Guidelines for Data Protection by Default

English translation - Only the Spanish version is deemed authentic

v. October 2020

EXECUTIVE SUMMARY

This guide develops in a practical way the application of data protection by default, or DPbD, in the processing of personal data according to the provisions of Article 25 of the GDPR and the guide published by the European Data Protection Board "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default".

DPbD measures relate to the rational application of the data minimisation principle, under the criteria of adequacy, relevance and need with regard to the purposes in the design of the different phases of processing, as provided for in Article 25.2.

This document identifies the strategies that must govern the application of DPbD, such as optimisation, configurability and restriction in the processing of personal data by default. Subsequently, the specific measures for the implementation of DPbD are detailed in relation to the amount of personal data collected, the extent of the processing, the storage period and the accessibility to the data. Finally, the documentation and audit requirements in relation to DPbD are included.

The recipients are the data controllers and data protection officers, in addition to those units or departments within the controlling entity that are in charge of the design, selection, development, deployment, and operation of applications and services. It is also addressed to those in the role of processors, or technology providers, to the extent that they provide products and services to controllers, and seek that these meet the requirements of DPbD established in the GDPR.

Keywords: GDPR, accountability, data protection by default, data protection by design, risk, data minimisation.

TABLE OF CONTENTS

I. PURPOSE AND RECIPIENTS

The purpose of this document is to provide a practical guide for the implementation of specific measures for data protection by default.

As provided for in the second paragraph of Article 25 of Regulation (EU) 2016/679, General Data Protection (hereinafter RGPD), it is the responsibility of the controller to implement the measures for data protection by default (hereinafter DPbD).

This guide is addressed to the Data Protection Officers and, specifically, to those units or departments within the controlling entity that are in charge of the design, selection, development, deployment and use of applications and services.

In the event that the controlling entity uses the services of third parties for the effective implementation of a processing operation, the data controller has the obligation, according to Article 28 of the GDPR, to "use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

In this regard, the data controller must bear in mind their obligation to apply data protection by design and by default when designating both the processors and the providers of products and solutions to be used for processing. On the other hand, Recital 78 of the GDPR urges the producers of products, services and applications, although not regarded as data controllers or processors, to consider the right to data protection when developing and designing such products, services and applications, and to ensure, with due attention to the state of the art, that data controllers and processors are able to fulfil their data protection obligations.

Therefore, this guide is also intended for processors, producers or technology providers who want their products or services to enable controllers to meet DPbD requirements set out in the GDPR.

Nevertheless, it is important to remember that the criterion for establishing responsibility in a processing operation is based on determining who specifies the purposes intended and the means used. Where the processor, or system/solution provider, includes in its products collateral processing of end-users' personal data (e.g. to "improve the service", "debug the system", "offer advertising", "monitor the use of licences", "maintain the solution", etc.), they could be assuming, in these cases, the status of data controller.

II. INTRODUCTION

Article 25 of the GDPR establishes that the principles, rights and obligations relating to data protection set out in said Regulation must be considered 'by design and by default'. In this regard, a proven application of data protection by default becomes one of the measures of accountability that allows to prove compliance with the obligations established in the regulation.

Although compliance with the requirements set out in the Regulation is mandatory regardless of the nature and size of the controlling entity, the GDPR is flexible when selecting the measures to guarantee this compliance, with the possibility of opting for different approaches and alternatives when implementing the DPbD dimension.

The “default” configuration of applications, products and services is common in the development and production of systems when determining their operation. The GDPR has established the controllers’ obligation to guarantee DPbD protection of the personal data being processed according to this “default” configuration.

Paragraph 2 of that Article states that:

> *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.*

The parameters of the different configuration options that define the implementation of the processing must be established by the controller. In some cases, depending on the nature of the processing, in the design developed by the data controller some of these configuration options may be made available to the user.

In turn, the document "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"[1] of the European Data Protection Board (hereinafter the EDPB Guidelines) states in paragraph 2. 2 "Data Protection by Default" that DPbD refers to the choices made regarding the configuration values or processing options set in the systems and procedures implementing the processing and determining the amount of personal data collected, the scope of its processing, the storage period and its accessibility.

The GDPR requires the data controller to set up a default configuration for processing that respects data protection principles, advocating minimally intrusive processing: minimum amount of personal data, minimum extent of processing, minimum storage period and minimum accessibility to personal data. All of this, furthermore, without the intervention of the data subject being necessary to guarantee that these minimums are established. Hence, DPbD is not limited to requirements regarding programmes or devices, but also affects the design of the processing itself, regardless of the means on which it is carried out.

Paragraph 47 of the same Guide states that security measures should always be included by default:

[1] Draft version published at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es

Information security shall always be a default for all systems, transfers, solutions and options when processing personal data.

This means that, although the risk of the processing to rights and freedoms is low[2], the controller cannot ignore the establishment of security measures. However, when choosing the specific security measures to be implemented, the process of selecting each one of them must be guided by an analysis of risks to the rights and freedoms of natural persons, as established in Article 32 of the GDPR.

It is not the intention of the GDPR to be exhaustive in the measures to be implemented simply because personal data is being processed. It includes the concept of DPbD, to cover all those measures and guarantees of "default configuration" which, regardless of the risk, must be established due to "the nature, scope, context and purposes of processing"[3].

As an accountability measure, DPbD must be approached in an integrated manner with the rest of the guarantees established in the GDPR and as an integral part of the organisation's procedures and culture.

On the one hand, as stated in the EDPB Guide, DPbD is related to data protection by design. DPbD measures must be taken into account from the conception of the processing and implemented through the data protection measures and guarantees identified in the design of the solution.

The selection of measures and guarantees for DPbD impacts on the requirements established on the security domains (confidentiality, availability, integrity and authenticity) from a "default security" point of view. However, it should be noted that default security may, in certain situations, conflict with DPbD. A specific example is to excessively monitor or authenticate users so that personal information obtained from the user may represent a risk[4] to the rights and freedoms of users whose access to the system, product or service is intended to be managed.

Finally, DPbD is related to transparency, since only by knowing the characteristics of the processing will the user be able to decide, freely and with knowledge of the possible consequences, to go beyond the initial configuration that is more respectful of privacy, selecting those options of the application, product or service that have a significant impact on it.

[2] The risk associated with processing, however low, will never be zero.

[3] Article 24.1 of the GDPR

[4] A risk to their rights and freedoms in terms of systematic and thorough observation or assessment of personal aspects.

III. APPLICATION OF DATA PROTECTION BY DEFAULT

Section 2.2 of the EDPB Guidelines provides an analysis of Article 25(2) of the GDPR. The opinion established by the European Data Protection Board regarding the implementation of DPbD measures focuses on three strategies:

- **Optimisation:** Optimisation of processing aims to analyse it from the point of view of data protection, which means implementing measures in relation to the amount of data collected, the extent of processing, its storage and accessibility.
- **Configuration:** This strategy must allow the processing to be configurable with regard to personal data by means of values (settings) available in the applications, devices or systems that implement it. Part of this configurability must be under the control of the user.
- **Restriction:** The restriction guarantees that, by default, the processing is as respectful of privacy as possible, so that the configuration options must be set, by default, to those values that limit the amount of data collected, the extent of processing, its storage and accessibility.

These three strategies are linked to the corresponding minimisation and control strategies defined in the Guidelines for Data Protection by Design of the AEPD, as is also explained in section 2.2 of the EDPB Guidelines.

