2.3 How to face security and privacy challenges

This module focuses on the General Data Protection Regulation and its associated rights and obligations, for institutions and individuals alike.

Complying with the GDPR

The General Data Protection Regulation (GDPR) is meant to provide a standardized, privacy-conscious and secure way through which **personal data** is processed. Although it is a European regulation, and therefore should have effects only on the soil of the Member States of the European Union, the GDPR protects the personal data and the rights of data subjects as long as they are EU citizens, no matter where they are living. Article 3 of the Regulation specifies that any data processing that has effects on EU citizens must comply with GDPR rules, even if it takes place outside of the EU borders. This is meant to provide a broad protection to EU citizens' rights anywhere on the globe. A natural person whose personal data is being processed is called a **data subject**.

But what exactly is "personal data"? Personal data are any information which are related to an identified or identifiable natural person. The data subjects are identifiable if they can be directly or indirectly identified through the processed information. Examples could be the name, an ID number, their home address, or certain characteristics of their being, such as those that may express a physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. Even the number plate of a car, or the IP address of a device, could be considered personal data, as they potentially allow the identification of a person.

Since the definition includes "any information," one must assume that the term "personal data" should be as broadly interpreted as possible.

The GDPR, however, has no effect on data which is not personal. Everything you will read throughout this document therefore does not apply to the processing of non-personal data.

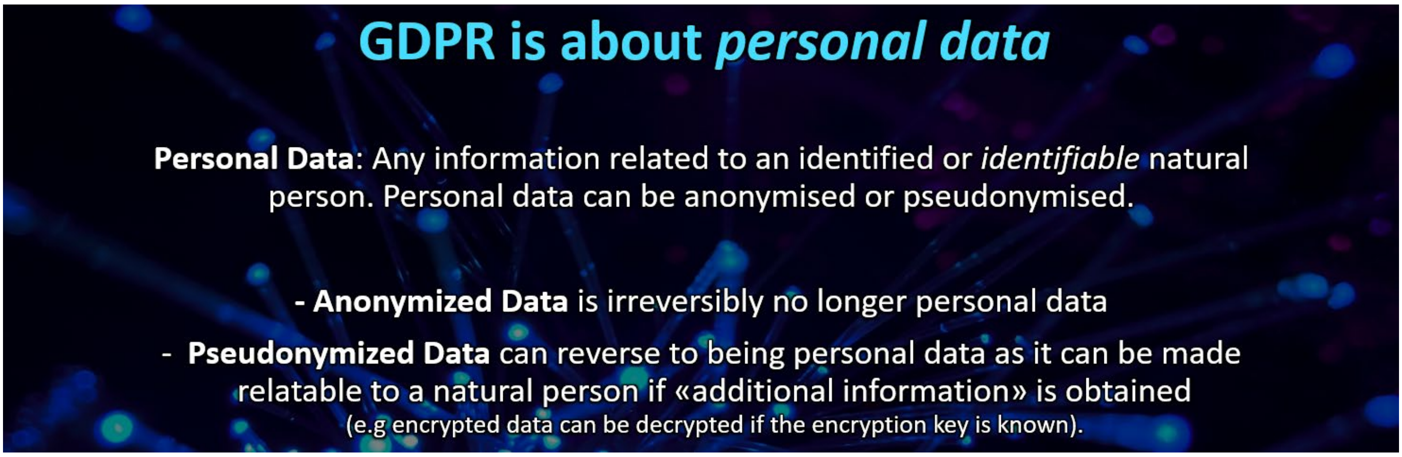
Personal data can become non-personal data through a process called **anonymisation.** The GDPR itself offers a definition of anonymisation: "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". There are no specific ways to anonymise data; rather, it's the end result that counts: the impossibility of relating an information to a natural person. A good summary of anonymised data, outside the scope of this module, can be found in a very well made document by UK's Information Commissioner's Office[1].

[1] ICO, *Anonymisation: managing data protection risk code of practice,* retrieved in September 2021, https://ico.org.uk/media/1061/anonymisation-code.pdf

Co-funded by the
Erasmus+ Programme
of the European Union

Often, data which is thought anonymised is not really anonymised, but rather **pseudonymised**. This term is also defined by the GDPR: "[pseudonymisation consists in] the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information". In this case, data is relatable to a natural person, but only if at least another information is obtained. In other words, while anonymising data makes it impossible, forever, to relate that information to a natural person, pseudo-anonymising it makes it *temporarily impossible* to do so. Anonymisation is definitive, while pseudo-anonymisation is reversable, provided that other information is obtained.

