A Guide to Privacy by Design

V. october 2019

V. october 2019

TABLE OF CONTENTS

I. PRIVACY BY DESIGN

THE CONCEPT OF PRIVACY BY DESIGN

The idea of "data protection by design" has been around for more than 20 years and a great deal of work has been carried out in this area under the term "privacy by design" (*Privacy by Design*, PbD). This concept was developed by Anne Cavoukian, Ontario's Data Protection Commissioner, in the 90's and presented at the 31st International Conference of Data Protection and Privacy Commissioners in 2009 with the title *"Privacy by Design: The Definitive Workshop"* [1][2]. It was internationally accepted at the 32nd International Conference of Data Protection and Privacy Commissioners, held in Jerusalem in 2010, with the adoption of the "Resolution on Privacy by Design" [3].

This resolution recognised the importance of incorporating privacy principles within the design, operating and management processes of organisational systems, in order to attain a frame of integral protection regarding data protection. It also encouraged the adoption of the Foundational Principles of Privacy by Design as defined by Ann Cavoukian, and invited Data Protection Authorities to actively work on and promote the inclusion of privacy by design in policies and legislation on data protection within their respective States.

The Foundational Principles of Privacy by Design
1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Security: Full Lifecycle Protection
6. Visibility and Transparency: Keep it Open
7. Respect for User Privacy: Keep it User-Centric

Table 1 – Principles of "Privacy by design"

The General Data Protection Regulation (EU) 2016/679 [4](hereinafter, GDPR), in Article 25 [5] and under the heading "Data protection by design and by default" incorporates the practice of considering privacy requirements from the first stages of product and service design into data protection regulations. It therefore confers on it the status of a legal requirement in order to integrate the guarantees for protecting citizens' rights and freedoms with regard to their personal data from the early development stages of

1 Peter Hustinx, European Data Protection Supervisor. *Privacy by Design: Delivering the Promises,* Madrid 2009 https://edps.europa.eu/sites/edp/files/publication/09-11-02_madrid_privacybydesign_en.pdf

2 Ann Cavoukian, Identity in the Information Society, Aug 2010, Volume 3, Issue 2, pp 247-251. *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D* https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0062-y.pdf

3 Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem (Israel) 27-29/10/2010 https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

4 General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

5 Article 25. "Data protection by design and by default" - General Regulation (EU) 2016/679, on Data Protection https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3126-1-1

systems and products. Understood therefore as the need to consider privacy and the principles of data protection from the inception of any type of processing and for the purposes of drafting this document, the terms “data protection by design” and “privacy by design” can be considered as equivalent [6] [7] [8].

Privacy by Design (hereinafter, PbD) involves a focus geared towards risk management and accountability [9] to establish strategies that incorporate privacy protection throughout the life cycle of an object (whether it is a system, a hardware or software product, a service or a process). By an object’s life cycle we take to mean all the stages that it goes through, from its concept development until its removal, passing through the stages of development, production, operation, maintenance and withdrawal. Furthermore, it involves taking into account not only the application of measures for privacy protection in the early stages of the project, but also to consider all the business processes and practices that process associated data, thus achieving a true governance of personal data management by organisations.

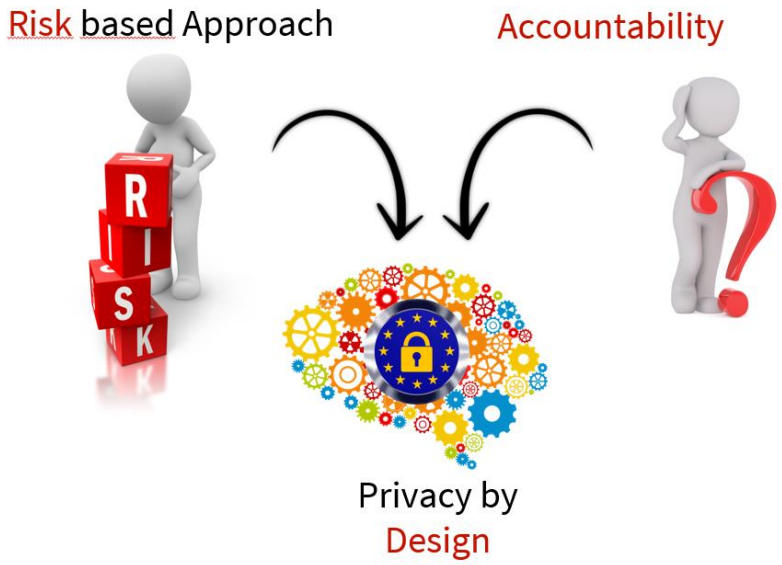


Figure 1 – Privacy by design and by default as the comprehensive approach to risk and accountability.

6 European Data Protection Supervisor (EDPS). *Opinion 5/2018 Preliminary Opinion on Privacy by design,* May 2018 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf “*’Privacy by Design’ or ‘Data Protection by Design’? For the purpose of this Opinion, we use the term “privacy by design” to designate the broad concept of technological measures for ensuring privacy as it has developed in the international debate over the last few decades. In contrast, we use the terms “data protection by design” and “data protection by default” to designate the specific legal obligations established by Article 25 of the GDPR.”*

7 European Union Agency for Cybersecurity (ENISA). *Privacy and Data Protection by Design – from policy to engineering*, Dec 2014 https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport *“The term “Privacy by Design”, or its variation “Data Protection by Design”, has been coined as a development method for privacy-friendly systems and services, thereby going beyond mere technical solutions and addressing organisational procedures and business models as well”.*

8 Information Commissioner’s Office (ICO). *Data protection by design and default*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ *“This concept is not new. Previously known as ‘privacy by design’, it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.”*

9 The new European regulations are a paradigm change in how the rights and freedoms of data subjects are guaranteed when it comes to the processing of their personal data. They have a risk-based focus, a dynamic and continually improving approach to better understand the risks to privacy and to determine the technical and organisational measures to be implemented, and from the perspective of accountability, understood as a continuous and traceable critical self-analysis of the data controller in fulfilling the duties assigned to them by law.