The EDPB Guidelines state that DPbD measures must be in line with those adopted in the framework of data protection by design, specifically aimed at the implementation of the data minimisation principle, and that such measures must be selected according to their suitability for achieving this objective in the terms indicated above. Additionally, it is made explicit that only personal data that are necessary for the specific purpose of the processing must be processed. Explicit reference is made to articles 5.1.b, c, d and e of the GDPR. In particular, Article 5.1.c of the GDPR establishes the minimisation principle as that personal data "shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Likewise, the EDPB Guidelines state that the fact that personal data is needed to fulfil a purpose does not mean that all types of operations in the processing of such data can be carried out at any frequency. This means that the processing must be analysed in its different phases and in each one of them the minimum essential data for the operation to be carried out in each phase will be processed, the extent of the phases in which the data is processed will be the minimum necessary, the storage period of the information will be as short as possible and accessibility to the personal data will be the strict minimum, as established in article 25.2 of the GDPR:

> *Art. 25.2 ...That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.*

The application of the minimisation principle is not trivial, as it requires studying, justifying and establishing which data are necessary for processing. The necessary data are determined through an analysis of the data set with regard to the effectiveness that needs to be achieved to fulfil the purposes of the processing. Such analysis, in terms of the extent of subjects involved and the data processed for each subject, will depend on the type of processing. For example, in relation to the extent of data subjects, statistical science establishes that the group of subjects necessary to obtain the confidence level and interval

desired in a processing operation does not imply access to the data of the whole population, but that there are analytical procedures to establish the necessary volume[5].

However, it is a mistake to apply the minimisation principle in a way that compromises the purpose of the processing. For example, in relation to the extent of data processed about a subject, designing a clinical evaluation that collects insufficient information so that it is not possible to reach a diagnosis of the individual with the adequate levels of precision, would not only fail to comply with the minimisation principle, but would even be contrary to the principle of processing fairness, as it would be unfeasible to comply with the declared purpose. Consequently, the application of the minimisation principle implies an objective and rational analysis of the processing.

[5] For example, an analysis of a population of 40 million with a 99% confidence level and 1% confidence interval might require data from fewer than 20,000 people (https://www.surveysystem.com/sscalc.htm, https://www.calculator.net/sample-size-calculator.html)

IV. OPTIMISING PROCESSING

Optimising processing is a fundamental activity in any organisation with the aim of achieving continuous improvement in its effectiveness and efficiency. This section will only address such optimisation from the point of view of personal data protection, a vision that should be integrated into the entity's overall quality process.

For the adoption of any measure of accountability it is essential to analyse the processing activity, divide it into phases, determine the processing operations carried out in each of them, know the characteristics of each phase and optimise it, at least from the point of view of data protection. As indicated above, this task is not exclusive to DPbD, but is included in the strategy for the rational implementation of accountability measures.

The optimisation of the processing for the implementation of DPbD must be carried out by means of the following activities, which in some cases will be done in parallel:

- A breakdown and analysis of the processing into phases
- The definition of use cases
- The analysis of the relationship between processing operations carried out by the same controller
- The optimisation of the processing

A. PROCESSING ANALYSIS

In order to ensure that DPbD measures are correctly adapted, the controller must analyse the processing that they intend to carry out. Such analysis must go beyond considering the processing as a black box. It is necessary to identify within it those specific operations that are carried out and the relationship between them.

The operations that may be part of a processing operation and which are of interest for data protection are defined, in a non-exhaustive manner, in Article 4.2 of the GDPR as:

> *...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.*

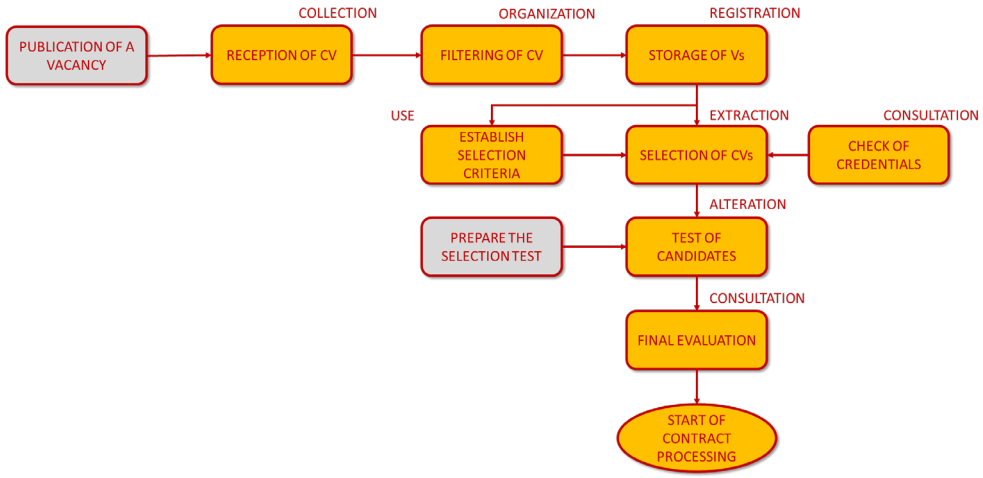

Figure 1. Simplified example of a processing activity relating to personnel selection. In this case, the operation or operations carried out are identified for each phase. Those phases which, in this example, would not process personal data are marked in shading.

Processing activities are structured in phases that implement operations. However, it is possible that, as part of a processing operation, there are phases that do not process personal data so that, and in principle, these phases would be transparent from the point of view of data protection[6].

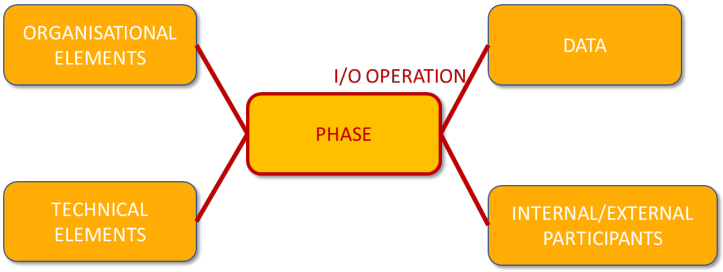

Figure 2. Elements that configure the phases of a processing operation

The implementation of the operations in each phase in which the processing is structured can be carried out with organisational measures and/or technical elements. Organisational measures, which may include aspects such as the roles assigned to each person, the physical layout of facilities (e.g. isolation of interview areas) or the generation and destruction of physical reports may be even more important and effective than technical components.

Processing operations may be implemented by means of components developed *ad-hoc*, i.e. specifically for such processing or by means of standard components or adaptations of *ad-hoc* developments of other processing operations. These components may include applications, servers, operating systems, network components, libraries, development environments, etc. They may also be third party components, standards or simply components available to the controller, which are reused for a new purpose. Among these are even components that may be of an organisational rather than technical nature, such as customer services.

In these cases, the term off-the-shelf[7] components is usually used, meaning pre-existing components that are "taken off the shelf". Off-the-shelf components are those prefabricated components, designed for a different specific purpose, which even come from previous uses by the same entity, or of general purpose, which are incorporated into the implementation of a processing operation.

The GDPR states that, when establishing the default configuration, the data controller must take into account the requirements for the specific purpose pursued by the processing. Therefore, in the analysis carried out of the processing activity, the relevance and need to carry out each of the different phases/operations of personal data processing identified must be determined.

