GDPR and data protection globally

Clément Levallois

2017-11-01

Table of Contents

last modified: 2017-11-13

1. Personal data and privacy: why are the stakes so high?

Businesses must of course make sure they comply with the existing rules governing the protection of personal data, to avoid reputation damages and litigation.

But why is the protection of personal data such an important matter in the first place?

After all, don't we all give up routinely much of our personal data to companies like Google or Facebook, without consequences?

We discuss the notions of personal data and privacy in this separate document.

2. 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: they were not translated into legislation in the US (source), but were translated into a Directive in the EU.

(full text of the Directive, presentation of the Directive on Wikipedia)

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?

→ 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. In the US:

- There is a regulatory framework on data protection for data collected / 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. 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 Facebook complied with the Safe Harbor Act. The lawsuit went to the European Court of Justice which ended up declaring invalid the Safe Harbor Act because:

"legislation permitting the public authorities to have access on a generalised 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. It differs from the Safe Harbor Act in the following:

(source for the following bullet points)

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 generalised access

3. Effective protection of EU citizens' rights with several redress possibilities

4. An annual joint review mechanism between the EU and the US

3. Key definitions

(source: Dataiku's white paper on GDPR)

a. Personal data

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

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 human being on whom personal data is being collected.

d. Data controller (DC)

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)

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

Until 2017, it is 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 breach of data privacy.

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

a. Prior consent

It 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 Scherms 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", detailed in this factsheet by the EU.

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 is enforced on **May 25, 2018**.

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

(source: Dataiku's white paper on GDPR)

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 GDPR, both data controllers **and processors** 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 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 will 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

It will be 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: USA, India, China

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

Data protection not enacted in a single piece of legislation.

Except for general laws: National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection.

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

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: http://www.clementlevallois.net

Or get in touch via Twitter: @seinecle