The final goal is to ensure that data protection is present from the early stages of development and not a layer added to a product or system. Privacy should be an integrated part of the nature of said product or service.

THE FOUNDATIONAL PRINCIPLES OF PRIVACY BY DESIGN

PbD is based on the conception of privacy as the default modus operandi within the business models of organisations, extending to information technology systems that support data processing, related business processes and practices, and physical and logical design of the channels of communication utilised. Privacy can be ensured by putting into practice the seven Foundational Principles defined by Ann Cavoukian [10] [11]:

1. Proactive not Reactive; Preventative not Remedial.

PbD involves anticipating events that affect privacy before they take place.

Any system, process or infrastructure that uses personal data must be conceived and designed from the beginning by identifying possible risks to the rights and freedoms of the data subjects and minimising them before they can cause actual damage. PbD policy is characterised by the adoption of proactive measures that anticipate threats, identify weaknesses in systems to neutralise or minimise risks instead of applying remedial measures to resolve security incidents once they have taken place. That is to say, PbD avoids "the policy of rectification" and anticipates the materialisation of risk.

This involves:

- A clear commitment by the organisation which must be promoted from the highest levels of the Administration.
- Developing a culture of commitment and continued improvement by all workers, as a policy means nothing until and unless it is translated into concrete actions that are fuelled by results.
- Defining and assigning concrete responsibilities so that each member of the organisation is clearly aware of their tasks with regard to privacy.
- Developing systematic methods based on indicators for the early detection of processes and practices that are deficient in guaranteeing privacy.

2. Privacy as the Default Setting

PbD seeks to provide the user with the highest levels of privacy possible given the state of the art, and especially, that personal data are automatically protected in any system, application, product or service.

The default setting must be established by design to be set to the level that provides the maximum possible privacy. If the subject does not modify the setting, their privacy is guaranteed and must remain intact, as it is integrated into the system and constitutes the default setting.

---

10 Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada. *Privacy by Design: The 7 Foundational Principles,* Jan 2011 https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

11 Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada. *Operationalizing Privacy by Design. A guide to implementing strong privacy practices,* Dec 2012 http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf

This principle, in practical terms, is based on data minimisation throughout the stages of processing: compilation, use, retention and distribution.

For this it is necessary to:

- Make data collection criteria as restricted as possible.
- Limit the use of personal data to the goals for which they were collected and ensure that there is a legitimate basis for processing.
- Restrict access to personal data to the parties involved in the processing in accordance with the "*need to know*" principle and according to the function behind the creation of differentiated access profiles.
- Define strict time limits for retention and to establish operational mechanisms that guarantee compliance.
- To create technological and procedural barriers to the unauthorised linking of independent sources of data.

3. Privacy Embedded into Design

Privacy must be an integral and inseparable part of the systems, applications, products and services, as well as the business practices and processes of an organisation. It is not an additional layer or module that is added to a pre-existing entity, rather it must be integrated into the group of non-functional requirements from the stages of concept development and design themselves.

To guarantee that privacy is accounted for in the early design stages, we must:

- Consider it as an essential requirement within the life cycle of systems and services, as well as in the design of organisational processes.
- Perform a risk analysis of the rights and freedoms of persons and when applicable, perform data protection impact assessments, as an integral part of any new processing initiative.
- Document all decisions that are adopted within the organisation from a "*privacy design thinking*" perspective.

4. Full Functionality: Positive-Sum, not Zero-Sum

It has traditionally been understood as privacy gained at the cost of other functionalities, thus presenting dichotomies such as privacy vs. usability, privacy vs. functionality, privacy vs. business benefit, and even privacy vs. security.

This is a contrived approach [12] and the goal must be to seek an optimal balance for a "win-win" search, with an open mind that accepts new solutions for fully functional, effective and efficient solutions both at business and privacy levels.

For this, from the first stages of concept development of products and services, an organisation must:

12These approaches were already discussed when concepts such as cybersecurity or quality control were introduced in organisations.

- Assume that different and legitimate interests may coexist: those of the organisation and those of the users to whom it provides services, and that it is necessary to identify, assess and balance them accordingly.
- Establish channels of communication for collaboration and consultation for the participants in order to comprehend and bring together multiple interests that, at first glance, may seem to diverge.
- If the proposed solutions threaten privacy, seek new solutions and alternatives to achieve the intended functionality and purposes, but never losing sight of the fact that risks to the user's privacy must be adequately managed.

5. End-to-End Security: Full Lifecycle Protection

Privacy is born in design, before the system is set in motion, and it must be guaranteed throughout the life cycle of the data.

Information security involves the confidentiality, integrity, availability and resilience of the systems that store it. Privacy also guarantees *unlinkability*, transparency and the data subject's capacity for intervention and control in the processing *(intervenability)*.

To integrate privacy throughout the stages of data processing, the different operations involved (collection, recording, classification, conservation, consultation, distribution, limitation, erasure, etc.) must be thoroughly analysed and in each case, the most adequate measures for information protection must be implemented, among which are:

- Early pseudonymisation or anonymisation techniques such as k-anonymity [13].
- Classification and organisation of data and processing operations based on access profiles.
- Default encryption so that the "natural" state of data when stolen or robbed is "illegible".
- The safe and guaranteed destruction of the information at the end of its life cycle.