We can therefore say that GDPR is, first and foremost, about *personal data*.



GDPR is about *personal data*

Personal Data: Any information related to an identified or *identifiable* natural person. Personal data can be anonymised or pseudonymised.

- **Anonymized Data** is irreversibly no longer personal data
- **Pseudonymized Data** can reverse to being personal data as it can be made relatable to a natural person if «additional information» is obtained (e.g encrypted data can be decrypted if the encryption key is known).

While processing personal data, the first and perhaps most important requirement that the GDPR establishes is that a **data controller must be identified.** The "data controller" is whoever is in charge of processing personal data, be it a physical person or a juridical construct. It needs to be pre-emptively identified so that data subjects may reach him to exercise their rights. Moreover, the data controller must define which kind of data are processed and used and for what end. It is also held accountable for every violation in these procedures. It is mandatory for the data controller to maintain a record of data processing activities, under its responsibility.
The data controller may be helped by a data processor, i.e. someone who carries out processing on behalf of the data controller[2].

Any processing of data must have a **time limit**, according to article 5 of GDPR. In general, article 5 specifies ways that are meant to grant transparency and fairness to data subjects. So, a time limit must be set, and data must not be kept over that limit. Data must be kept safe and be stored in such a way that it is immediately available to the user if he or she desires to access it.

Perhaps the most important action that has to be undertaken when obtaining personal data from different subjects is the creation of a **Privacy Notice**, "a public document from an organization that explains how that organization processes personal data and how it applies data protection principles"[3]. This document must be written in a plain,

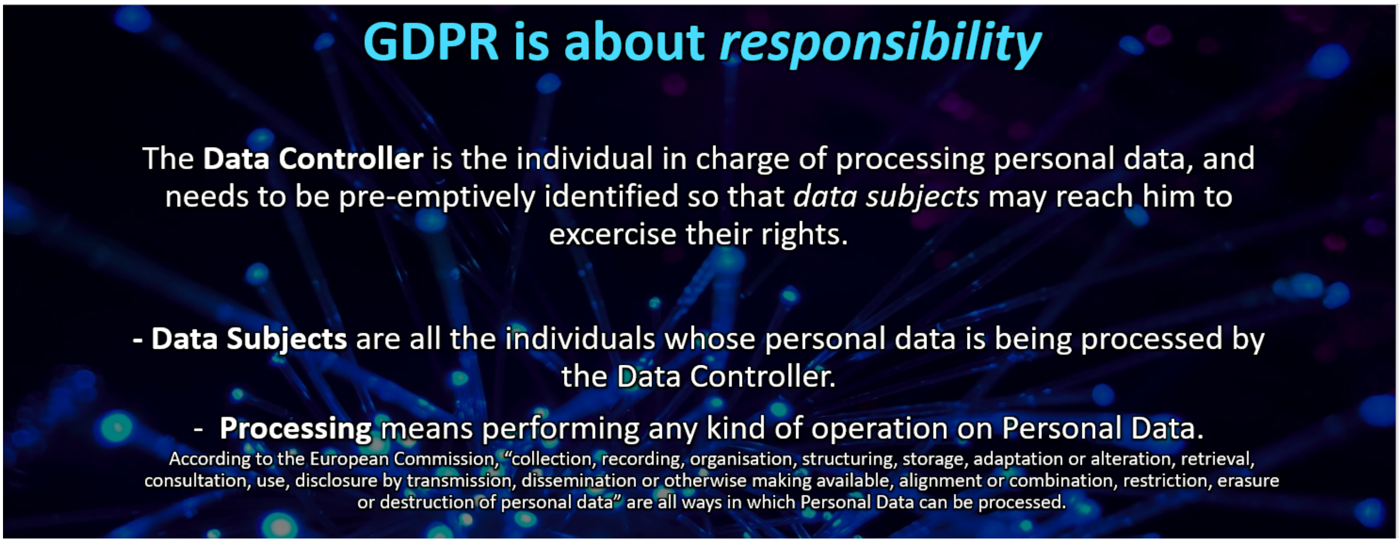
[2] For more information on the data processor, please see article 28 GDPR: https://gdpr-info.eu/art-28-gdpr/
[3] From https://gdpr.eu/privacy-notice/

transparent and intelligible way, so that every data subject can easily understand how their personal data will be processed.

