similar to those of the GDPR, but allow for more exceptions when necessary in light of the fight against crime or the protection of public order.
- *Personal data* is information relating to an identified or identifiable natural person (meaning a person of flesh and blood and not, for example, a legal person). The sentence 'Chelsea Manning is a hero' contains personal data, the sentence 'Grass is green' or 'Amazon's delivery service stinks' does not.
- The *data subject* is the person that the personal data refer to. In the sentence 'Eric has blue eyes', Eric is the data subject.

- The GDPR applies when personal data are processed, where *processing* is almost every action involving personal data, such as gathering, storing and using, but also correcting, completing and deleting data.
- The *controller* is the person or organisation responsible for processing personal data. The controller decides which data will be processed, how and why. For example, if a pizza delivery service processes the name and the post code of a customer, the pizza delivery service is the controller.
- The controller can be assisted by a *processor*. The processor is the person or organisation that processes data on behalf of the controller. For example, a cloud provider that is paid by the pizza delivery service to store personal data on its behalf can be considered a processor. When the GDPR applies, there is always a data subject and always a data controller, but not necessarily a processor, because the data controller can also chose to perform all data processing activities on its own. If a processor is appointed, in principle, the data controller is responsible for the actions of the processor.
- Two parties that determine the purpose and means for processing personal data together will be considered *joint controllers,* and they will share the responsibilities imposed by the GDPR.
- If the processor contracts another party to process personal data on its behalf, that party will be considered a *sub-processor.* If the cloud provider hired by the pizza delivery service to store personal data contracts a number of data centres which provide storage space, these data centres are sub-processors. The processor should see to it that the sub-processor abides by the rules and obligations under the GDPR; ultimately, the controller is responsible for the conduct of both the processor and the sub-processor.
- If a controller or processor processes personal data about EU citizens, but does not have an establishment in the EU, it has to appoint a *representative*. The representative should be based on EU territory and serves as the main contact point

for that organisation within the EU, for example for data subjects that want to invoke their rights or for supervisory authorities in the course of their investigations.

- Many organisations processing personal data are obliged to appoint a *Data Protection Officer* (DPO). DPOs must ensure that the rules in the GDPR are respected by the organisations that have appointed them.
- Each Member State has to set up a *national supervisory authority*, usually called the Data Protection Authority. This is an independent but government-funded public organisation responsible for overseeing the applicability of and compliance with the GDPR by people and organisations processing personal data.
- Member States can also appoint more than one supervisory authority, for example a separate supervisory authority per region or province or a separate supervisory authority for specific sectors, such as the telecom sector. In that case, there should be one *main supervisory authority* which is the national supervisory authority that coordinates the actions of the various national data protection authorities and participates, on behalf of all national supervisory authorities of that Member State, in the European Data Protection Board. When a country only has one national supervisory authority, that authority is the main supervisory authority.
- All main supervisory authorities of each EU Member State participate in the *European Data Protection Board* (*EDPB*). This Board can issue opinions and guidelines on the interpretation of the GDPR and can function as an arbitration mechanism when two or more national supervisory authorities have a conflict. Under the 1995 Data Protection Directive, the European Data Protection Board was called the *Article 29 Working Group*. This Working Group no longer exists.
- The *European Data Protection Supervisor* (EDPS) is the Data Protection Authority for the EU and advises on the processing of personal data by EU institutions. The GDPR does not apply when an EU institution itself processes personal data.

Data processing by EU institutions is covered by a separate Regulation which includes rules similar to the GDPR.

– When a company operates in more than one EU country and/or processes data about citizens of more than one EU country, each of the national supervisory authorities of those countries are considered a *supervisory authority concerned*. This means that they should be consulted by and have a right to object to the decisions taken by the lead supervisory authority.
– The *lead supervisory authority* is the supervisory authority concerned that takes the lead in overseeing the activities of an organisation in more than one EU country. The other supervisory authorities concerned follow the lead of this authority, but can submit objections to its decisions to the EDPB.

1. Introduction

The General Data Protection Regulation (GDPR) contains rules about when and under what conditions it is permitted to collect, store, analyse and use personal data. Virtually every person and every organisation processes personal data: an online advertising company, a governmental organisation that registers car ownership, a school teacher who gives grades to students or a private person posting a photo of her friends on Facebook.

