# DATA PROTECTION AND PRIVACY
# University of Genoa

## Lesson 2: Privacy by design and Privacy by default

# Designated natural person

Section 2-o (art. 2-quaterdecies, Italian Privacy Code) Allocation of tasks and functions to designated entities

1. The controller or processor may provide under their own responsibility and within the framework of the respective organisation that specific tasks and functions relating to the processing of personal data be allocated to expressly designated natural persons acting under the controller's or processor's authority ("Referente privacy")

2. The controller or processor shall set out the most appropriate arrangements to authorise the persons acting under their authority to process personal data ("Incaricato/Autorizzato al trattamento")

# Process owner

The person responsible for the process and the contact person for all information relating to the flows

# Data Protection Officer (art. 37- 39 GDPR)

The person responsible for monitoring the compliance of the organization for which they work, giving advice and guidance relating to data protection obligations and acting as a contact point between data subjects and the relevant supervisory authority

# Actors

DPO

CONTROLLER

PROCESSOR

DESIGNATED ENTITY

PROCESS OWNER

REFERENTE PRIVACY

## Data Protection by Design (art. 25 n.1, GDPR)

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

## Data Protection by Default (art. 25 n.2, GDPR)

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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

Il titolare attua misure tecniche e organizzative per garantire che siano trattati solo i dati personali necessari per l'attività Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.  non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

The controller needs to configure the data processing by providing, before proceeding with the processing, the essential guarantees to protect the rights of the interested parties, taking into account the overall cost and the risks for the interested parties

A preventive analysis and application commitment is required on the part of the controller, which must take the form of a series of specific and demonstrable activities

The most important activity is the Risk analysis, which detects the negative impacts of the processing on the freedoms and rights of the interested parties

## What are the risks for freedoms and the rights of data subjects?

They may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects

## EDPB Guidelines n. 4/2019 on art. 25 GDPR - Data Protection by design and by default (adopted 20 Oct. 2020)

The controller shall implement appropriate technical and organisational measures which are designed to implement the data protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements and protect the rights and freedoms of data subjects. Both appropriate measures and necessary safeguards are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing

Technical and organizational measures and necessary safeguards can be understood in a broad sense as any method or means that a controller may employ in the processing. Being appropriate means that the measures and necessary safeguards should be suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness

A technical or organisational measure and safeguard can be anything from the use of advanced technical solutions to the basic training of personnel. Examples that may be suitable, depending on the context and risks associated with the processing in question, includes pseudonymization of personal data; storing personal data available in a structured, commonly machine readable format; enabling data subjects to intervene in the processing; providing information about the storage of personal data; having malware detection systems; training employees about basic “cyber hygiene”; establishing privacy and information security management systems, obligating processors contractually to implement specific data minimisation practices, etc.

Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences:

**First**, it means that Art. 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk6 . Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing

**Second**, controllers should be able to demonstrate that the principles have been maintained

The implemented measures and safeguards should achieve the desired effect in terms of data protection, and the controller should have documentation of the implemented technical and organizational measures. To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness.

A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective.

KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments.

Alternatively to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards

Article 25 (1) lists elements that the controller has to take into account when determining the measures of a specific processing operation. These elements all contribute to determine whether a measure is appropriate to effectively implement the principles. Thus, each of these elements is not a goal in and of themselves, but are factors to be considered together to reach the objective

The reference to "**state of the art**" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape

The controller may take the **cost of implementation** into account when choosing and applying appropriate technical and organisational measures and necessary safeguards that effectively implement the principles in order to protect the rights of data subjects.
The cost refers to resources in general, including time and human resources

Controllers must take into consideration the nature, scope, context and purpose of processing when determining needed measures.
The concept of **nature** can be understood as the inherent characteristics of the processing.
The **scope** refers to the size and range of the processing.
The **context** relates to the circumstances of the processing, which may influence the expectations of the data subject, while the purpose pertains to the aims of the processing

Data protection by design shall be implemented "**at the time of determination of the means for processing**"

The "means for processing" range from the general to the detailed design elements of the processing, including the architecture, procedures, protocols, layout and appearance

The "**time of determination of the means for processing**" refers to the period of time when the controller is deciding how the processing will be conducted and the manner in which the processing will occur and the mechanisms which will be used to conduct such processing. It's in the process of making such decisions that the controller must assess the appropriate measures and safeguards to effectively implement the principles and rights of data subjects into the processing, and take into account elements such as the state of the art, cost of implementation, nature, scope, context and purpose, and risks. This includes the time of procuring and implementing data processing software, hardware, and services

Once the processing has started, the controller has a **continued obligation to maintain DPbDD**, i.e. the continued effective implementation of the principles in order to protect the rights, staying up to date on the state of the art, reassessing the level of risk, etc. The nature, scope and context of processing operations, as well as the risk may change over the course of processing, which means that the controller must **re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards**

A “**default**”, as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program or device.
Such settings are also called “presets” or “factory presets”, especially for electronic devices

The term **“by default” when processing personal data**, refers to **making choices regarding configuration values or processing options that are set or prescribed in a processing system**, such as a software application, service or device, or a manual processing procedure that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility

If the controller uses third party software or off-the-shelf software, the controller should carry out a risk assessment of the product and make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off

The same considerations apply to organisational measures supporting processing operations. They should be designed to process, at the outset, only the **minimum amount of personal data necessary for the specific operations ("minimization")**. This should be particularly considered when allocating data access to staff with different roles and different access needs

**Dimensions of the data minimization obligation**

Article 25 (2) lists the dimensions of the data minimization obligation for default processing, by stating that the obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility

## “Amount of personal data collected”

Controllers should consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of integrity and confidentiality, data minimization and storage limitation when collecting large amounts of detailed personal data, and compare it to the reduction in risks when collecting smaller amounts and/or less detailed information about data subjects. In any case, the default setting shall not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data are unnecessary or if detailed data isn’t needed because less granular data is sufficient, then any surplus personal data shall not be collected.

The same default requirements apply to services independent of what platform or device in use, only the necessary personal data for the given purpose can be collected

## “The extent of their processing”

Processing operations performed on personal data shall be limited to what is necessary. Many processing operations may contribute to a processing purpose. Nevertheless, the fact that certain personal data is necessary to fulfill a purpose does not mean that all types of, and frequencies of, processing operations may be carried out on the data

## “The period of their storage” (1/2)

Personal data collected shall not be stored if it is not necessary for the purpose of the processing.
The controller shall limit the retention period to what is necessary for the purpose. If personal data is no longer necessary for the purpose of the processing, then it shall by default be deleted or anonymized. The length of the period of retention will therefore depend on the purpose of the processing in question. This obligation is directly related to the principle of storage limitation and shall be implemented by default, i.e. the controller should have systematic procedures for data deletion or anonymization embedded in the processing

## “The period of their storage” (2/2)

Anonymization of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of reidentification, are regularly assessed

## “Their accessibility” (1/5)

The controller should limit who has access and which types of access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations. Access controls should be observed for the whole data flow during the processing

## “Their accessibility” (2/5)

Personal data shall not be made accessible, without the individual’s intervention, to an indefinite number of natural persons. The controller shall by default limit accessibility and give the data subject the possibility to intervene before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons

## “Their accessibility” (3/5)

Making personal data available to an indefinite number of persons may result in even further dissemination of the data than initially intended. This is particularly relevant in the context of the Internet and search engines. This means that controllers should by default give data subjects an opportunity to intervene before personal data is made available on the open Internet. This is particularly important when it comes to children and vulnerable groups

## “Their accessibility” (4/5)

Depending on the legal grounds for processing, the opportunity to intervene could vary based on the context of the processing. For example, to ask for consent to make the personal data publicly accessible, or to have privacy settings so that data subjects themselves can control public access

## “Their accessibility” (5/5)

Even in the event that personal data is made available publicly with the permission and understanding of a data subject, it does not mean that any other controller with access to the personal data may freely process it themselves for their own purposes – they must have their own legal basis