6. Visibility and Transparency: Keep it Open

One of the keys to guaranteeing privacy is to be able to demonstrate it, verifying that the processing is in accordance with the given information.

Transparency in data processing is essential for demonstrating diligence and accountability before the Supervisory Authority and as a measure of trust before data subjects. As established in Recital 39 of the GDPR [14], it should be transparent to natural

13 Spanish Data Protection Agency (AEPD) – Unit of Evaluation and Technological Studies. *K-anonymity as a privacy measure,* June 2019 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad-en.pdf *K-anonymity is a property of anonymised data which makes it possible to quantify to what extent the anonymity of the subjects present in a dataset in which the identifiers have been removed is preserved. In other words, it is a measure of the risk that external agents can obtain information of a personal nature from anonymised data."*

14 General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

Promoting transparency and visibility requires the adoption of a series of measures such as:

- Making the privacy and data protection policies that govern the functioning of the organisation public.
- Developing and publishing concise, clear and comprehensible information clauses that are easily accessible and allow data subjects to understand the scope of the processing of their data, the risks that they may be exposed to, as well as how to exercise their rights regarding data protection.
- Although it is not compulsory for all controllers, making public or at least easily accessible for data subjects, the list of all the processing carried out in the organisation.
- Sharing the identity and contact details of the organisation's data controller
- Establishing accessible, simple and effective mechanisms of communication, compensation and complaints for the owners of the data.

7. Respect for User Privacy: Keep it User-Centric

Without forgetting the legitimate interests of the organisation with regard to the data processing it performs, the ultimate goal must be to guarantee the rights and freedoms of the users whose data is processed, and therefore, any adopted measure must focus towards guaranteeing their privacy. This involves designing "user-centric" processes, applications, products and services, anticipating their needs.

The user must play an active role in managing their data and in controlling what others do with it. Their inaction must not imply reduced privacy, referring back to one of the aforementioned principles which advocates a default privacy setting that offers the highest level of protection.

Designing processes, applications, products and services that are focused on guaranteeing the privacy of data subjects involves:

- Implementing privacy settings that are "robust" by default and where users are informed of the consequences to their privacy when established parameters are modified.
- Making available complete and suitable information that leads to an informed, free, specific and unambiguous consent that must be explicit in all cases that require it.
- Providing data subjects access to their data and to detailed information on the processing goals and communications carried out.
- Implementing efficient and effective mechanisms that allow data subjects to exercise their rights on data protection.

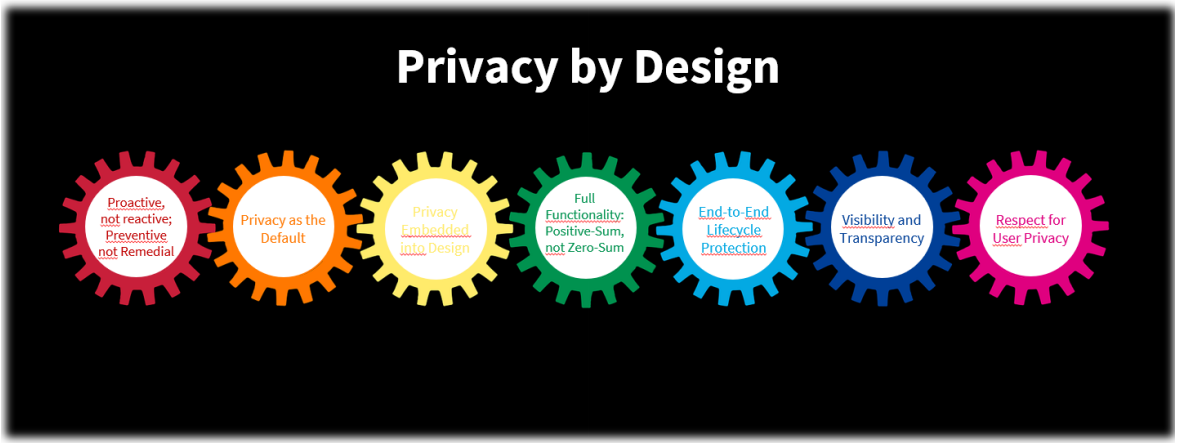


Figure 2 – The Foundational Principles of Privacy by Design

PARTIES BOUND BY DATA PROTECTION BY DESIGN

The GDPR establishes "data protection by design" as a legal requirement to be fulfilled. Article 83 [15] considers it a punishable offence[16] to not comply with this obligation and its correct application is one of the criteria for measuring the gravity of an infringement

As established by Article 25 of the GDPR [17], the obligation to implement data protection by design is applicable to all data controllers regardless of their size, the type of data processed or the nature of the processing. Concretely, it requires the appropriate technical and organisational measures to be implemented *"both at the time of the determination of the means for processing and at the time of the processing itself"*.