Ultimately, a critical review of each phase and its purpose is mandatory in order to apply the minimisation principle.

B. USE CASES

Processing operations may be very simple and linear, in which the default configuration options are very limited, but we can also find complex operations that may offer different

[6] Although the phases that do not process personal data or do not collaterally affect what is established in the GDPR do have an impact on the analysis of the effectiveness and efficiency of the processing, it would not be within the competencies of the GDPR to assess the suitability of these phases in a strict manner.

[7] Term also used in the EDPB Guidelines

functionalities to adapt to users with different profiles or specific needs. The adjustment of the service may depend on different circumstances: normal or premium services; adaptation to a minor, adult or elderly public; presence of added value services, etc. The different service settings are those that configure different use cases.

Depending on the type of service required by the user, or that the controller intends to offer them within the framework of the same processing operation, it will be necessary to collect and process a different extent of personal data. A simplified example could be the different cases of use of a banking app:

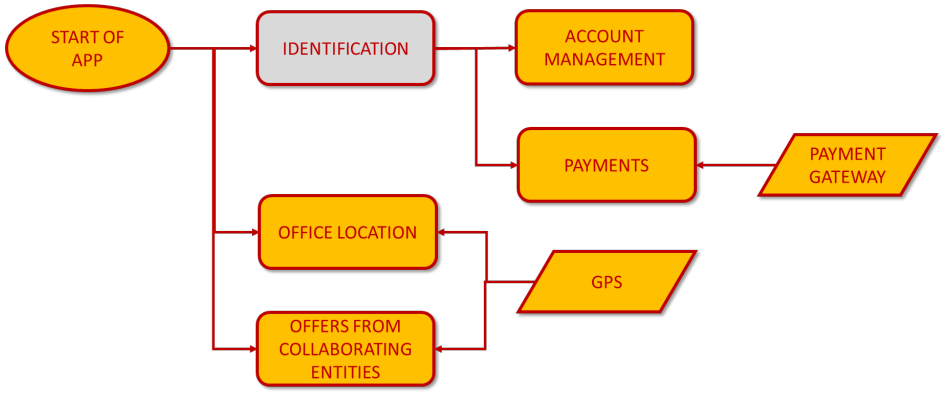

Figure 3. Breakdown into phases of processing in a simplified banking app.

The previous example shows a processing operation in which several use cases may be presented based on the functionality required by the end user:

- Account management, in which identification is required.
- Payments, in which, in addition to identification, communication with a payment interface is required.
- Office locations, which requires access to the current location.
- Reception of offers by proximity, which requires continuous geolocation of the data subject.

Depending on the use cases, the data controller must process a different extent of personal data, including user identification, interfaces with payment gateways, specific geolocation or continuous geolocation. This means that the processing must be configurable in terms of the type and extent of such data and that said configuration must be conditioned by the use case chosen by the user at any given time. The data that would be necessary for the potential use of all the future functionalities, including those that could be chosen by the user, should not be collected by default. For example, in the case of data collection on a web form for booking a service, like a repair service, where the request may be rejected due to unavailability, no more data should be collected initially than is necessary to make such booking, and not any additional data that would be used to provide the service in the case of vacancies. Where applicable, these should be requested once availability has been guaranteed.

Other processing operations in which different use cases may be found are, among others:

- In a social network, based on the degree of dissemination of personal information that the user wishes.
- On fitness bracelets, based on the services chosen: training, monitoring, statistics, health...

- In applications for monitoring epidemics, with regard to diagnostic or monitoring services.
- In telemedicine devices, based on the required processing.
- In platforms and applications in educational and training environments, based on the type of training or evaluation.
- Etc.

The use cases of a processing operation are linked to specific purposes and identify and group together options for configuring the processing so that the choice of a use case by the controller or the user determines the value of a series of configuration options.

The use cases must be determined by the data controller, who defines the different purposes of the processing and must establish the compromises between privacy, usability, functionality and security. The controller will have to assess the suitability of the use cases defined according to the reality and needs of the users, as well as their adaptation depending on whether the context of the processing changes over time. In accordance with the same minimisation principle, such assessment must be as unobtrusive as possible from the point of view of data protection. For example, it could be considered intrusive and disproportionate to automatically monitor users' usage habits for this purpose, while conducting usage surveys would be a less intrusive way. A relevant aspect to be taken into account when defining use cases is to consider the needs of subjects that belong to vulnerable groups, especially minors.

The use cases defined by the data controller must be able to be adjusted by the user.

Under no circumstances may the use cases defined by the data controller present the user with a dilemma of the type "take it or leave it" to access the contracted service and, consequently, impose some imposition for the processing of personal data that exceeds what is necessary. Access to a service may not be denied simply because the user has opted for a restrictive configuration regarding the amount of data processed or the extent of such processing[8].

C. RELATIONSHIPS BETWEEN PROCESSING OPERATIONS

Within an entity it will be common for several processing operations to access the same data sets and to make use of common data collection, processing or disclosure services[9]. These components that implement operations and are shared between processing operations are in many cases inherited systems[10]. In other cases, such as the implementation of applications in mobile systems, the processing operations are developed by means of standard third-party components shared between various applications that make common use of access to data processing services[11].

[8] In line with the provisions of section 3.1.2 of the EDPB "Guidelines 05/2020 on consent under Regulation 2016/679"

[9] With organisational implementation, such as a physical customer service desk, as well as technological, such as a web page.

[10] A computer system or application that is still in use due to replacement or redesign costs.

[11] With regard to the potential risks for data protection, consult: Progress of the study by IMDEA NETWORKS and UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios" https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-IMDEA-android.pdf

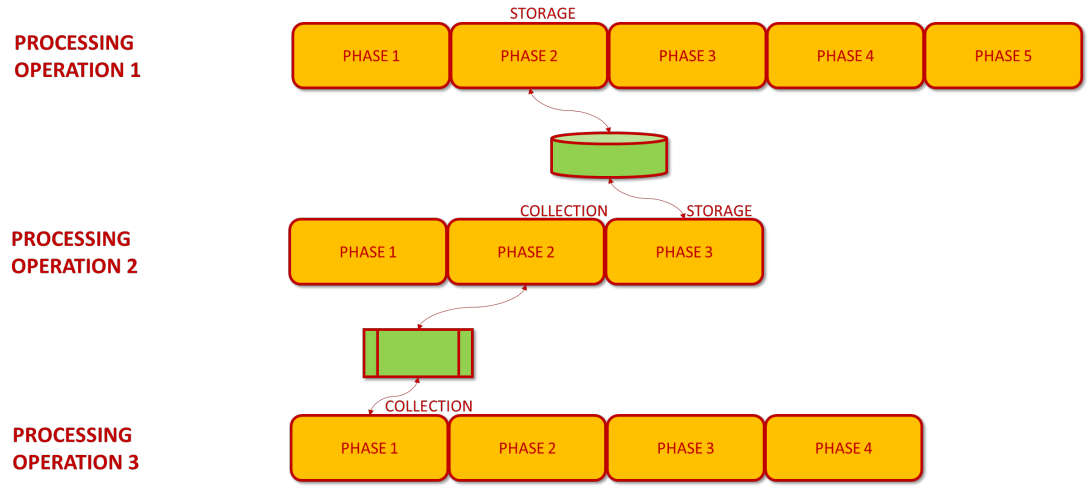

Figure 4. In this case, processing operations 1 and 2 include personal data storage phases, which are implemented in the entity's database services, while processing operations 2 and 3 include data collection phases implemented on the same data capture libraries (for example, an API on Android).

