GDPR and data protection globally

Clément Levallois

2017-11-01

Table of Contents

1. Evolution of data protection regulations in the EU . . . 1
   a. The Directive on Data Protection by the EU in 1995 . . . 1
   b. The case of EU citizen data hosted by US-based companies . . . 1
   c. GDPR, a new legal framework . . . 2
2. Key definitions . . . 3
   a. Personal data . . . 3
   b. Sensitive data . . . 3
   c. Data subject . . . 3
   d. Data controller (DC) . . . 3
   e. Data processor (DP) . . . 3
4. Four key principles for the rightful processing of personal data . . . 4
   a. Prior consent . . . 4
   b. Adequacy / legitimate purpose . . . 4
   c. Portability . . . 4
   d. Safety . . . 4
5. In 2018: the GDPR and what it changes . . . 5
   a. Application . . . 5
   b. Responsibility . . . 5
   c. Penalties . . . 5
   d. Consent . . . 5
   e. Data breaches . . . 5
   f. Data Subjects' Rights . . . 5
   g. Privacy by design . . . 6
   h. Data Protection Officer (DPO) Appointment . . . 6
6. Data protection: a quick view outside the EU . . . 6
   a. U.S.A. . . . 6
   b. India . . . 6
   c. China . . . 6
The end . . . 7

last modified: 2018-06-20

1. Evolution of data protection regulations in the EU

a. The Directive on Data Protection by the EU in 1995

This Directive derives from earlier guidelines adopted by the OECD as far back as 1980 on the Protection of Privacy and Transborder Flows of Personal Data.

These guidelines were adopted by OECD members but were non binding: for instance, the US did not translate the OECD guidelines on the protection of privacy into their legislation. In contrast, these guidelines were turned into a Directive in the EU, in 1995.

- full text of the EU Directive on Data Protection
- Wikipedia presentation of the EU Directive on Data Protection on

This Directive guarantees and facilitates the free movement of personal data across EU States, by providing a framework valid for all member States for the protection of personal data of EU citizens.

How is handled the issue of EU data owned by non EU companies? For example, what is the level of protection for the personal data of a French individual, owned by a US company on a server located in the US?

→ According to the 1995 Directive, th rule was simple: **it is forbidden to export personal data to a non EU-country with a lower level of personal data protection.**

b. The case of EU citizen data hosted by US-based companies

The case is important as major providers of services involving personal data (google search, gmail, gmaps, facebook, etc.) is hosted in the US.

The question is: what it the level of data protection in this case? US-level of protection or EU?

It should not be possible to host EU citizen personal data in the US because the US have much less

stringent regulations in these matters. Indeed, in the US:

- There is a regulatory framework on data protection for data collected or held by the Federal government
- But there is no general framework on data protection outside the Federal government (states level).

To remedy this situation, the Safe Harbor principles is an international agreement between the USA and EU which was put in place in 2000.

The Safe Harbor principles are a series of regulations which US companies can agree to follow if they want to host EU personal data outside the EU. These rules provide a level of data protection equivalent to the one guaranteed by the 1995 Data Protection Directive in the EU.

In October 2015, Maximillian Schrems (a student in law in Austria) launched a lawsuit against Facebook for failure to protect his personal data against the spying of the NSA in the USA.

The defense of Facebook was to argue that it complied with the Safe Harbor Act. The lawsuit went to the European Court of Justice which ended up **declaring the Safe Harbor Act invalid** because:

"legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life"."

The following months were a state of legal uncertainty as the EU data hosted on US servers were so under no legal conditions.

On 2nd February 2016, the EU and the US created a new legal agreement known as the EU-US Privacy Shield. The the Privacy Shield differs from the Safe Harbor Act in the following:

1. Stronger obligations on companies in the US to protect the personal data of Europeans' and stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission.
2. Access to personal data transferred under the new arrangement by public authorities on the US was scheduled to be subject to clear conditions, limitations and oversight, preventing generalized access by state surveillance organizations.
3. Effective protection of EU citizens' rights with several redress possibilities.
4. An annual joint review mechanism between the EU and the US.

c. GDPR, a new legal framework

The handling of EU citizen data outside of the EU is of a great legal complexity, as evidenced by the fragility of the EU-US legal agreements. Should the EU create special legal agreements with each and every country wishing for their companies to be able to host EU personal data? This seems like a bureaucratic nightmare (or a lawyer’s dream).

Instead, the EU has designed **a new legal principle** applying to all countries holding EU personal

data, without the need for bilateral agreements. **This is the GDPR**.

The **GDPR: General Data Protection Regulation** is a legal framework coming into place in 2018, replacing the 1995 Directive by a new, simple rule: EU citizen data must be handled according to the rules stated by the EU, **wherever these data are stored or processed**.

Before examining the GDPR in more details, we define the legal terms used in it:

2. Key definitions

Source for these key definitions : a synthetic whitepaper on the GDPR by Dataiku.

a. Personal data

Personal data is any information related to a human being (or data subject) that can be used to directly or indirectly identify that person.