Although it is the data controller who is responsible for fulfilling this obligation in light of Recital 78 [18] and the Article 28 of the GDPR [19], data protection by design also involves other participants in the processing of personal data, such as service providers, product and application developers or device manufacturers. The data controller must encourage them to *"take into account the right to data protection when developing and designing such products, services and applications"* and when they must engage another processor for data processing, they must 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 brief, it is the data controller who, as part of their duties, must limit their selection of products and processors to those that can ensure the fulfilment of the GDPR

15Article 83. "General conditions for imposing administrative fines" - General Data Protection Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e6301-1-1

16On 4 July 2019 the Romanian Data Protection authority announced that it had fined the company UNICREDIT BANK S.A for failure to comply with Article 25.1 of the GDPR https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit&lang=en

17 Article 25. "Data protection by design and by default" - General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3126-1-1

18 General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

19 Article 28. "Processor" General Data Protection Regulation (EU) 2016/679https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3210-1-1

requirements and is especially obliged by law to guarantee data protection by design and by default.

This requirement is also applicable to joint controllers based on their respective responsibilities jointly assumed in determining the means and purposes of the processing.

Figure 3 – Privacy by design as the basis of the organisation's culture of privacy

(The figure has been designed using images from Freepik.com)

II. PRIVACY REQUIREMENTS OF SYSTEMS

To understand how personal data processing can affect the privacy of individuals is key to designing and developing trustworthy systems from the point of view of data protection.

In Article 5 [20], the GDPR lists the basic principles to be adhered to when processing data, such that these six principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality) joined to accountability become the core and the goal that every system, application, service or process must ensure in its design, apart from the functional requirements or requisites of the system itself.

PRIVACY AND SECURITY GOALS

Traditionally, designing secure and trustworthy systems has focused on analysing risks and responding to threats that affect the security goals that are more geared towards privacy:

- confidentiality, avoiding unauthorised access to systems,
- integrity, protecting them from unauthorised modifications of information and
- availability, guaranteeing that the data and systems are always available when necessary.

20 Article 5. "Principles relating to processing of personal data" General Data Protection Regulation (EU) 2016/679https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1873-1-1

Nevertheless, although unauthorised access to and modification of personal data can become a critical aspect that threatens the privacy of individuals, there are other risk factors that may surface during an authorised data processing [21] and that must be identified during risk assessment of the rights and freedoms of data subjects.

The loss of control in decision making, excessive data collection, re-identification, discrimination and/or stigmatisation of persons, biases in automated decisions, users' lack of comprehension of the scope and the risks of unlawful processing or profiling that is invasive or incorrect, are examples of risks to privacy that have a clear effect on the rights and freedoms of persons which cannot be managed by using only a traditional risk model that focuses exclusively on security goals.

Keeping in mind the aforementioned scenario and the possible risks to privacy associated with the planned and authorised functioning of systems that collect, use and reveal personal data, it is necessary to widen the scope of analysis to include not only risks derived from unauthorised processing, but also those that may arise from planned and authorised information processing.

To cover these possible risks, it is necessary to include three new privacy-focused protection goals within the frame of analysis [22][23], whose guarantee safeguards the processing principles established by the GDPR:

- **Unlinkability:** seeks to process data in such a manner that the personal data within a domain cannot be linked to the personal data in a different domain, or that establishing such a link involves a disproportionate amount of effort. This privacy goal minimises the risk of an unauthorised use of personal data and the creation of profiles by interconnecting data from different sets, establishing guarantees regarding the principles of purpose limitation, data minimisation and storage limitation.
- **Transparency:** seeks to clarify data processing such that the collection, processing and use of information can be understood and reproduced by all the parties involved and at any time during the processing. This privacy goal strives to delineate the processing context and make the information on the goals and the legal, technical and organisational conditions applicable to them available before, during and after data processing to all involved parties, both for the controller and the subject whose data are processed, thus minimising the risks to the principles of loyalty and transparency.
- **Intervenability:** ensures that it is possible for the parties involved in personal data processing, and especially the subjects whose data are processed, to intervene in the processing whenever necessary to apply corrective measures to the information processing. This objective is closely linked to the definition and implementation of procedures for exercising data protection rights, presenting complaints or revoking consent given by the data subjects, as well the mechanisms to guarantee the data controller's evaluation of the fulfilment

21 Sean Brooks, Michael Garcia, Naomi Lefkovitz, Susanne Lightman, Ellen Nadeau - National Institute of Standards and Technology (NIST). *NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems*, Jan 2017 https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

22 Harald Zwingelberg, Marit Hansen. 7th PrimeLife International Summer (PRIMELIFE), Sep 2011, Trento, Italy. pp.245-260. *Privacy Protection Goals and Their Implications for eID Systems*. https://hal.inria.fr/hal-01517607/document

23 Marit Hansen. 7th PrimeLife International Summer (PRIMELIFE), Sep 2011, Trento, Italy. pp.14-31. *Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals* https://hal.inria.fr/hal-01517612/document

and effectiveness of the obligations that are assigned to them by law, which gives greater respect to the principles of accuracy and accountability highlighted by the GDPR.

These three new protection goals together with existing security goals establish a global framework of protection in personal data processing and determine, by means of a risk assessment, other non-functional attributes or requirements that the system must satisfy and which become entry points to privacy design processes.

PRIVACY PROTECTION GOALS		
UNLINKABILITY	**TRANSPARENCY**	**CONTROL**
Data minimisation Storage limitation Integrity and confidentiality	Lawfulness, fairness and transparency Purpose limitation	Purpose limitation Accuracy Integrity and confidentiality Accountability

Table 2: Guarantees of the GDPR processing principles through privacy goals

Viewed from a global perspective, these six protection goals complement each other [24] and occasionally overlap, which is why for each data protection impact assessment (DPIA) [25] [26] that is made on prospective data processing, the possible priority of one goal over another must be evaluated and the necessary safeguards adopted.