The controller must analyse each processing operation in the context of the organisation to identify the configuration needs of the services common to different processing operations for, for example and depending on their specific type:

- Determine the minimum data required for each processing operation, regardless of the data available.
- Carry out a logical and/or physical separation of personal data used in each processing operation.
- Manage access rights based on each processing operation.
- Establish an independent space, which could be logical or physical depending on the case, for the processing of sensitive data.

This analysis is closely related to the application of Article 6.4 of the GDPR and the limits stated in section 2.2 of the EDPB Guidelines, in the sense that controllers should be careful not to extend the limits of "compatible purposes" and bear in mind what processes will be within the reasonable expectations of the data subjects.

D. ADAPTATION OF THE PROCESSING

Together with the activities of analysis, determination of use cases and selection of shared components, it is necessary to assess each of the phases or stages of the processing operation for each of the use cases defined by the controller, as well as to determine:

- The need for the phase, in order to determine whether it is superfluous or avoidable from the point of view of the processing of personal data.
- The applicable minimisation, establishing:
  - The minimum set of personal data to be processed at this phase and which must be strictly necessary for the specific operations they support.
  - the need for inferred data, if any.
  - whether the phase may be implemented without using personal data.
- The storage period during which the personal data must be retained.
- The access criteria for applications, services and persons:

- What defined roles in the entity must have what access privileges and to what data.
- What roles outside the entity have been defined and with what access privileges and to what data.

- The control capacity to be given to the user over the previous options.

V. CONFIGURABILITY

A. PROCESSING CONFIGURABILITY

A service, system or application is "non-configurable" when in its design and implementation there are some fixed parameters that determine in an unalterable way the way in which the processing is going to be executed, either because it has acquired a non-configurable implementation or it has been configured with fixed values. In these cases, it is said that the functionality is "wired-in".

When the processing is configurable, it implies that it has been designed with a set of options that may be modified by the controller or even by the user. For example, it is possible to configure the collection of geolocalisation data, the information stored in the activity records, the permissions to access the content of the device, the identity information that will be requested from a system user, the possibility of encrypting communications, the use of advertising identifiers, etc. Additionally, each configuration option may be defined by a set of parameters[12], for example, in the case of configuring the application's activity record, in addition to a parameter for activating such record in a general way, there could be parameters for determining the maximum storage time, the actions subject to recording, the granularity of the record at the level of access types, the time information or identification information of the user and the device, etc.

At the time of implementation there will be parameters that may adopt any value, while others will be limited to a range of values. In turn, these parameters will adopt initial default values. The set of different options, their parameters and default values are established by the controller as requirements of the service, system or application.

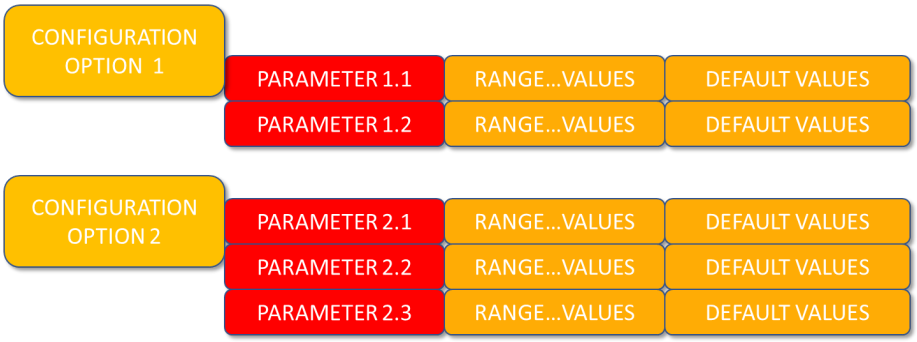

Figure 5 List of configuration options, parameters, ranges and default values

Pursuant to DPbD, the data controller must establish the configurability requirements in each of its phases, based on the analysis that has been carried out and the use cases identified. Such requirements must be translated into the design and implementation of the processing.

The default configuration determines the regular use of the service and the characteristics of the processing, provided that the controller does not offer the user the possibility of personalising it or that, by doing so, the user does not make use of it. The "default" configuration will consist of the set of pre-selected or pre-assigned "parameter-value" pairs in a system, application or service, which condition, in whole or in part, the way in which it operates.

[12] In the case of having the option to configure the encryption of disclosures, or the option to encrypt the stored data, there will be several parameters that could be set, such as the type of algorithm, block size, key length, key robustness characteristics, possibility of key reuse, random value generation mechanisms, etc.

The configurability has four aspects:

- The identification of the configurability requirements, which will be integrated as part of the privacy requirements by design of the processing and will result in the determination and selection of a set of configuration options, understood as the set of parameters that may be modified and their possible values, including the default value, which determine the behaviour of the system, application, product or service. Consequently, it will be necessary to identify:
  - Configurable parameters
  - The value ranges technically available
  - The default value assigned to each parameter
- Determine which of the configuration options will be under the exclusive control of the controller and with what limits.
- In the event that certain configuration options, due to the nature of the processing, are under the control of the user, it is necessary to establish which of the configuration options are those considered and with what limits.
- Determine whether the off-the-shelf components with which the processing is to be constructed comply with such configurability requirements and adjust their value.

This aspect of configurability must be especially valued when processing data on minors or data on groups of people in vulnerable situations (victims of gender violence, people at risk of social exclusion, etc.). For example, making it possible for access to victim assistance services not to appear in the call records or in the history of the device.

Finally, the establishment of configuration options and use cases must be input information in the stage of risk analysis for the rights and freedoms of individuals, in order to establish how the values assigned to the different parameters may affect the privacy of users, as well as the potential consequences of their subsequent modification by them or possible handling by third parties[13]. Users must be informed of the consequences and risks of configuration in a clear and concise manner so that they can make an informed decision regarding the impact on their privacy.

Choosing the default configuration is not a trivial matter. The following elements must be determined:

- The different use cases of the processing that are offered to the user based on the purposes.
- The minimum data in each of the phases and for each of the different use cases identified.
- Which of the possible use cases available will be configured as the default use case.
- The configuration parameters and their values based on the default use case selected.

A configurable parameter will not accept any value, but the possible values will be limited to a range or a limited set of configuration options[14]. However, the degree of configurability must be sufficiently broad to offer real configuration options to the controller or system user. In addition, the different configurable parameters may not be independent of each other and

[13] For example, a processing operation may allow the user to activate geolocation options, so the risk that a third party may manage or access such geolocation information must be analysed.

[14] This limitation may be technical, such as the length of a key may not have an infinite value, but a maximum value. It may also be a functional limitation, e.g. the configurability of passwords may be limited to only those that meet certain robustness requirements.

there may be technical links between them. Consequently, the configurability of a certain parameter is not measured by a "yes" or "no", but by a certain degree of configurability that may sometimes require an analysis of dependencies between parameters, as could be the case in the configuration of authentication or security systems.

The default configuration also affects organisational measures, as stated in section 2.2 of the EDPB Guidelines.

Among the additional desirable requirements, as stated in the EDPB Guidelines, is that the processing options and values should be universal for all instances of the application, device or service model implemented by the controller and that "out-of-the-box" approaches should be chosen for the implementation of the systems, minimising the processing of personal data and without the need to go through a lengthy configuration process before use.