The GDPR document has 88 pages, containing no fewer than 99 articles and 173 recitals that provide more background information on the articles. The GDPR contains rules on retention periods, the conditions for sharing personal data with others, rules for processing sensitive personal data and several obligations related to issues such as transparency, accountability and data security.

This book explains these rules in plain language. It discusses the situations in which the GDPR applies (Chapter 2), what the basic data protection principles of the EU are (Chapter 3), the duties of organisations that process personal data (Chapter 4), which rights citizens can invoke (Chapter 5) and how these rights and duties are enforced (Chapter 6).

This book is aimed primarily at private and public organisations that want to understand what rules they have to comply with; data protection officers who are looking for a quick guide to the data protection landscape; citizens who want to know which rights they can invoke, and how; and students who want to know what is in the GDPR, without having to plough through almost 100 pages of legal jargon.

This first chapter will provide important background information on the right to data protection in the EU and will introduce the main ideas behind it, it will explain what the new rules provided by the GDPR look like and why it is important to understand and respect them. If you are only interested to know what is actually in the GDPR, please go to Chapter 2 directly.

1.1 The who, what, where, when and why of the GDPR

Who? Europe is a continent of about 50 sovereign national states. It encompasses a complex web of supra-national organs and institutions, of which the difference between the European Union and the Council of Europe is the most important.

The European Union has adopted the Charter of Fundamental Rights, the General Data Protection Regulation and a large number of legal instruments in other fields, such as telecommunication law, agriculture, law enforcement and immigration. The European Court of Justice (ECJ) is the highest court of the European Union. Twenty-eight countries are members of the European Union (twenty-seven when the Brexit is finalised). The Council of Europe has adopted the European Convention on Human Rights (ECHR), which is overseen by the European Court of Human Rights (ECtHR). Forty-seven European countries are members of the Council of Europe. All EU Member States are also members of the Council of Europe.

Initially, the division of tasks between the Council of Europe and the European Union was clear: the Council of Europe focused on protecting human rights, while the EU, as the successor of the *European Coal and Steel Community*, was mainly concerned with economic and socio-economic issues. Gradually, however, the European Union has adopted rules and regulations on almost every aspect of society, including human rights. The Charter of Fundamental Rights can be seen as the constitution of the European Union; together with the ECHR, it is the highest human rights instrument in Europe. There is no official hierarchy between the two documents or the two courts, but informally, the ECHR and the judgments of the ECtHR take precedence over the Charter and the judgments of the ECJ.

The Charter of Fundamental Rights of the European Union contains rights such as freedom of religion, freedom of speech, the right to privacy and the right to data protection. The General Data Protection Regulation contains specific rules that detail how

the fundamental right to data protection is guaranteed in the EU. The GDPR can be compared to a country's anti-discrimination law that lays down specific rules on how to interpret and apply the constitutional prohibition on discrimination. The constitutional doctrine has higher legal status than the law, just like the fundamental right to data protection in the Charter has priority over the GDPR.

EU laws such as the General Data Protection Regulation take precedence over national laws. If, for example, Italian law conflicted with the GDPR, the Italian law would be declared invalid and the GDPR would take precedence. Similarly, decisions by the ECtHR and the ECJ take precedence over decisions by national courts.

What? The new rules on data protection in the EU are set out in a Regulation: the General Data Protection Regulation. The old rules were set out in a Directive: the Data Protection Directive of 1995. The difference between a Regulation and a Directive has important practical effects.

A Directive is a document that is adopted by the EU but needs to be implemented by each Member State individually. Citizens can only rely directly on an EU Directive on an incidental basis and in principle have to refer to the national law that is based on that Directive. This means that although the general legal framework is set out by the EU, each country implements these rules slightly differently, according to its cultural and political standards.

In contrast to a Directive, a Regulation has direct effect. This means that citizens can directly rely on the Regulation. Member States do not need to implement the rules contained in the GDPR in their national laws. This harmonises the data protection rules across the European Union. Persons and organisations that process personal data have to respect the Regulation as such. The GDPR makes an exception to this rule on a small number of points, such as the processing of sensitive personal data, the processing of personal data of minors and the exceptions to the data protection framework that are allowed when processing personal data is

necessary in a number of clearly defined matters of public interest. On these points, Member States are allowed to provide specific rules and there may be slight differences between countries.