III. PRIVACY ENGINEERING: PRIVACY ENGINEERING

Privacy Engineering [27] [28] is a systematic process with a risk-oriented focus whose goal is to translate into practical and operational terms, the principles of privacy by design (PbD) within the life cycle of information systems entrusted with personal data processing:

- specifying the privacy properties and functionalities that must be fulfilled by the system such that their design and implementation is possible (*privacy requirements definition*)
- designing the architecture and implementing system elements that cover the defined privacy requirements (*privacy design and development*)

24 Marit Hansen, Meiko Jensen, Martin Rost.. International Workshop on Privacy Engineering. *Protection Goals for Privacy Engineering*, May 2015 https://www.ieee-security.org/TC/SPW2015/IWPE/2.pdf

25 Spanish Data Protection Agency (AEPD). *Guía para la Evaluación de Impacto en la Protección de Datos personales,* Oct 2018 https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

26 Spanish Data Protection Agency (AEPD). *Template for Data Protection Impact Assessment Report (DPIA) for Public Administrations* https://www.aepd.es/media/guias/Modelo_Informe_PIA_V15_EN.rtf

27 This section deals with privacy engineering as a process within the design and development of an object. Privacy engineering may also be understood as a discipline, as described in: : https://www.aepd.es/en/blog/2019-09-11-ingenieria-privacidad.html

28 Massachusetts Institute of Technology Research & Engineering (MITRE) – Privacy Community of Practice (CoP). *Privacy Engineering Framework*, Jul 2014 https://www.mitre.org/sites/default/files/publications/14-2545-presentation-privacy-engineering-framework-july2014.pdf

- confirming that the defined privacy requirements have been correctly implemented and fulfil the expectations and needs of the stakeholders (*privacy verification and validation*)

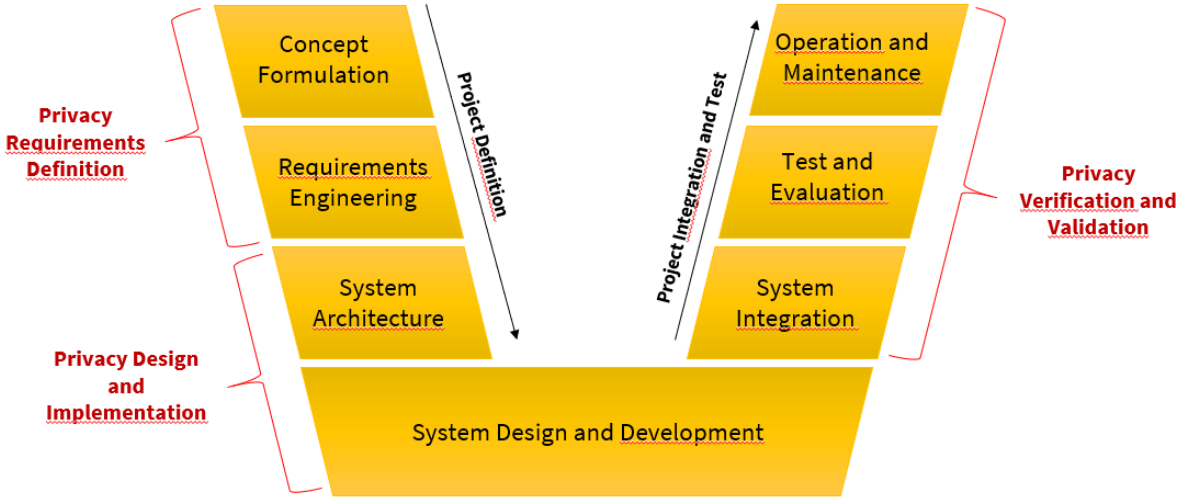


Figure 4 - Privacy Engineering [28]

The goal is to make privacy an integrated part of system design, such that privacy requirements are defined in terms of fully implementable properties and functionalities and any privacy risk that is identified is appropriately managed by the system in a proactive manner.

For this, a systematic and methodological approach is required, transferring the *what* of the concept development and analysis stages (identified privacy requirements) to the *how* of the design and implementation stages (concrete strategies and solutions), thus working sequentially at different levels of abstraction.

At the highest level, in the initial stages of concept development of the object and the analysis of its requirements, it is necessary to work with **privacy design strategies** [29], high-level general approaches meant to identify tactics to be followed during the different stages of data processing, in order to guarantee privacy goals and the fulfilment of data processing principles. The strategies provide an accessible model for engineers designing an object to define the privacy requirements identified during the analysis and requirement stages. Privacy design strategies serve as bridges between processing principles imposed by law and the implementation of privacy in concrete solutions. As we shall see later, they are centred on responding to actions that may present a threat to privacy in processing activities and their use is not exclusionary. On the contrary, it is desirable that all or most of them should be applied in order to make the developed object as *privacy-friendly* as possible.

Privacy design strategies are manifested, at the lowermost level, in **privacy design patterns** [29] . These are reusable solutions that are employed in the design stage and can be applied to solving common privacy problems that frequently crop up in product and systems development. The goal of these patterns is to create a catalogue of reusable solutions in the privacy design of systems and to standardise the design process.

29 Jaap-Henk Hoepman. Institute for Computing and Information Sciences (ICIS) – Radboud University Nijmegen, The Netherlands. *Privacy Design Strategies,* Oct 2012 https://www.cs.ru.nl/~jhh/publications/pdp.pdf

The association between patterns and strategies is not one-to-one, that is, the same pattern can implement and respond to multiple privacy strategies, providing solutions to different problems that appear throughout data processing activities.