B. CONFIGURABILITY OF COMPONENTS

The use of third party components (addressed in section IV.A "Processing analysis") may limit the capacity of the controller or the processor to the extent that it may affect the correct execution of the requirements established by the controller for the application of the configurability requirements. Therefore, it is important to determine, with regard to these components, which values are prefixed and unalterable, which parameters are configurable and the default value with which they are configured, as well as the set of possible values that they could adopt.

The problem that the standard components may present in a processing operation is that they were developed with an objective and purpose that may be different, even completely different, from that of the processing operation in which the controller uses them. Therefore, a key aspect of the configuration process is to find out whether these components carry out processing activities which are not necessary for the processing operation analysed. That is to say, if they are implementing additional and non-configurable functionalities that generate side effects such as, for example, disclosure to third parties, collection of traffic data, logs, etc.

When selecting the components, the controller must take into account the use of PETs or "Privacy Enhancing Technologies". PETs are an organised and coherent set of ICT solutions that implement privacy strategies and patterns, including processing configurability features.

In the event that these standard components do not comply with the principles of minimisation, the legitimacy of the processing and, where applicable, the possibility of deactivating the additional functionalities and, if necessary, the possibility of not using them and opting for another alternative component must be analysed.

C. USER CONTROL[15]

Once a parameter relating to a processing operation is configurable, it is necessary to determine whether it is appropriate to give the user control over its configuration. For example, a service that allows search engines to index user data under certain configuration conditions could allow the user to determine the extent of indexable data, individually or by category.

[15] The English term commonly used is "intervenability" which could also be translated as capacity for participation, intervention, control or influence.

It is not always necessary to give the user control over the configuration options. On the contrary, in some cases it is not appropriate and this option should not be offered. For example, the user should not be allowed to set their own access role to the system, but this task should depend on the administrator.

User control means that users have the possibility to make decisions regarding configuration actions, but it also implies transparency and information about the result and consequences of the options that users can choose.

In this case, it is important that the user is adequately informed and understands the consequences, in terms of privacy, rights and freedoms, of choosing one or another configuration or modifying the default values (e.g. in cases where the user wants to broaden the initial processing purposes with extended functionalities). Adequate information must be in line with the expectations that the user has about the system. The user must also have relevant information about the accessibility by third parties to their personal data and the moment when this is taking place, such as receiving information that a continuous recording of their geolocation is being carried out by means of an icon on the screen[16]. This information should make it easier for the subject to exercise their rights, for which it will also be necessary to have adequate and agile tools.

The way in which the effects of the configuration changes chosen by the user are implemented must be perfectly established by the controller in order to inform the user of the precise moment in which these are effective, as well as the additional actions they may have to carry out (for example, rebooting the system). These should be as little disruptive to the user as possible, thus avoiding consequences such as loss of data or previously configured personalisation characteristics.

In this regard, it is necessary to bear in mind that an excess of information or configuration options required to launch and use the system may lead the user to make erroneous decisions that could affect their rights and freedoms. The number and frequency of changes must be considered together with the amount of information provided to the user. Therefore, and in the interest of usability, an appropriate way to avoid, or at least limit, the information fatigue that a large number of configuration questions entails is to offer the user the possibility of choosing between use cases that group together configuration options. This provides a fluid mode of interaction and avoids burdening the end user with an infinite number of questions to answer and options to select.

The information provided about the different functionalities of the use cases must raise the user's awareness of what data (and its associated metadata) will be necessary for the system, application, product or service to provide and manage that specific functionality.

The application of use cases allows a two-tier approach to processing control by the user: a first layer to select general use cases and a second layer for the detailed configuration of each one of them.

In any case, if a modification takes place, it must be possible to revert the change to the initial preset values and to recover the "privacy friendly" configuration established at origin in an easy, simple and intuitive way.

User actions that change configuration options must be active, aware and informed and must not be confused with any other actions. For this purpose, reference is made to the guidelines on consent[17] published by the EDPB.

---

[16] Article 13 of the GDPR states that “Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information...”

[17] Guidelines 05/2020 on consent under Regulation 2016/679”
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

VI. RESTRICTION BY DEFAULT

The use case that, being the most restrictive by default, allows access to the basic functionality of the system (initial functionality, factory settings, ...) must always be available and selected initially without the need for any change by the controller or the user.

The default use case must be that which complies, in the most restrictive way possible, with the principle of minimisation. Data controllers must select the appropriate configuration options in order to ensure that only data strictly necessary to achieve the purpose of the processing that has been enabled will be collected. It must be noted that this case of minimal intrusion may not be unique and that, depending on the complexity of the processing, there may be several restrictive use cases. In such circumstances, the data controller must justify the choice of that established by default.

The user will have to modify the default configuration if they wish to extend the processing of personal data beyond the legal basis on which the main processing for which the "default" configuration has been made is based, or if the new functionalities involve purposes that are not compatible with the original purpose for which the personal data were initially collected.

Pursuant to the fairness principle established in article 5.1.a of the GDPR, the data controller must guarantee that dark patterns are not used, i.e. user interfaces designed to influence, through psychological manipulations and in a disguised form, the choices of the data subject, at least with regard to the processing of their personal data. An example of this type of pattern is to offer the user an attractive purpose based on their behavioural analysis to mask a transfer of data to a third party for purposes that have not been clearly defined[18].

[18] An explanation of the dark patterns can be found at https://en.wikipedia.org/wiki/Dark_pattern and examples at www.darkpatterns.org.

VII. MEASURES OF DATA PROTECTION BY DEFAULT

As described in chapter "III Application of data protection by default", implementing DPbD strategies requires the adoption of measures on:

- The amount of personal data collected.
- The extent of processing.
- The storage periods.
- The accessibility to the data.

These DPbD measures are grouped through configuration options that allow the extent of the processing to be determined. Among the configuration options are those that allow the controller to configure the processing, those that are under the control of the user in their "privacy panel" and the configuration requirements of the shared components.

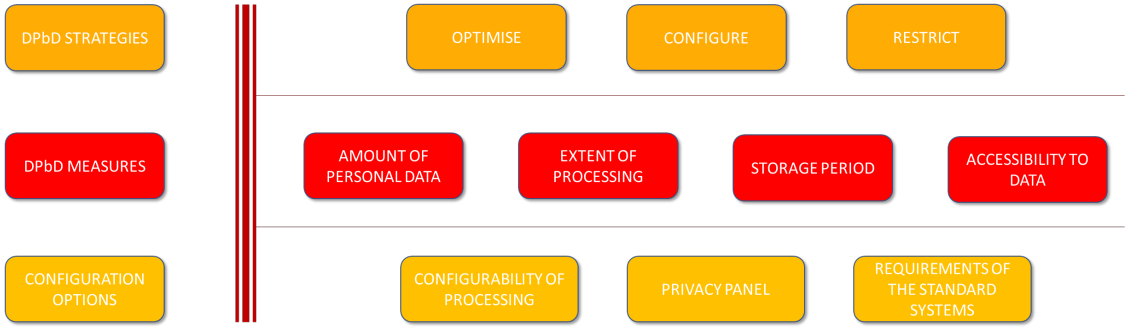

Figure 6. DPbD strategies, measures and configuration options

And to facilitate the practical application of DPbD, the last section of this chapter provides guidance on the characteristics of the configuration options that could be included in a processing operation.