Where? Of the 50 independent sovereign nations on the European continent, 47 are members of the Council of Europe. Only countries such as Belarus and Vatican City are not. This means that almost all European countries are bound by the European Convention on Human Rights, including such countries as Russia, Turkey and the United Kingdom, even after Brexit (Brexit means leaving the EU, not the Council of Europe). The European Union has far fewer Member States, namely 28. These are: Austria, Belgium, Bulgaria, the Czech Republic, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. Consequently, only 28 countries are directly bound by the General Data Protection Regulation and when Brexit is finalised, this number will drop to 27.

Nevertheless, the Regulation will have a broader effect for at least three reasons.

First, four countries – Iceland, Norway, Switzerland and Liechtenstein – are part of the European Free Trade Association. These countries participate in the European Single Market. Iceland, Norway and Liechtenstein have agreed that the GDPR should apply on their territory, while Switzerland has made a special arrangement (see section 3.5). There are also countries that would like to join the European Union and are therefore generally inclined to follow the rules of the EU. These are Albania, Montenegro, Serbia, North Macedonia, Bosnia-Herzegovina and Kosovo (there are also official negotiations with Turkey, but these have stagnated). Finally, there are overseas territories where the GDPR is directly applicable, such as former colonies of EU countries in South America, which are still part of their national territory.

Second, the GDPR applies not only to organisations based in the EU, but also to organisations based outside the EU that

operate in the EU's market. For example, if a US company offers products through a website targeted at German-speaking customers (German being the main language of Austria, Germany and Switzerland) and processes personal data of its customers, it is directly bound by the GDPR, even though it might not have an establishment in the EU.

Third, the GDPR sets the highest data protection standard in the world. As these rules are equally applicable throughout the EU, personal data may be transferred from each EU country to every other EU country. However, in principle, it is not permitted to transfer personal data to countries outside the EU, as this would mean that the strict data protection rules would no longer apply.

There can be an exception to this prohibition if, on the one hand, after negotiations with the European Commission and after substantial changes to its national legislation, a non-EU country has adopted legislation that provides a level of data protection similar to that of the GDPR. The European Commission has so far recognised Andorra, Argentina, Canada (but only for commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing an adequate level of protection. A special arrangement has been made for the United States of America and there are ongoing adequacy talks with South Korea. Thus, a company operating on EU soil with an office in Poland and its headquarters in Israel may safely transfer personal data of EU citizens to its headquarters.

On the other hand, if a country does not have a data protection regime equivalent to that of the GDPR, a non-EU-based organisation may commit itself to upholding such a level of data protection. For example, if a Swedish and an Australian organisation want to share personal data, this is in principle prohibited, unless they sign a contract in which the Australian organisation commits itself to treating the personal data it receives under a data protection framework that is essentially equivalent to the framework provided by the GDPR.

Because most multinationals around the world want to do business in the European Union (the second-largest economy in

the world) or with organisations within the EU, and because this almost by definition involves processing personal data, these organisations will need to commit themselves to the EU data protection regime, at least with respect to the processing of personal data about EU citizens and activities taking place on EU soil.

When? The Regulation was adopted in April 2016 and entered into force in May 2018. This gave organisations processing personal data two years to implement the data protection rules in their internal operations. The GDPR replaces the Data Protection Directive of 1995. In fairness, most of the rules contained in the GDPR were already present in the 1995 Directive. The reason for replacing the Directive was that it contained few possibilities for fines and sanctions for organisations that did not respect the data protection rules. This meant that not all organisations made it a priority to respect the data protection principles. Under the GDPR, this has changed and a sanction of up to 20 million euros or, for a company, up to 4% of its total worldwide annual turnover in the previous financial year, can be imposed for each violation, among other measures. That is why, from May 2018, most organisations needed to do two things: implement the rules that had been in place since 1995 and implement a number of additional rules provided by the GDPR.

Why? The reason for replacing the Directive with the Regulation was that there was a gap between law and practice. The Data Protection Directive already contained strict data protection rules, but these were only marginally respected by companies and governmental organisations. To remedy this problem, five changes to the data protection regime were made.