Finally, at the lowermost level, the development stage, we find improved privacy technologies or **PETS (Privacy Enhancing Technologies)** that are used to implement privacy design patterns with a concrete technology [29]. The Commission, in its communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PET) defines them *as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system."*[30]. Similar to privacy design patterns and strategies, a single PET can be used to implement multiple design pattern solutions.

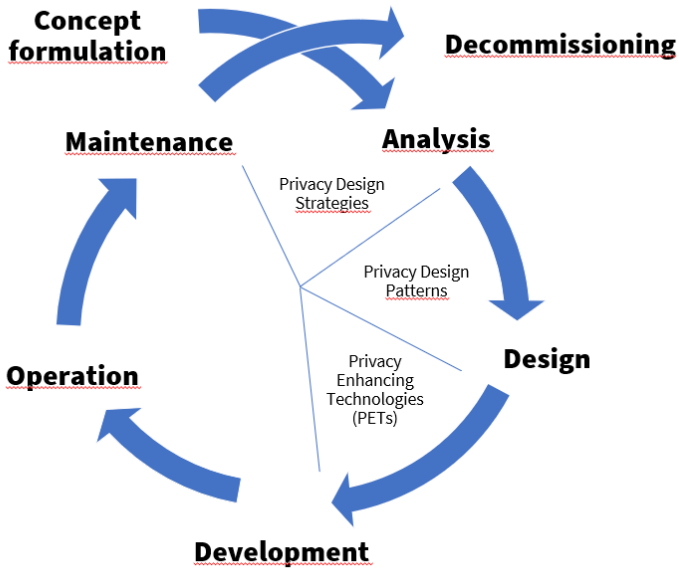


Figure 5 – Privacy strategies, patterns and techniques (PET) within a system's life cycle [31].

IV. PRIVACY DESIGN STRATEGIES

Current research identifies eight privacy design strategies [31][32] that are known as 'minimise', 'hide', 'separate', 'abstract', 'inform', 'control', 'enforce' and 'demonstrate'.

In turn, these eight strategies can be divided into two categories [31]: data-oriented strategies and process oriented strategies. The first includes the strategies of 'minimise', 'hide', 'separate' and 'abstract' and is of a more technical nature and focuses on *privacy-friendly* processing of collected data. The second category includes the strategies of

30 COM(2007)228 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on promoting data protection by Privacy Enhancing Technologies (PETs) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

31 Jaap-Henk Hoepman. *Privacy Design Strategies (The Little Blue Book)*, Mar 2019 https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

32 Michael Colesky, Jaap-Henk Hoepman – Digital Security. Radboud University Nijmegen, The Netherlands, Christiaan Hillen – Valori Security. Nieuwegein, The Netherlands. *A Critical Analysis of Privacy Design Strategies*, May 2016 https://www.researchgate.net/publication/305870977_A_Critical_Analysis_of_Privacy_Design_Strategies

'inform', 'control', 'enforce' and 'demonstrate'. These are of a more organisational nature and geared towards defining processes that implement responsible personal data management.

PRIVACY PROTECTION GOAL	DATA ORIENTED PRIVACY PROTECTION STRATEGIES	PROCESS ORIENTED PRIVACY PROTECTION STRATEGIES
UNLINKABILITY	MINIMISE, ABSTRACT, SEPARATE, HIDE	
CONTROL		CONTROL, ENFORCE, DEMONSTRATE
TRANSPARENCY		INFORM

Table 3 – Link between privacy goals and privacy design strategies

Although, depending on the context, certain strategies may be more applicable than others within a system's frame of development, these eight strategies, considered from the initial stages of concept development and analysis and jointly applied, permit the inclusion of safeguards and protection measures in data processing operations and procedures, making it possible for final results to take into account privacy requirements that guarantee the rights and freedoms of data subjects.

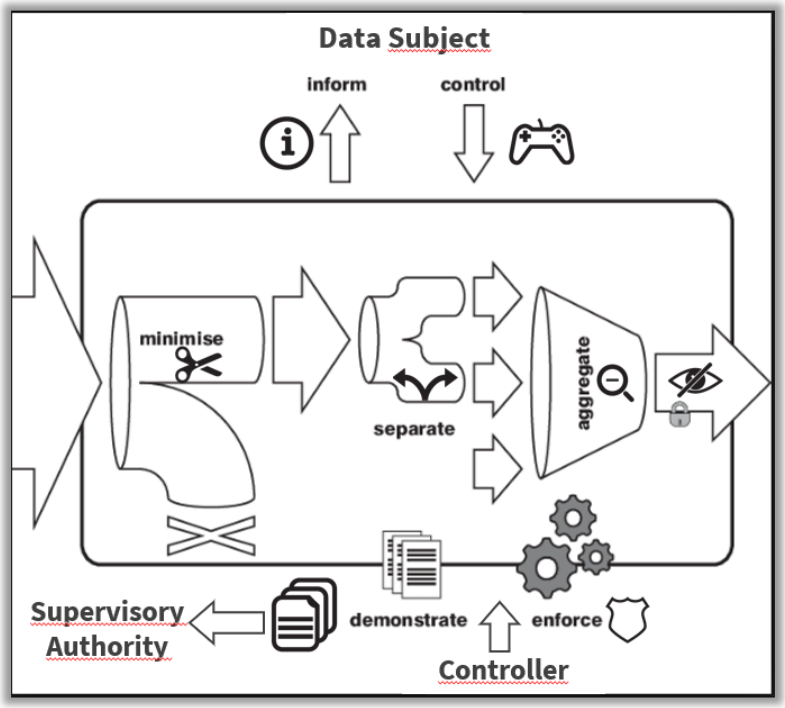


Figure 6 – Privacy Design Strategies

Minimise

The goal of this strategy is to collect and process the least amount of data possible, thus averting the processing of unnecessary data and limiting possible impacts on

privacy. This may be achieved by collecting data from fewer subjects (reducing the population size) or less data from subjects (reducing the volume of collected information), for which the following tactics may be used:

- **Select:** select only the sample of relevant individuals and the attributes required, with a conservative approach when establishing the selection criteria and processing only the data that satisfy the selection criteria (white list).
- **Exclude:** is the reverse of the earlier approach and consists of excluding beforehand subjects and attributes that are irrelevant to the processing (black list). In this case, an open attitude must be adopted, excluding as much information as possible unless their inclusion can be justified as being absolutely necessary for the intended goal.
- **Strip:** partially eliminate personal data as soon as they cease to be necessary, which requires establishing beforehand the storage period of each of the collected data, and to establish automatic deleting mechanisms when said period is over. In case the data are part of a record that has more information than is necessary, the value of the unnecessary fields can be modified to a prefixed default value.
- **Destroy:** completely delete personal data as soon as they cease to be relevant, ensuring that it is impossible to recover both the data and any backup copies.

It is also important to remember that only strictly necessary data must be communicated and shared, and in case of processing where new personal information is extrapolated, generated data that is not necessary to achieve the intended purpose must also be deleted.

Hide

This strategy focuses on limiting data observability by establishing necessary means to guarantee the protection of confidentiality and unlinkability. The following tactics are used to implement this strategy:

- **Restrict:** restrict access to personal data by setting limits through an access control policy that implements a *"need to know"* principle both in space (details and type of data accessed) and in time (processing stages).
- **Obfuscate:** make personal data unintelligible for those who are not authorised to consult it, using encryption techniques and hashing, both for storage operations as well as information transmission.
- **Dissociate:** eliminate the link between datasets that should be kept independent, as well as the identification attributes of data records to avert correlations between them, with special attention to metadata.
- **Mix:** Group together information on various subjects using generalisation and suppression techniques[33] to avoid correlations.

33 Spanish Data Protection Agency (AEPD) – Unit of Evaluation and Technological Studies. *K-anonymity as a privacy measure,* June 2019 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-kanonimidad-en.pdf

Separate

The goal of this strategy is to avoid, or at least minimise the risk that while processing, within one entity, different personal data of the same individual that are used in independent processes, can be combined to create a complete profile of the data subject. For this, it is necessary to maintain independent processing contexts that make it difficult to correlate datasets that should be unlinked. The following tactics help to implement a separation strategy:

- **Isolate:** collect and store personal data in different databases or applications that are independent, either logically or are executed on different physical systems, adopting additional measures to guarantee unlinkability, such as the programmed deletion of database indexes.
- **Distribute:** Spread out the collection and processing of different subsets of personal data corresponding to different types of processing over management and handling units that are physically independent within the system, and use different systems and applications to implement decentralised and distributed architectures that process the information locally whenever possible, instead of using centralised solutions with unified access which may depend on a single control unit.

Abstract

The idea behind this strategy is to limit the details of the processed personal data as much as possible. While the 'minimise' strategy makes a previous selection of the data to be collected, this strategy focuses on the degree of detail in which the data are processed and on their aggregation by using three tactics:

- **Summarise:** generalise the values of the attributes using value ranges or intervals, instead of a concrete field value.
- **Group:** aggregate information of a group of records into categories instead of using the detailed information on each of the subjects that belong to the group, by using average or general values.
- **Perturb:** use approximate values or modify the real data using some type of random noise instead of employing the exact value of the personal data.

For each data processing, it is necessary to study how the level of detail of the entered data affects the result, and what is the degree of precision necessary for effective processing. Especially, the length of time after the data was collected may affect their relevance, which is why it is useful to periodically review the stored information and apply these strategies [34].

Inform

This strategy implements the transparency goals and principles established by the Regulation and seeks to make data subjects fully aware of the processing of their data in a timely manner. Whenever processing is carried out, the subjects whose data is processed must be aware of what is being processed, to what end and which third parties

34We must remember that even an aggregated processing of records may pose a certain risk to privacy when a data subject may be classified as belonging to a particular group or profile (for example, persons with a specific illness or that have a concrete risk profile).

are given this information, in addition to all that is laid down in Articles 13 [35] and 14 [36] of the GDPR. Transparency with regard to this information is a basic requirement of privacy as it allows data subjects to make informed decisions on the processing and accordingly provide free, specific, informed and unambiguous consent. Any modification in processing regarding previously provided information must be communicated, including possible security breaches that may significantly affect the freedoms and liberties of data subjects. This strategy is based on the existence of privacy clauses that facilitate the global communication of this information to the data subjects, along with the use of the following tactics:

- **Supply:** provide data subjects with all the information required by the GDPR on what personal data is processed, how it is processed and why, by identifying the motive and goal. Details on data storage periods must be provided, as well as on the sharing of this data with third parties. Along with this information, which must be accessible and continually provided in order to promote an authentic transparency, it must also indicate who can be contacted by the data subjects and how, in order to ask questions on their privacy as well as their rights with regard to personal data protection.
- **Explain:** provide information on data processing in a concise, transparent, intelligible and easily accessible fashion in clear and simple language. To avoid dense, complex and unwieldy information policies, it is worth adopting a layered approach which first provides basic information at the same time and within the same data collection medium and makes additional detailed information available at a second level [37].
- **Notify:** inform data subjects of the processing when the data are not derived directly from them, at the time these have been obtained and within a maximum of one month, or if they are going to be used for communication with them, in the first message. Subjects must also be informed if their data is going to be transferred to third parties. Mechanisms to notify subjects of security breaches that may have happened and may pose a serious risk to their freedoms and rights must also be implemented, using clear and simple language to describe the nature of the breach.