A. AMOUNT OF PERSONAL DATA COLLECTED.

As stated in the EDPB Guidelines, the term "amount" implies both qualitative and quantitative data factors. The data controller must consider the volume of personal data processed, the level of detail, the different categories, the sensitivity (special categories of data) and the types of personal data required and necessary to carry out a processing operation, including both the data collected and those generated or inferred from them.

B. EXTENT OF PROCESSING.

The implementation of DPbD implies that the processing operations on personal data carried out by the controller will be limited to what is strictly necessary to fulfil the stated purpose.

Consequently, when the processing is studied as a set of phases, it must be ensured that the operations carried out in each one of them are only those necessary, and on the data required, to fulfil the purpose of said phase. In particular, the data controller and, where appropriate, the user must be able to configure the extent of the processing in each phase, namely according to the use cases.

C. STORAGE PERIOD.

Limitations on the storage period are linked to the extent of the processing, since the storage of the data is itself a processing operation. However, due to its specificity, it is analysed independently.

The application of the minimisation principle regarding the storage period establishes that, if a personal data is no longer needed after a phase of the processing has been carried out, such data must be deleted (which could imply in some cases blocking[19] or anonymisation). Any storage period must be objectively justifiable and substantiated. For example, in cases where it is necessary to use captchas on websites that process biometric information to detect robots, such as mouse movement, the storage of that information for use in subsequent stages of processing must be justified.

D. ACCESSIBILITY TO THE DATA

As stated in the EDPB Guidelines, the data controller must establish who can access the personal data, both with regard to personnel within the organisation and to third parties, whether they are other entities and bodies or even automated systems such as search engines, cloud servers or any other application or service system that accesses the data used in the processing. The degree of accessibility to the data must be established on the basis of an analysis of need to fulfil the purpose of the processing.

Such analysis must be carried out for each of the phases of the processing and implemented by means of:

- A definition of the roles and responsibilities of the organisation members.
- A policy for controlling access privileges as part of the organisational measures adopted.
- The inclusion of mechanisms for controlling access to information which implement the defined policy, and which will be partly of an organisational and technical nature.

The controller must limit the accessibility to personal data by default and, where necessary, consult the subject of the personal data before publishing it or making it accessible in any way to an indefinite number of people. To this end, the processing must be configurable by the data controller, and if applicable by the user, in order to adjust the degree of accessibility to the different use cases.

Standard components may be used in processing operations for the implementation of data operations. In practice, it will be very common for different processing operations to share these standard components and access shared services with other processing operations in data collection, storage and transfer tasks. Therefore, it is necessary to be able to configure (limit) the possible disclosure of data with other processing operations that is not necessary for the original purpose.

E. PRACTICAL APPLICATION OF THE MEASURES TO BE IMPLEMENTED: CONFIGURATION OPTIONS

Annex II contains a list for guidance purposes of those options in which a processing operation could be configured to implement the measures regarding the amount of personal data used, the extent of the processing, the storage period, the accessibility to the data and any other circumstance in the processing that may affect the privacy of the users.

[19] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673#a3-4

Associated with each of these configuration options, the controller must determine the specific parameters[20], establishing the ranges or possible values that the parameters can accept, as well as which of said parameters or values is set by default, depending on the use cases.

Therefore, the processing configurability requirements will contain the list of options, detailing parameters, ranges and values by default. Such requirements will be applied by design, both for the development of *ad-hoc* components and for the use or acquisition of standard components, as well as for the definition of part of the interface with the user.

The options that may be configured by the user will form part of their "privacy panel", and they will be able to modify the value by default originally configured for these options at their discretion. It should again be noted that not all configuration options must be available to the user, or to all types of users, and their determination will be limited to the process of defining the requirements for configurability of the processing[21].

It is important to stress that not all the options included in the list are applicable to all cases, nor are all the possible configuration options that a specific processing operation may have contemplated. The list detailed in Annex II will have to be adapted and in some cases extended for each specific processing operation. For this reason, the list will also be available in a spreadsheet on the AEPD's Innovation and Technology microsite, so that it may be used by controllers, processors and technology providers, and updated more quickly.

[20] As noted in a previous footnote, in the case of having the option to configure the encryption of disclosures, or the option to encrypt the stored data, there will be several parameters that could be set, such as the type of algorithm, block size, key length, key robustness characteristics, possibility of key reuse, random value generation mechanisms, etc.

[21] As noted above, there are cases in which the user's role should not be able to be altered by the users themselves.

VIII. DOCUMENTATION AND AUDIT

As established by the principle of accountability in Article 24.1 of the GDPR, DPbD guarantees and measures must be documented and collect sufficient information to allow, in a satisfactory and demonstrable manner, accreditation of compliance with the GDPR. Such documentation must enable the traceability of the decisions and verifications made pursuant to the minimisation principles referred to above.

The documentation relating to the standard components, which the controller has the obligation to ensure is complete and sufficient[22] to justify the decision to have included the component in the processing, must be included in the documentation of the processing. In particular, when such standard component corresponds to a service developed by a third party, the controller must guarantee that the necessary information to determine the correct application of the DPbD principle in said system, product or service is described in the documentation.

In short, the processing must be auditable throughout its life cycle, including the withdrawal stage.

The audit to determine the correct application of DPbD will be integrated within a data protection audit plan and this, in turn, within the general audit plan of the processing that could cover objectives beyond the GDPR.

The DPbD forms part of the conditions of strict compliance with the GDPR that are not subject to or conditioned by the result of an analysis of risks to rights and freedoms, such as, among others, the existence of a legal basis that legitimises the processing or the information requirements established in Articles 13 and 14. Therefore, the controls to be analysed in the case of an audit which include DPbD will not be selected as a result of an analysis of risks to rights and freedoms.

The basic controls that should be considered to determine compliance with DPbD are listed below, by way of example and not exhaustively. As mentioned above, this list of verifications should be considered as limited to a DPbD audit on its own and should be integrated into the overall framework of a data protection audit:

1. Verify that the necessary documentation is available in the controlling entity to apply DPbD in an objective manner; in particular, the definition of the roles and obligations of the members of the organisation, the access control policy, the information policy and any other significant documentation.
2. Verify that the entity has procedures in place to ensure compliance with the aforementioned policies and that these are operational.
3. Verify that basic information regarding the processing is available, in particular on the nature, scope, context and purposes, as well as the analysis of proportionality and need.
4. Have documented an analysis of the processing from the point of view of DPbD.
    a. Verify that the processing analysis has been broken down into phases and identify for each phase the operations, the organisational and technical implementation, the personal data and the internal and external parties involved.
    b. The standard components are identified.

[22] Commercial information or information contained in advertising actions cannot be considered complete and sufficient information.

c. Likewise, the interactions, services, systems and operations shared with other processing actions must be identified.

d. Each phase has been studied for optimisation in relation to need, minimisation, storage, access and controls.

e. The use cases of the processing have been defined and the criteria have been considered by the controller for their determination.

f. In particular, the protection of the privacy of subjects from vulnerable groups, especially minors, has been considered in the definition of the use cases.

