A Practical Look into GDPR for IT

Part 2

Abstract

This is the second article in a short series about the new EU General Data Protection Regulation (GDPR) [1]. This article is mostly concerned with a discussion of the risk approach adopted by the GDPR called Data Protection Impact Analysis (DPIA) and with some generic and overall security measures that can be implemented to mitigate some common risks.

The main subject of the first article of this short series has been the interpretation from the point of view of a company's IT department of the GDPR requirement of "Data Protection by Design and by Default." In the first article there has also been a discussion of the consequences for a company's IT department of the requirement of "Security of Processing." But before entering in more practical and technical IT issues, it is necessary to consider one of the main cornerstones of the GDPR, that is its risk-based approach to data protection.

GDPR, Risks and data protection

The GDPR does not require any particular security measure to be always implemented, neither for the manual processing of the citizens' personal data nor for the IT security measures to be adopted. This is already a notable difference with respect to previous approaches to the management of Privacy data. For example, in Italy the previous Privacy law did mandate some minimal technical IT security measures to be applied always when managing Privacy data. More technical IT security measures, as for example strict retention time or particular encryption, were requested when managing special data, like data related to health or religion, politics etc.

The GDPR instead does not mandate any particular IT security measure but in practice requires that every company performs **Risk Assessments** on the citizens' personal data that it manages and that, based on the outcomes of the Risk Assessments, implements mitigating security measures to reduce these risks.

But which risks have to be considered?

GDPR Article 35 and Recital 84, and the WP29 in [2] state that should be assessed:

the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

This is an extremely important point to keep always in mind: the focus of GDPR's risk analysis is not the company business, the services, processes or IT systems, but it is the citizens' personal data that the company manages. We are used to consider risks to the company business, instead the GDPR asks us to evaluate the risk of third parties, typically the company's customers and the company's employees. Obviously the company business is strongly related to these third parties, but there can be cases in which the company business can have opposite needs with respect to these parties. Obvious and well known examples of this are:

- the case of marketing and advertisement in which there is a well known tension between the company need of information about its customers and the privacy of the customers who would like to divulge as little as possible information about themselves;
- some type of monitoring[1] of the employees' activities which can help very much companies to improve the efficiency of their internal processes, against the employees who would prefer in case to be judged on their overall performance and contribution to the company business.

This approach is very different from what we have been used to, and it is usually adopted by many standards, among which it is enough just to mention ISO/IEC-27001 as an example.

It is to be noted that non-compliance with performing the risk analysis, or performing it in an incorrect way (!), or not consulting with the national Privacy supervisory authority when required (or in doubt), can lead to the substantial administrative fines indicated in the GDPR [2].

The Data Protection Impact Analysis (DPIA)

But how should a company proceed to perform risks analysis compliant with the GDPR?

Here actually things get complicated. The GDRP states that a company is required to perform a Data Protection Impact Analysis (DPIA), also called Privacy Impact Analysis (PIA) only when the processing is

likely to result in a high risk to the rights and freedoms of natural persons

(Article 35(1)). This looks like a chicken-and-egg problem: it is requested to perform an Impact

1 In some countries it is totally illegal to monitor the activities of an employee at work.

Analysis when there are high risks, but how can it be known if there are high risk without first performing the analysis?

The WP29 has published a guideline [2] to help with this point. In this guideline the WP29 indicates 10 cases in which it is most likely that the DPIA is required, and it also states:

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law.

The WP29 also states that:

a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This might mean where similar technology is used to collect the same sort of data for the same purposes.

Other important GDPR's requirements concerning the DPIA are:

- the DPIA must be carried out "prior to the processing" (Articles 35(1) and 35(10), Recitals 90 and 93), and this is consistent with the "data protection by design and by default" principles (Article 25 and Recital 78)
- the DPIA is requested for all (high risk) processing operations of personal data initiated or that change significantly after the GDPR becomes applicable on 25 May 2018, but the WP29 strongly recommends to carry out DPIAs for processing operations already underway prior to May 2018
- the DPIA must be reviewed when there is a change of the risks presented by the processing operation (Article 35(11)).

And finally, how should be a DPIA performed?

The GDPR does not mandated any methodology or standard to perform the DPIA. In [2] are indicated some required components of the DPIA and standards like ISO/IEC 31000 or the guidelines to appear in ISO/IEC 29134 [3] (see Annex 1 of [2]) which can help in performing the DPIA.

DPIA and IT projects

Since the GDPR does not mandate neither the approach nor a methodology to perform the DPIA and Risk Assessments, there can be different ways to implement the required risk-based processes.

One possible way is to consider the DPIA as the outcome of a business process which leads to the definition of the business requirements for an IT project. In this case, when an IT project starts, the business will provide the IT with the DPIA on the data which will be managed by the project.

As mentioned in the previous section, the GDPR does not require to perform a DPIA for every project. The DPIA is information based, so once it is done it can be applied to multiple projects as far as the treatment of the data is evaluated. In case a project requires new data or new treatment of existing data, the DPIA should be updated.

Referring to what has been described in the previous article, with this approach the DPIA would be a business input document to the IT "Designing Data Protection by Default" and should provide from the business point of view:

- the identification of the GDPR data
- the classification the GDPR data relatively to the risks due to their processing and storing in the IT systems and services
- the definition of the business protection requirements needed for the different types of GDPR data.