The Privacy Notice must first and foremost list the identity and contact details of the organization, and its Data Controller. Sometimes, a different subject may be identified: the **Data Protection Officer**. Having a Data Protection Officer (DPO) is not mandatory. It is, however, if AI instruments are used. The DPO is therefore a person that assumes responsibility of protecting the processed data and is able to interact with the public to assist in privacy-related problems and questions.
Having a Data Protection Officer is also mandatory if an institution's core activity consists in processing sensitive data on a large scale or is involved in regular, systematic and large-scale monitoring of individuals. In that respect, monitoring the behaviour of individuals includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising[4].

The difference between the Data Controller and the Data Protection Officer lies in the fact that the former can also be a juridical construct – and not a natural person – under whose responsibility the whole processing of personal data is conducted. On the contrary, the DPO does not have a specific responsibility in processing personal data correctly, but he should ensure that the organisation processes the personal data of data subjects in compliance with the applicable data protection rules.

So, many of GDPR's concerns regard the *attribution of responsibility*: the need to identify specific individuals that are responsible for the correct processing of personal data.



GDPR is about *responsibility*

The **Data Controller** is the individual in charge of processing personal data, and needs to be pre-emptively identified so that *data subjects* may reach him to excercise their rights.

- **Data Subjects** are all the individuals whose personal data is being processed by the Data Controller.

- **Processing** means performing any kind of operation on Personal Data.

According to the European Commission, "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data" are all ways in which Personal Data can be processed.

Following up on the identification of the Data Controller, and maybe the Data Protection Officer, the Privacy Notice has to **provide a purpose** for the organization to process an individual's personal data: a reason why that personal

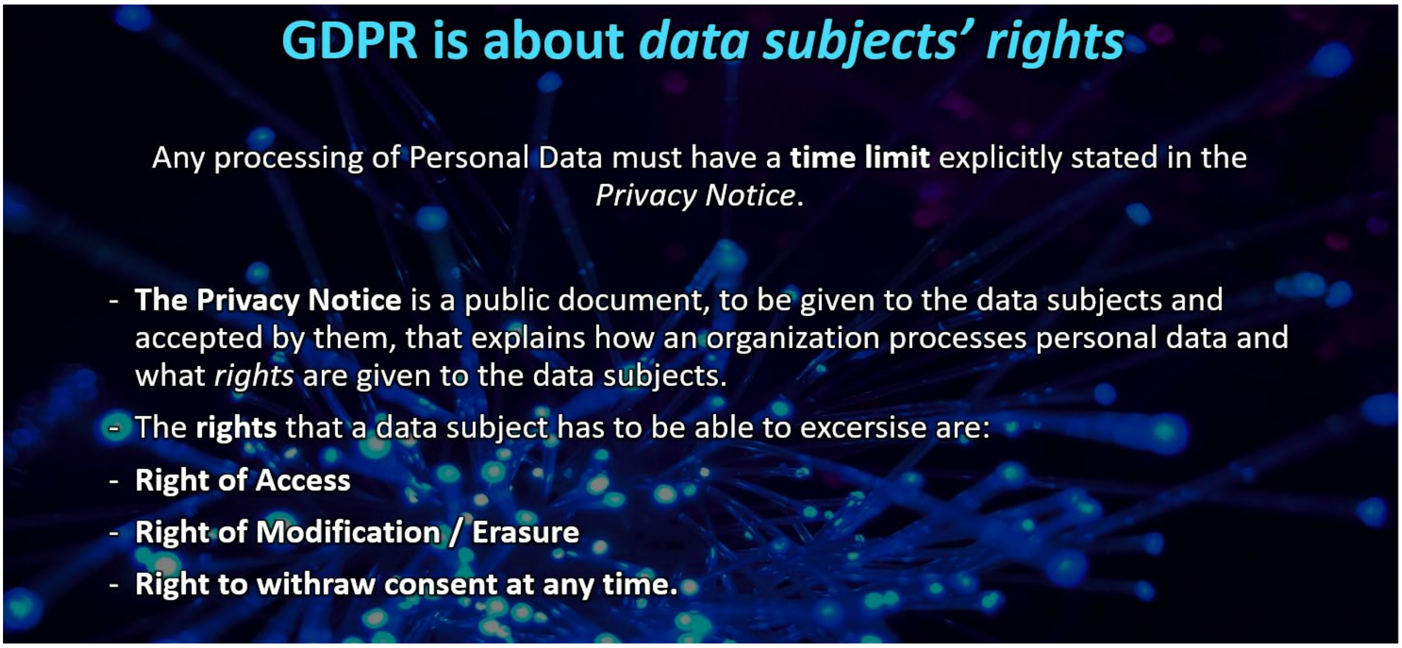
[4] European Commission, *Does my company/organisation need to have a Data Protection Officer (DPO)?*, retrieved September 2021, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_en

Co-funded by the
Erasmus+ Programme
of the European Union

data is needed. Then, it will also have to provide a timing for the processing of data, as no processing can last forever, nor can data be stored forever: the processing of data and its storage must have strict time limits.

The GDPR allows the data subject to exercise a number of rights upon his or her data. These same rights must be explicitly reported in the Privacy Notice.
First, data subjects may require ***access*** to their personal data. If they do, they must be shown what personal data has been collected from them, when and for what purpose.
They may also require some form of ***modification*** of that same data, maybe because some information has changed or is no longer true, or maybe because the data was incorrect to begin with.
Data subjects have also the right to ***withdraw consent*** at any time, forcing the Data Controller to erase all of their processed personal data.
This is extremely important: it is of paramount importance that users are able to obtain access to their data, if they so desire. They must also be able to promptly request corrections or the elimination of certain information.

Therefore, the GDPR focuses heavily on data subjects and their rights.



GDPR is about *data subjects' rights*

Any processing of Personal Data must have a **time limit** explicitly stated in the *Privacy Notice*.

- **The Privacy Notice** is a public document, to be given to the data subjects and accepted by them, that explains how an organization processes personal data and what *rights* are given to the data subjects.
- The **rights** that a data subject has to be able to excersise are:
- **Right of Access**
- **Right of Modification / Erasure**
- **Right to withraw consent at any time.**

It is not uncommon for data to be processed incorrectly. The data subject has therefore also the right to **lodge a complaint** with a supervisory authority. Each Member State of the European Union has a National Authority to which the complaint must be addressed. Under the GDPR, the EU's data protection authorities can impose **fines** of up to €20 million, or 4 percent of worldwide turnover for the preceding financial year—whichever is higher. For example, in late 2020 France fined Amazon €35 million for failing to get cookie consent on the shop's website.

The recent surge in the **use of Artificial Intelligence** to analyse and process big quantities of data has been taken into account by the GDPR, although it entered into force in 2016, a time when AI use was not as widespread as it is today.

In general, the processing of data may produce effects on the data subjects that may "significantly affect"[5] them. It is unclear what the GDPR really means when quoting these "significant effects", so they are usually interpreted in the broadest way possible. For example, employees may be hired or fired because of information gained by automatically processing personal data.

In these cases, when "significant effects" arise, the data subject has the right not to be subject to a decision based solely on automated processing. In other words, a human being must always supervise the work of the algorithm: artificial intelligence is viewed as a mere tool that can never produce effects without human intervention.

Finally, the GDPR implicitly admits that there can be no privacy without security. For this reason, it introduces the concepts of **privacy by design** and **security by design:** "the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" and, "shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". These formulae, found in articles 13, 25 and 32 are deliberately generic. There is no indication of a proper and specific way of processing data in a privacy-conscious or secure way *by design*, but, just like regarding anonymization of data, what counts is the end result.

In plain terms, the data controller must be able to demonstrate that privacy and data protection issues are taken into account in the design phase of any system, service, product or process. The data controller must therefore set up a way of processing and keeping personal data based on the current state of the art methodologies in privacy and security matters.

There is however a limit on how far data controllers have to go in order to be compliant to these rules: it would be unreasonable to require every institution to process and keep data in the most secure and costliest way possible. The amount of effort that a data controller must go through is therefore proportionate to "the risk faced by the personal data that is being processed". A small dentists' studio, for instance, won't be required to keep personal data in the same way that a large hospital does.

The Data Controller should therefore assess the risks his data processing faces and implement measures that are enough to reasonably ensure that it is processed in a GDPR-compliant way.

If a data breach happens, there must be procedures that oblige the Data Controller to notify the personal data breach to the relevant supervisory authority no later than 72 hours after the breach.

The Privacy Notice

As it was shown in the previous paragraph, an important requirement when processing personal data is to submit a Privacy Notice (PN) to the data subject. The Privacy Notice is a document that must be drafted by the data controller and explains how and why personal data is processed, for how long and in which way the data subjects can exercise their rights. It is important that the PN is written in an easy-to-understand manner, and must be presented to the data subjects before their data gets processed[6].

It is possible to divide the Privacy Notices' requirements into two: stylistic requirements and content requirements. Regarding the **stylistic requirements**, the PN must be:

[5] As per article 22 GDPR.

[6] Articles 12 and 13 GDPR

Co-funded by the
Erasmus+ Programme
of the European Union

- Written in a concise, transparent, intelligible, and easily accessible form
- Written in clear and plain language, particularly for any information addressed specifically to a child
- Delivered in a timely manner, before the processing happens
- Provided free of charge

Regarding the **content requirements**, the PN must include the following information:

- The identity and contact details of the organization, its Data Controller and its Data Protection Officer, when present.
- The purpose of the processing: why is that data needed, and what is the legal basis for the processing and, if applicable, the legitimate interests pursued by the controller or by third parties?
- The recipients or categories of recipients of the personal data, if any.
- The details regarding any transfer of personal data to a third country, if that could happen, and the safeguards taken.
- A specification of the period during which the data collected is retained. This time period must be specifically limited and cannot be forever.
- The existence of each data subject's rights: access, rectification, portability, erasure. Also, the right to revoke consent at any time[7].
- The right to lodge a complaint with a supervisory authority.
- The existence of an automated decision-making system, including profiling, and information about how this system has been set up. In any case, this automated decision-making system cannot by itself produce effects on the data subject, but it needs a human being to eventually confirm its decisions.

Moreover, if personal data is acquired from the data subject, the data controller must provide information about whether the provision of personal data is a legal or contractual obligation or a necessary requirement for the conclusion of a contract, and whether the data subject is under an obligation to provide personal data, as well as the possible consequences of failure to provide such data.
Instead, if personal data is not acquired from the data subject, the data controller must provide information about the categories of personal data concerned and the source from which the personal data originate and, where applicable, whether the data come from publicly accessible sources.
If cookies are used, then the data subject must be informed about their presence, whether they are necessary to provide services or not, and if not how to avoid them (for example by setting up their browser in such a way as to automatically refuse them), the purposes of the cookies and the period of their storage.

[7] Right of access: the Data Subjects must be able to access their data as soon as possible after submitting a request.
Right of rectification: the Data Subjects must be able to ask for their data to be modified.
Right of portability: the Data Subjects must be able to make copies of their processed data.
Right of erasure: the Data Subjects must be able to revoke their consent at any time and to force the erasure of their data from the organization's database.

Co-funded by the
Erasmus+ Programme
of the European Union

The GDPR.eu webpage offers some suggestions on how to build an effective Privacy Notice by simply formulating precise and complete answers to certain questions[8], therefore dividing the PN into as many paragraphs as these same questions:

- What data is collected?
- How does this organization collect personal data?
- For what purpose will that data be used?
- How will that data be stored?
- Are there third parties who will receive that data? If so, who are they, and why do they receive it?
- What are the data protection rights offered to the user? (access, rectification, portability, erasure).
- What are cookies?
- How are cookies used in this webpage/service?
- What types of cookies are used?
- How to manage cookies?
- How and when do changes to this privacy policy occur?[9]
- How to contact the organization?
- How to contact the appropriate authorities?
- Is an automated decision-making system, including profiling been implemented? If yes, how this system has been set up?
- If personal data is acquired from the data subject, is the provision of personal data a legal or contractual obligation or a necessary requirement for the conclusion of a contract? Is the data subject is under an obligation to provide personal data? What are the possible consequences of failure to provide such data?
- If personal data is not acquired from the data subject, what categories of personal data are processed? from which source the personal data originate? Does the data come from publicly accessible sources?

[8] See https://gdpr.eu/privacy-notice/

[9] Data controllers are invited to keep their privacy policy under regular review and make it so that any updates to it can be easily .

Co-funded by the
Erasmus+ Programme
of the European Union