5. Verify that the life cycle of the data is adjusted to the use cases.
6. Verify that the controller adjusts the use cases to the real operations and needs of the user and checks the evolution of such operations in time.
7. Verify that the controller does not oblige the user to accept more intrusive processing (a greater amount of data or a greater extent of operations) as a condition for accessing a service.
8. Verify that the configuration options are correctly identified and defined regarding:
    a. Type of DPbD measures (the amount of personal data collected, the extent of processing, the storage period, the accessibility to the data or other actions)
    b. Configurable parameters and range of values associated with a sufficiently broad set of alternatives.
    c. Default values associated with each parameter.
    d. Configuration parameter dependencies and possible conflicts between chosen values, even with other options.
    e. Which roles (controller or user types) have control over the configuration options and limits of such control.
9. Verify that the configurability requirements established by the controller have been transferred by design and are correctly implemented.
    a. Verify that there is a justified decision about non-configurable options, identifying the functional or legal reasons that motivate this.
    b. In particular, to verify which off-the-shelf components fulfil the configuration requirements set out in the documentation and, where appropriate, determine the configuration limitations they have and the way in which they affect processing[23].
10. Verify the possibility of coexistence of alternative configurations in different instances of the application on different devices.
11. Verify that security measures have been implemented.
12. Verify that the default use case is the one that complies more restrictively with the minimisation principle.
13. Verify that the configuration change options offered to the user provide explanations that allow the user to make an informed decision.

[23] For example, in the case of implementing a corporate blog, if a tool developed by a third party is used (Wordpress, Blogger, SharePoint, etc), in each case the default configuration will be different and must be assessed.

a. Verify that the user receives sufficient information about the effects and consequences of the configuration changes to make a conscious choice. For example, in the case of choosing a lower protection encryption in exchange for access or higher performance, notify the possible consequences of such a change.

b. In particular, to provide information on when the configuration changes become effective.

c. Verify that “dark patterns” are not used to manipulate the user's choice process or to influence in a disguised way their decision regarding the scope of processing.

14. Verify that a change of configuration requires a conscious, free and intentional action by the user.
15. Verify the possibility of revoking choices at any time as easily as they were selected.
16. Verify that the user can return to the most restrictive initial configuration if they choose to change the configuration.
17. Verify that a change of configuration by the user, especially if it is a change towards more restrictive processing conditions in terms of minimisation, does not negatively affect the user.
18. Verify that the relevant documentation relating to the implementation of DPbD measures has been transferred to the stage of risk management for rights and freedoms and, in particular, to security risk management.
19. Verify that the relevant documentation regarding the implementation of DPbD has been used to configure the information and transparency policy provided to the user.

Pursuant to the provisions of control number 6: “the controller adjusts the use cases to the real operations and needs of the user and checks the evolution of such operations in time”, the above list should be considered as a generic minimum of controls to be reviewed and may be extended for specific processing operations. Due to the evolution of the processing environment, the updates of the processing and the possible social impact, which may be unpredictable, it is necessary to continuously adapt the use cases defined in the processing and, consequently, the necessary verification controls.

IX. CONCLUSIONS

Article 25 of the GDPR establishes DPbD as one of the accountability measures, integrated with the rest of the guarantees established in the GDPR, and being able to opt for different approaches and alternatives when implementing the DPbD dimension.

Although this paper focuses on how to address Article 25 obligations with regard to DPbD, all actions related to the implementation of DPbD in a processing operation must be addressed in an integrated manner with the rest of the measures and guarantees set out in the GDPR.

Both personal data controllers and processors and technology providers to the extent of their obligations must bear in mind DPbD measures. On the one hand, technology providers must provide technical solutions that include the possibility of establishing default configurations that comply with the principles of the GDPR, and on the other hand, controllers, and processors insofar as they offer services to execute their instructions, must choose solutions that fulfil these requirements and demand that technology providers comply with them.

The GDPR requires the data controller to set up a default configuration for processing that respects data protection principles, advocating minimally intrusive processing: minimum amount of personal data, minimum extent of processing, minimum storage period and minimum accessibility to personal data.

These minimums must be established "by default", i.e. DPbD must be applied whenever personal data are processed regardless of the nature of such processing. The establishment of privacy measures by default does not derive from the result of an analysis of risks to rights and freedoms, but rather they are measures and guarantees that must be established in any case.

User privacy panels must facilitate configurability by offering a two-tier approach through specific use cases and configuration options. Additionally, the information provided to the user about the consequences of their choices must be complete and transparent. These panels and the way the information is provided should also be in some way standard, both regarding the use of icons and in the distribution of configuration options in the user interface, in order to improve transparency and usability.

The application of DPbD must be demonstrable, which means that its implementation must be justified, documented and auditable. In this regard, the third paragraph of Article 25 of the GDPR establishes that:

> *3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.*

The use of certifications approved in accordance with Article 42 of the GDPR is one of the ways in which the controller would be able to demonstrate compliance with the implementation of DPbD measures.

X. ANNEX I: GDPR

A. ARTICLE 6.4

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

d. the possible consequences of the intended further processing for data subjects;

e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

B. ARTICLE 25 DATA PROTECTION BY DESIGN AND BY DEFAULT

1. 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.

2. 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.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

C. RECITAL 78

78. The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design

and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling data subjects to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."

XI. ANNEX II: LIST OF CONFIGURATION OPTIONS

List, non-exhaustive and for guidance purposes, of those options in which a processing operation could be configured to implement the measures regarding the amount of personal data used, the extent of the processing, the storage period, the accessibility to the data and any other circumstance in the processing that may affect the privacy of the users.

	Configuration options grouped by type of measure	Options that could be set in the processing by the controller	Options that could be included in the privacy panel	Configuration options that could be set in the off-the-shelf components
Amount of personal data				
	Operation in anonymous mode.	X	X	
	Operation without the need to create a user account.	X	X	
	Operation with different user accounts on the same device for the same data subject.	X	X	
	Operation with different user accounts on different devices for the same data subject and processing.	X	X	
	Identification by means of tools and technologies that enhance privacy, such as attribute-based credentials, zero knowledge tests, etc.	X	X	
	Aggregation of data: in time, in space, by groups, etc.	X		
	Calibration of data granularity: e.g. decrease the frequency of collection of data on location, measurement, etc.	X		
	Generalisation of data: use ranges for age, postal addresses for addresses.	X		
	Adjustment of the extent of the data collected according to the use cases	X		

	Alternatives and wilfulness in the contact information requested to the user: e-mail, postal, telephone...	X	X	
	Monitoring techniques in processing (cookies, pixel tags, fingerprint, etc.)	X	X	
	Configuration of unique identifiers (tracking IDs), programming of their reset and notification of activation times.	X	X	
	Device metadata collected from the device (battery consumption, O.S., versions, languages, etc.)	X	X	
	Metadata included in the processed or generated media (in documents, photos, videos, etc.)	X	X	
	Information collected about the user's Internet connection (device from which they connect, IP address, data from the device's sensors, application used, browsing and search log, web page request, date and time log, etc.) and information regarding elements located near the device (Wi-Fi access points, mobile phone service antennas, activated bluetooth devices, etc.)	X	X	
	Information collected about user activity on the device: powering up, activating applications, using the keyboard or mouse, etc.	X	X	
	Mechanisms for the staggered collection of information required for processing. Delaying the collection of data until the phase in which they are necessary.	X		
	Type and amount of new data inferred from automated processes such as machine learning or other artificial intelligence techniques.	X		
	Data enrichment and linking to external data sets	X		
	Free activation and deactivation of data collection systems (cameras, microphones, GPS, bluetooth, wifi, movement, etc.).	X	X	
	Establishing a temporary schedule of when sensors (e.g. cameras, microphones, etc.) can be operational.	X	X	