In any case, the DPIA should be a required document in any IT project which manages personal data.

Moreover, it is from the DPIA that an IT project is able to design the security measures to protect the personal data, and to manage and mitigate the risks ascertained.

But what about residual risks after the design and implementation of the IT security measures? This is actually a quite common situation since it often happens that the technical security measures do not manage to completely mitigate all the risks. In some cases the security measures do exist, but they will prevent or make it very difficult to access and to manage the personal data so that it is necessary to adopt only part of them and to strike a balance between security and usability.

If there are residual risks and in the case when these are still high from the point of view of the DPIA, it is then necessary to consult with the national Privacy Supervisory Authority. Otherwise the risks should be accepted by the business.

From risks to IT security measures

Having understood that data protection security measures should be implemented according to a risk-based approach and with the purpose of mitigate the ascertained risks, it follows that it is not possible to give some general security guidelines valid in all situations and for all IT projects, services and systems. Anyway it is still possible to consider as examples some IT security measures that in most cases can be adopted.

It is useful to start from a very simple concept, which is a trivial consequence for the IT services and systems of the GDPR requirements:

access to GDPR data must be authenticated and authorised.

This follows from the basic GDPR requirement that only authorised personnel can process GDPR data, see for example Articles 28 and 30.

Authentication and authorization, despite being standard IT security measures, are by large not trivial to implement. In principle, to be sure to satisfy a priori some GDPR requirements, the IT services and systems should provide

authentication and authorisation to the single GDPR data.

Instead usually authentication and authorization are provided for the full IT service or system, and in some cases just for the entire company's IT. Implementing such a fine grained access control can be not trivial at all.

A case study

To understand in a little more detail which could be the GDPR's requirements to an IT service, we consider the case of a generic IT service which manages also some GDPR data. This IT service is provided by an application built with the standard 3-layers: the application users' front-end, the application server (middle-ware), and the back-end, typically a database. This application can exchange data, including GDPR data, with other applications.

Who can in principle access the GDPR data? The list can be rather long but for our purposes we limit it to the following:

- the users of the application
- the administrators of the application
- the database administrators
- the operating system administrators

- the network administrators
- the backup administrators.

Recalling that one of the principles of GDPR is 'data minimisation' and the security concept of "Least Privilege", that is to build a system so that each user has the minimum privileges needed to perform her work, one can devise and implement the following generic security measures:[2]

- encrypt all communications between applications, instances, processes at the application level;[3]
- encrypt all filesystems and storage used to store application data;
- encrypt all storage used by databases (this feature is usually called Transparent Data Encryption, TDE) including backups.

By doing this we obtain that backup administrators, network administrators and operating system administrators do not have any more access to any application data, including GDPR data. Besides having increased the security level of all the IT infrastructure, there is no need to worry about this personnel and the GDPR. By introducing this kind of encryption we have minimised the exposure of the GDPR data by reducing the access privileges of a rather large class of user (administrators).

Obviously the application users, application administrators and database administrators have access to the GDPR data, but they need to have this access to perform their job.

Do we still really need to implement for these users the authentication and authorisation at the GDPR data level?

The answer to this question obviously lies in the DPIA and the outcomes of the risk assessments, but, if possible, there is a mitigating security measure that, in some cases, can be implemented instead of such a granular access control: monitoring, tracing and logging.

Broadly there are three approaches to tracing and logging: the first one is coarse and lightweight and consists in tracing and logging the access, login and logout, to the application, operating systems, databases etc. of users, application administrators and database administrators. By knowing who is connected to the service at a particular time, it is possible to get the list of people that could have accessed the GDPR data at that time. This can be implemented typically without too much effort.

It is possible to improve on this basic tracing, by having the application or directly the database

---

2 In this respect, Google's approach to the internal security of its IT services described in [4] can be of interest.

3 Communication encryption can also be implemented host-to-host or gateway-to-gateway at the network level, here we consider only the simplest case of application-to-application communication encryption.

recording the user who has created, modified or deleted data, in particular GDPR data. In this way it is possible to know exactly who has acted on GDPR data, but not who has seen it or copy it. This approach can be more complex to implement, can require to modify the applications so to be aware also in the back-end of the front-end users acting on the data, and the dimensions of the logs can start to be meaningful.

Finally, the previous approach can be further improved by recording also all read accesses to some particular data, in particular GDPR data. This implements a full tracing of all possible accesses to the data, but besides producing quite large amounts of logs, it can also have big impacts on the performances of services and applications.

Having discussed access and monitoring of accesses to GDPR data, one should not forget the GDPR's requirements of resilience and availability. In most cases these can be satisfied with standard IT measures like high-availability, backups, business continuity and disaster recovery services, depending on the requirements from the risks analysis and the DPIA.

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] Article 29 Data Protection Working Group, “Guidelines on Data Protection Impact Assessment (DPIA)”, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[3] ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO) - https://www.iso.org/standard/62289.html

[4] Google, “Google Infrastructure Security Design Overview”, February 24, 2017, https://cloud.google.com/security/security-design/

Andrea Pasquinucci (PhD CISA CISSP)