For example: name, photos, email addresses, bank details, posts on social networking websites, medical information, IP addresses, etc.

b. Sensitive data

Sensitive data is a special category of personal data (including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life) to which additional protections apply.

c. Data subject

A data subject is a human being on whom personal data is being collected.

d. Data controller (DC)

A data controller is an entity that determines the purposes, conditions, and means of the processing of personal data. When the organization is large enough, a dedicated position of "Data Controller" can be created.

Ex: in France, the DC is in charge of declaring the personal data being processed to the CNIL.

e. Data processor (DP)

A data processor An entity that processes personal data on behalf of the controller (e.g., cloud and data center providers).

Until 2017, it was considered that the data processor is just "executing" the mission given by the DC:

- the DP is in charge of proper security measures to ensure data protection against breach, loss…
- but the DP is not liable for the improper collection procedures of personal data set up by the

data controller.

Starting in 2018 with the GDPR (see next), the DP is co-responsible with the DC in case of a data breach compromising the personal data of subjects.

4. Four key principles for the rightful processing of personal data

a. Prior consent

Prior consent is required before collecting personal data in view of processing it:

- Data collection policy should be made clearly available to users
- Opt out should be possible
- Consent should be presented clearly

b. Adequacy / legitimate purpose

The data collected should be exactly necessary to run the service, not more.

Time out: information should be deleted when service stops. In France, there is a 13 month limit after which consent must be renewed.

c. Portability

→ Information should be available on request

In 2011 Max Schrems requested all his Facebook data. He received 1,200 pages of it.

Thanks to his efforts, now most of social media offer a one-click download of your personal data.

Portability also covers the "right to be forgotten".

d. Safety

All reasonable precautions should be taken against data breaches.

Precautions taken should be scaled to the damage which would result from a breach in security.

Basics: define and manage access rights to each relevant aspects of the data.

Users should be told about security breaches potentially affecting their data

5. In 2018: the GDPR and what it changes

GDPR stands for "General Data Protection Regulation". It was adopted by the EU on April 14, 2016 and was enforced on **May 25, 2018**.

Its key novelties, compared to the EU Data Protection Directive, are:

a. Application

The GDPR applies to any company (regardless of their location, size, and sector) processing the personal data of people residing in the EU.

For example, a US-based company processing the personal data within the United States of EU citizens is required to comply.

b. Responsibility

Under the GDPR, both the data controller and the data processor must comply with the legislation. Under the previous/current Data Protection Directive, only data controllers were held liable for data protection compliance, not data processors.

c. Penalties

With a maximum fine of up to 4 percent of annual global turnover or €20 million (whichever is greater), penalties for non-compliance are steep.

d. Consent

Under the GDPR, companies will no longer be able to use long, illegible terms and conditions full of legalese; consent for collection and use of personal data must be in plain language and detail the purpose of data processing.

e. Data breaches

Increased regulation surrounding the disclosure of **data breaches** ; specifically, much quicker reporting is required (within 72 hours).

f. Data Subjects' Rights

EU data subjects have expanded rights when it comes to data protection, including:

- the **right to be forgotten** (have their data erased),
- the right to access (obtain information about exactly what data is being processed where and for what purpose),
- and the right to data portability (receive a copy of the personal data concerning them).

Citizens now also have the right to question and fight decisions that affect them that have been made on a purely algorithmic basis.

g. Privacy by design

Privacy by design is a legal requirement to consider data privacy on the onset of all projects and initiatives, not as an afterthought.

h. Data Protection Officer (DPO) Appointment

Controllers and processors whose core business is regular and systematic monitoring of data subjects on a large scale or who deal with special categories of data will be required to appoint a DPO. The DPO may be appointed from within, hired, or contracted, but (among other specific requirements) (s)he must be an expert on data protection law and practices.

6. Data protection: a quick view outside the EU

a. U.S.A.

→ Framework on data protection for data collected / held by the Federal government

→ But no general framework on data protection outside the Fed. gov

b. India

IT Act of 2000 + IT Rules 2011

→ Focus on **sensitive** personal information:

Passwords, financial information, health condition, sexual orientation, biometric information

→ No need to declare data processing activities to an authority

c. China

In China, data protection is not enacted in a single piece of legislation, except for laws of a broader scope: National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection.

Rather, China has sector based pieces of legislation, such as the Regulation on Personal Information Protection of Telecom and Internet Users (MIIT Regulation).

The Chinese state is developing initiatives such as the Social Credit System, which are based on a

mass surveillance systems, as opposed to the free control for an individual of his personal data.

d. Legislation for the protection of personal data in other countries

To have a synthetic view of data protection laws in other countries, visit this website by Thomson Reuters.

The end

Find references for this lesson, and other lessons, here.

This course is made by Clement Levallois.

Discover my other courses in data / tech for business: https://www.clementlevallois.net

Or get in touch via Twitter: @seinecle