	Incorporation of obfuscation mechanisms to avoid the processing of biometric data in photos, video, keyboard, mouse, etc.	X	X	
	Physical blockers (such as camera lens cover tabs, speaker blockers, etc.)	X	X	
	Use of privacy masks or pixelation in video surveillance systems.	X		
Extent of processing				
	Definition and design of processing operations to minimise the amount of temporary copies of data generated and to minimise storage times, transfers and disclosures	X		
	Pseudonymisation according to the processing operations that may exist in each phase or stage.	X		
	Local and isolated processing, including the possibility of local storage.	X		
	Additional processing of the collected metadata - log files.	X		
	Exercise of right to object, right of imitation or right to erasure	X	X	
	Configuration of the processing for profiling or automated decisions (case of cookies)	X		
	Possibility of configuring all optional processing operations for non-essential purposes, such as data processing for service improvement, usage analysis, ad customisation, detection of usage patterns, etc.	X	X	
	Configuration of a secure deletion of temporary files, mainly those outside the user's device and outside the controller's systems	X		
	Incorporation of a user data reset option to resume the relationship from scratch	X	X	
	Configuration of the data enrichment option	X		

	Considering mechanisms for auditing the existence of Dark Patterns	X		
	Specific section for configuration options related to sensitive data		X	
	Help and transparency panel with examples of use and possible risks and consequences for the rights and freedoms of the user		X	
	Incorporation of a specific means (button or link) to return to the initial configuration with default values		X	
Storage period				
	Configuration of session data erasure after closing.	X	X	
	Configuration of maximum time limits for logging out of the application or devices.	X	X	
	Time limits for the storage of user profiles.		X	
	Configuration of the management of temporary copies.	X		
	Control of the erasure of temporary copies.		X	
	Elimination of the user's trace in the service: “right to be forgotten”	X	X	
	Identification, within the record of data files collected from the sections, or data within sections, that may be anonymised.	X		
	Programming of automatic blocking and erasure mechanisms.	X		
	Programming of automatic mechanisms for the erasure of outputs to printing devices.	X		
	Configuration of historical data storage periods in the service: e.g., on purchase sites, last articles, last consultations, etc.	X	X	

	Incorporation of generic anonymisation mechanisms.	X		
Accessibility to the data				
	Profile information of the data subject shown to the user and third parties: name, pseudonym, telephone number, etc.	X	X	
	Information about the data subject that is shown to third parties: e.g. selective disclosure of CV elements, medical history, etc.	X		
	Information about the status of the data subject accessible to third parties. For example, in messaging applications, information on availability, message writing, message reception, message reading, etc.	X	X	
	Classification and labelling of processing operations, document sections and/or data within sections, which can be managed through an access control policy.	X		
	Organisation, classification and labelling of the application or service based on data sensitivity, sections or processing operations.	X		
	Possibility of defining and configuring access profiles and granular assignment of privileges.	X		
	Automatic session blocks.	X	X	
	Assignment of data access profiles based on user roles for each processing phase.	X		
	Workspace design (isolated interview areas, non-accessible physical files, non-transparent folders, screens not exposed to third parties or with privacy filters, headphones for telephones, call centres, clean table policies, etc.).	X		
	Information management parameters such as where the data is stored and processed, whether it is done in plain language or using encryption, the access control mechanisms implemented, whether there are multiple copies of the data, including instances that have been unsecuredly deleted, that may be accessed by third parties.	X		

	Control of data storage encryption.	X	X	
	Control of data communication encryption.	X	X	
	Procedures for managing access to shared print/output devices where documents may be left behind by the user.	X		
	Where applicable, prohibition of printing.	X		
	Control of print output deletion.		X	
	Procedures for managing removable storage devices for periodic formatting.	X		
	The retention or deletion of session information in applications, shared systems, disclosures or systems provided to the employee or end user.	X		
	The type and amount of metadata collected in the documentation generated by the system utilities (word processors, drawing tools, cameras and videos, etc.).	X		
	In the sending of messages, configuring the incorporation of conversation threads, as well as configuring the possibility of sending confirmation of multiple recipients.	X		
	Mechanisms to avoid indexation on the Internet	X		
	Organisational and technical measures for reviewing and filtering information to be made public.	X		
	Systems of anonymisation and/or pseudonymisation of texts to be disseminated.	X		
	Parameters for managing the connectivity elements of the devices (WiFi, Bluetooth, NFC, etc.).	X		
	Alerts regarding the connectivity status of devices.	X	X	

	Controls to prevent the disclosure of unique device identifiers (Advertising-ID, IP, MAC, serial number, IMSI, IMEI, etc.).	X		
	Access control mechanisms for passive systems (such as contactless cards) with the incorporation of terminal authentication protocols or with physical measures to prevent electromagnetic access.	X		
	Accessibility controls for user content on social networks.	X		
	Incorporation of controls to collect affirmative and clear confirmation actions before disclosing personal data, so that dissemination is blocked by default.	X		
	Configuration of notices and reminders to data subjects about what information dissemination and disclosure policies are in place.	X	X	
	Definition and configuration of access permissions on datasets (databases, file systems, image galleries, etc.) and information capturing elements such as sensors (cameras, GPS, microphones, etc.) of the device and information regarding elements located near the device (Wi-Fi access points, mobile phone service antennas, activated bluetooth devices, etc.)	X		
	Definition and configuration of data access permission policies between applications and libraries, as in the case of mobile phones.	X		
	Definition of access profiles based on privileges or other technological and procedural barriers that prevent the unauthorised linking of independent data sources.	X		
	Content recorded in the logs (who, when, to what, what action, for what purpose, ... the data is accessed).	X		
	Definition of automatic warning systems for specific events.	X		
	Traceability of data disclosure between controllers, processors and subprocessors.	X		
	Configurable security options (apart from encryption options).	X		

	Allowing different access configurations for different devices.	X		
	Configuration of warning systems for abnormal data access.	X		
	Configuration of some of the security parameters, particularly the keys and how to balance the security/performance/functionality ratio based on the robustness required by the user.		X	
	Control of the distribution scope of the information that is distributed in the application environment (social networks, work networks, etc.).		X	
	Configuration of the reception of warnings when information is being made accessible to third parties.		X	
	Control of the metadata incorporated in the information generated or distributed.		X	
	“Right to be forgotten” mechanism regarding the information published in social networks or other systems.		X	
	Choice of where personal data is stored, either on local or remote devices and, in the latter case, other parameters such as processors or countries.		X	
	History of profiles and entities that have accessed your information.		X	
	Information on access to your data by authorised users.		X	
	Information on the latest changes carried out and the profile that has made the change.		X	
	Configurability of access controls by functionalities provided.			X
	Configurability of logical separation of data groups.			X
	Configurability of physical separation of data groups.			X

	Selective disabling or cancellation of functionalities.			X
General				
	In the event that the service is multi-device, the possibility (not obligation) of applying general privacy criteria applicable to all of them and in a single action.	X	X	
	Reminders, icons and warnings of all those actions that affect the privacy of the information: configuration changes, access to data by third parties such as video capture, sound, position, etc.	X	X	

XII. REFERENCES

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons in relation to the processing of personal data and the free circulation of these data and repealing Directive 95/46/EC (GDPR).

  https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1592307014433&from=ES

- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

  https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es.

- "Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default", dec. 2018. European Union Agency for Cybersecurity (ENISA).

  https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2