1. *Harmonisation of the rules*: there were substantial differences in the way EU countries had implemented the rules from the 1995 Data Protection Directive in their national legislation. One of the explicit goals of the 1995 EU data protection framework was removing obstacles to the transfer of personal data within the European Union, by laying down

one common level of data protection. However, because a Directive needs to be implemented by each Member State individually and because they have a margin of discretion when doing so, organisations still had to comply with different rules in, for example, Germany and the Netherlands, which hampered business operations. Consequently, companies often established their headquarters in the country with the most flexible interpretation of the data protection rules. This obstacle has been addressed by laying down the data protection framework in a Regulation instead of a Directive.

2. *Harmonisation of enforcement:* the second problem with the 1995 Directive was that enforcement of the data protection rules also took place at national level. Each EU country had to ensure compliance with the data protection framework on its own territory. Countries differed as to how actively they enforced the data protection rules; some had a well-equipped, well-resourced and well-functioning data protection authority, while others had understaffed data protection authorities with very limited powers of oversight and enforcement. Again, this allowed companies to place their headquarters in countries with a low level of enforcement, thereby practically circumventing the EU data protection rules. This problem is tackled in the GDPR by placing more powers of oversight and enforcement in the hands of EU bodies and by allowing national supervisory authorities to take action across the EU.
3. *Enforcement powers strengthened:* because there were few rules on sanctions and fines in the Data Protection Directive, not all boardrooms put data protection compliance at the top of their agenda. The GDPR tackles this problem by enabling supervisory authorities to impose high sanctions and penalties in case of a violation. The GDPR also gives the data protection authorities powers to act more stringently and effectively. The emphasis on enforcing the data protection framework has meant that the decision-making process regarding data protection within organisations has moved from the lower echelons to the boardroom.

4. *Distributed enforcement:* under the Data Protection Directive, the basic model for enforcement was that every EU Member State would install a governmental organisation tasked with overseeing the application of the data protection regime and sanctioning violations. Such a model was still viable in the 1990s, because the number of data-driven processes was limited. Like other sectors with a sector-specific supervisory authority, such as telecoms, finance and healthcare, it was still possible for a national data protection authority to oversee all or most data-driven processes on its territory. But this is no longer viable, because data processing is not limited to a specific sector or to a number of organisations. Rather, virtually every organisation and every person processes personal data. As it is impossible for one governmental agency to oversee all people and organisations on its territory, the GDPR moves the role of the governmental supervisory authority to the second tier. At the first level, organisations processing personal data are not only obliged to follow the data protection principles, they also have to create instruments of oversight and control within their organisation. Among others, they have to document all data processes within their organisation; do an impact assessment for riskier and larger-scale data operations in order to prevent and mitigate harm; and implement organisational and technical measures to ensure compliance with the GDPR. Many organisations also have to appoint an independent Data Protection Officer to ensure GDPR compliance. At the second level, the supervisory authorities have the role of assessing the extent to which organisations adequately oversee their own compliance with the GDPR. Not only can supervisory authorities sanction organisations that do not adequately protect personal data, they can also impose fines when organisations do not adequately monitor their own compliance with the data protection framework, whether or not any of the material rules and provisions have been violated.

5. *Less emphasis on individual control:* the 1995 Directive emphasised the rights of data subjects – the individuals whose personal data are processed. This created a problem, because most citizens do not keep tabs on all the data that are gathered about them via cookies, sensors, CCTV cameras and other devices. People who are unaware of the fact that their data are gathered will not invoke their legal rights. In addition, because data processing is so widespread in modern society, it is almost impossible for an individual to take control over her personal data. It is estimated that there are about 5,000 organisations that process personal data about an average citizen. It is impossible for any person to assess in every case whether an organisation has respected all relevant data protection rules and if it has not, to start legal proceedings to correct any violation. For example, if a citizen read the terms and conditions and privacy policies she has to agree with on the internet, this alone would take on average one to two months a year. That is why the GDPR not only strengthens the rights of data subjects and increases obligations of transparency for organisations processing personal data, it also gives supervisory authorities increased powers to take action against violations of the GDPR, independent of any complaint by an individual, and explicitly allows Member States to provide a framework for collective actions. In addition, the GDPR discourages organisations from relying on the consent of individuals for legitimating data processing activities.

1.2 When is the GDPR relevant?

Many people and organisations believe that the GDPR is not applicable to them, but this assumption is usually false. Almost every organisation and every person processes personal data. Here are some basic examples to give you an idea: