A Practical Look into GDPR for IT

Part 1

Abstract

This is the first article in a short series about the new EU General Data Protection Regulation (GDPR) looking, from the personal perspective of the author, into ways in which the IT systems and services can satisfy it or to help companies in satisfying it. This article is mostly concerned with the requirement of "data protection by design and by default" (Article 25) and how companies' IT can satisfy it.

In this and a few following articles, we will consider some issues related to IT and in particular IT Security, which impact or are impacted by the new EU Regulation on Data Protection, or in everyday parlance, the new EU Regulation on "Privacy".

There are many aspects related to this new Regulation which range from issues of organization within a company, governance, responsibilities, processes etc. Compliance to the Regulation requires that many different processes, technologies and employees' roles are modified or introduced in every company. In these articles we will consider only aspects related to IT, avoiding as far as possible other non IT related considerations.

It should also be noted that at the time of writing these articles, not too many detailed guidelines and interpretations of the Regulation have appeared. This implies that on some specific points it is not yet possible to be exactly sure of which are the correct approaches compliant with the Regulation.

GDPR is here

On April 14th, 2016 the European Union issued the General Data Protection Regulation ("GDPR" [1]) which will come in full adoption on May 25th, 2018. The main purpose of this Regulation is to provide the EU citizens with better protection to their personal data. The Regulation clearly defines the rights of the individuals and the obligations of the entities that are processing or are responsible

for the processing of the data of individuals. The GDPR supersedes the EU Directive 95/46/EC [2]. GDPR is a Regulation, which means that it applies directly as law in all EU countries, whereas the previous Directive defined the goals which should have been achieved, but each individual EU country should have created its own laws to reach them [3]. Still the Regulation leaves some points to be implemented by existing or new laws of each country, by giving only the principles to which each local law should adhere.

A very important point is that with the GDPR, all EU countries will have the same data protection ("Privacy") law which on one side will guarantee that all EU citizens will receive the same protection to their own information when managed by companies and entities, and on the other side, that all companies offering services to EU citizens will have to implement and guarantee the same protections to the data, creating a fair marketplace both among the companies and to the citizens.

But the important point is that, as the time of writing this article, the GDPR is already a valid law in all EU countries, and that, simplifying a bit for the sake of the argument, only from May 25th, 2018 fines and penalties will be imposed to those found not compliant. The legislator has indicated which are the scales of the fines and penalties for non compliance, and they are huge. Depending on the type of non compliance, the fines can be up to:

- € 20 millions or 4 percent of total worldwide annual turnover (whichever is the greatest).

This is not little money for any company, and it just means one thing: <u>we are already late</u>.

A new approach to be compliant

The GDPR introduces quite a few new concepts and requirements. In this and the following articles we will consider a few of them among those which have the largest impact. Our selection of subjects is quite personal and we do not give any guarantee to cover all aspects needed to develop a comprehensive approach to the compliance for the Regulation.

The issue from which we start is by now quite well known and discussed. The GDPR, following a similar approach to other recent regulations, standards etc., adopts the concept of

Data protection by design and by default (Article 25).

This is a very short phrase, but it has a lot of consequences. First of all, it is related to the following similar statement

IT Security by design and by default

It should be obvious that the two statements cover different aspects even if they have an obvious overlap. First of all, the GDPR is concerned with the overall managing of personal data, both within IT systems and by company personnel in general. Data protection can be achieved only if there are

processes in the company which define how data is to be managed and responsibilities for those who have to manage it. Part, even a great part, of the data management is done by IT systems and services which have to provide functionalities to implement the requested processes.

Limiting ourselves only to IT systems and services, we need to understand how it is possible to guarantee that data protection is implemented "by design and by default."

Designing Data Protection By Default

The GDPR is one of the few legislations and standards that requires explicitly to implement security measures in the development cycles of IT systems and services. Indeed companies will need to demonstrate that the IT systems and services they have developed or acquired have been designed so to implement the company's data protection policies. To achieve this companies need to implement a few things.

First of all, companies should have policies, standards and/or guidelines which:

- identify the GDPR data
- classify the GDPR data relatively to the risks due to their processing and storing in the IT systems and services
- define the protection requirements needed for the different types of GDPR data
- map the protection requirements to the classes of IT systems and services, for example IT systems and services open to public access or with restricted access, accessible on Internet or only on a private network etc.

Then, there should be procedures on how IT systems and services should be designed, both if developed or acquired, new or modified. In particular, when designing a new IT system or service, or designing some modifications to an existing one, it should be clearly documented which GDPR data are processed and stored by the system or service.

It could be very valuable to have a **Map of GDPR Data** as one of the documents, or a section of the technical document, describing the IT system or service. This Map should be included among the documents describing the IT system or service when deployed in production, and before that, it should be formalized at least also at the User Acceptance Tests (UAT). This Map should be updated for each deploy in production of new versions of the IT system or service.

The Map of the GDPR Data just tells us which GDPR data is processed and stored by each IT system or service, and it is only the first step in designing data protection by default. With the Map one only knows which data has to be protected, one does not know how to protect it.

The company's classification of the GDPR data and the associated protection requirements should then be translated by the IT architects designing the IT system or service in technical protection features. And these features should be implemented in the IT system or service by the developers. The GDPR requires that the IT architects document how the protection requirements are satisfied by the security features designed in the IT system or service. So a dedicated document or a section of the technical design documentation should describe which security features satisfy the protection requirements for all data identified in the Map of GDPR data.

But a last step is needed: companies need to demonstrate that the designed security measures are correctly implemented. To do that, Article 32.1.d requires that it is implemented "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." Thus companies need to implement and document tests on the IT systems and services explicitly to show that the security features satisfying the GDPR data protection requirements are implemented and that they work as expected.

Summarizing, to implement data protection by design and by default, companies need to have default processes for designing security features in each and all IT systems and services, described in policies, standards and/or guidelines which contain, for the "by default" requirement:

- how to identify and classify GDPR data
- which are the protection requirements for GDPR data
- which are the GDPR activities in the standard process to develop an IT system or service

and for the "by design" requirement, for each IT system or service:

- the Map of GDPR data processed or stored
- the documented IT security measured designed to satisfy the data protection requirements
- the documented IT security tests which prove the implementation and effectiveness of the security measures.

Security of Processing (Article 32)

Besides the general notion of "Data Protection by Design and by Default", the GDPR has many other explicit and implicit requirements on security, and in particular IT security, for the protection of data. The first requirements which must be addressed are listed in Article 32 about Security of Processing. As it has already been discussed, the GDPR requires to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk", but more detailed requirements are described together with some indications of approaches and technologies

which can be adopted to implement the needed security measures.

IT systems and services which process and store GDPR data, must ensure in a continuous, "ongoing" way, their:

- confidentiality
- integrity
- availability
- resilience.

Confidentiality, integrity and availability are the main characteristics of IT security, to which the GDPR adds resilience, which can be described as the elasticity to sustain and recover quickly from incidents. Indeed the GDPR correctly gives for granted that incidents will happen and that the three characteristics of IT security will be violated. So it is necessary to recover as fast and smoothly as possible from incidents as requested explicitly by Article 32.1.c.

Resilience and recovery require not only that IT systems and services are designed and developed with the needed security features, as discussed in the previous section, but also that companies implement both technical and organisational procedures to manage incidents in particular with respect to the recovery from them.

So even if not explicitly mentioned, a dedicated approach to IT (security) **Incident Management** is needed to be really compliant to the GDPR.[1]

Article 32 and other articles of the GDPR require that IT systems and services ensure the following properties for the GDPR data that they process and store:

- authenticity
- integrity
- confidentiality
- availability
- freshness and correctness.

If integrity, confidentiality and availability can be dealt within IT systems and services mostly with technical security features, authenticity requires that the processes of acquisition and maintenance of the data are designed and implemented so to identify and monitor who is processing the data and

1 Incident management will be obviously relevant when Data Breaches will be considered in one of the following articles in this series.

for whom the processing is done. Indeed the data can be processed directly by the user/citizen to whom it belongs for example by means of a public web application, or it can be processed by a company employee who collects the citizen data by other means and processes them in the company's IT systems and services.

This also requires that IT systems and services produce logs of accesses to themselves and if needed, to the data itself, by their users. These logs must also be collected, securely stored and reviewed to verify that only authorized users have access to all GDPR data.

Identification, authentication and authorization of the users of the IT systems and services are crucial to ensure the correctness of the processes which manage the GDPR data.

Finally the freshness and correctness of the GDPR data depends mostly on the processes of acquisition and maintenance adopted and implemented by the company and supported by the IT systems and services.

But the GDPR mentions, as suggestion, also some technical security measures that can be implemented to protect the data, like:

- Data minimisation (4 references)
- Pseudonymisation (12 references)
- Encryption (4 references).

It si important to keep in mind that "encrypting" some GDPR data "somewhere" does not ensure compliance with the GDPR. The GDPR is quite explicit, and repeats many times,[2] that the security measures implemented must assure an appropriate level of security to the processing and storing of GDPR data: it is a risk-based approach, there are no technical measures which are mandated.

A note is due on the meaning of Pseudonymisation. Pseudonymisation is a weaker form of anonymisation, with which real data is substituted with a pseudonym but that allows re-identification, that is it is possible to track it back (even with some effort) to the original data.

In all, the following differences should be noted:

- Data minimisation reduces the presence of GDPR data to the IT systems and services where it is absolutely needed, but the data remains in clear
- Pseudonymisation makes the data per se not directly referring to the citizen, but with some extra information, even of public knowledge, allows to reconstruct the full information

2 The GDPR's Data Protection Impact Assessment will be discussed in one of the following articles.

- Encryption makes the data available only to those who possess the secret key which allows to decrypt it.

Technically other security measures exist, like for example tokenisation, which can be implemented to protect GDPR data. The GDPR does not require any of them, but suggests to adopt the ones which best fit the security and the protection of the data.

More considerations on the IT technical security measures which can be adopted to achieve GDPR Data Protection and the compliance to the legislation, will be discussed in the following articles.

References

[1] European Union, "General Data Protection Regulation 2016/679", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[2] European Union, "European Data Protection Directive 95/46/EC ", http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

[3] European Union, "Regulations, Directives and other acts", https://europa.eu/european-union/eu-law/legal-acts_en

[4] Article 29 Data Protection Working Group, "Guidelines on the right to data portability", http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Andrea Pasquinucci (PhD CISA CISSP)