Considering that data collection procedures are varied, the means of notification must be adapted to the circumstances of each method used including, additionally, the possible use of standardised icons that offer an overall view of the anticipated processing.

Control

This strategy is closed linked to the 'inform' strategy and it seeks to provide subjects with control over the collection, processing, use and transfer of their personal data by

35Article 13. "Information to be provided where personal data are collected from the data subject" - General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

36Article 14. "Information to be provided where personal data have not been obtained from the data subject" - General Data Protection Regulation (EU) 2016/679 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

37 Spanish Data Protection Agency, Catalan Data Protection Authority, Basque Data Protection Agency. *Guide for compliance on the duty to inform*, Jan 2017 https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

implementing mechanisms that allow them to exercise their rights of access to, rectification, erasure, objection, portability and restricting their data and its processing, as well as the right to give and withdraw consent or modify privacy options in applications and services. To implement these mechanisms, the following tactics are used:

- **Consent:** acquire the consent of data subjects, in cases without any other basis of legitimacy, and which must be given unambiguously, by demonstrating either a clear affirmative action which must be explicit in certain situations such as the processing of sensitive data, the adopting of certain automated decisions or in international transfers. Besides, the subject must be able to withdraw their consent at any time, by guaranteed mechanisms and procedures that make it as easy to withdraw consent as it is to give it.
- **Alert:** to provide real-time notification to the user when personal data is being collected, even when general information on the legal basis of the processing has been provided or even when the subject has already given their consent.
- **Choose:** to provide granular functionality [38] of applications and services, especially when it comes to basic functionality, without it being contingent on the user's consent to process personal data that is not required for execution.
- **Update:** implement mechanism that make it easy for users to or even lets them directly make revisions, updates and rectifications of the provided data for a specific processing, so that they are accurate and reflect reality.
- **Retract:** provide mechanisms for users to withdraw or ask for the deletion of their personal data provided to a controller for processing.

Technological advances that make it possible to continuously collect data also makes it possible for data to be easily managed by the data subjects through the implementation of privacy platforms where they can access, update, cancel and modify the selected privacy settings. These functions must be accounted for when designing an application.

Enforce

This strategy ensures that personal data processing is compatible with and respects the legal requirements and duties imposed by regulations. For this, it is necessary to define a privacy framework and an administrative structure that includes a data protection policy supported by the senior levels of management, as well as the roles and responsibilities that are entrusted with its compliance. Privacy culture must be an essential part of the organisation and all members must be participants. The following tactics may help to achieve this:

- **Create:** Specify a data protection policy that reflects internally the privacy clauses that are communicated to data subjects. The necessary structures must be created, and resources assigned to support this policy and ensure that the organisation's processing activities respect and comply with data protection regulations. A training and awareness plan must also be developed

38 Functions that require consent to for their legal use must be made available separately irrespective of whether they are the main goal of the object or not.

for all members that seeks to ensure a committed and responsible attitude as part of accountability.

- **Maintain:** to support the policy defined by establishing procedures and implementing the necessary technical and organisational measures. The existence of effective mechanisms and procedures must be reviewed in order to guarantee the exercise of rights, the handling and notifying of security incidents, adjusting possible processing activities to legal requirements and providing proof of compliance with the obligations imposed by regulations.
- **Uphold:** to ensure the compliance, effectiveness and efficiency of the privacy policy and the procedures, measures and controls implemented so that they account for all processing activities carried out and for the day to day activities of the organisation.

The figure of the Data Protection Officer plays an essential role in implementing this strategy, by assessing the controller and supervising the compliance with data protection regulations within the organisation. Implementing privacy management models such as that recently proposed by the ISO/IEC 27701:2019 [39] standard is also effective. It lists the requirements and provides directions for establishing, implementing, maintaining and continually improving a *Privacy Information Management System* (PIMS).

Demonstrate

This strategy goes one step further than the earlier strategy and its goal is that in accordance with Article 24 of the GDPR [40], the data controller must be able to demonstrate to data subjects as well the supervisory authorities that the applicable data protection policy is being adhered to, in addition to other legal requirements and obligations imposed by the Regulation. From a practical point of view, this implements the accountability demanded by the Regulation, based on a critical, continuous and traceable self-analysis of all decisions on data processing and ensuring authentic management of personal data within the organisation. The following tactics are used to carry out this strategy in order to ensure and demonstrate that the processing is in accordance with the Regulation:

- **Record:** document each and every decision taken even when they contradict each other, identifying who took the decision, when and why.
- **Audit:** carry out a systematic, independent and documented review of the degree of compliance with the data protection policy.
- **Report:** document audit results and any other incident regarding personal data processing operations and make them available to the supervisory authorities whenever required. In case of new data processing and if the result of the data protection impact evaluation shows that processing involves a high degree of risk to the rights and freedoms of the data subjects if the controller

39 Technical Committee ISO/IEC JTC 1 /SC 27. *ISO/IEC 27701:2019 Security techniques – Extension to ISP/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines,* August 2019 https://www.iso.org/standard/71670.html

40Article 24. "Responsibility of the controller" General Data Protection Regulation (EU) 2016/679https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3106-1-1

does not adopt measures to mitigate it, perform the prior consultation referred to in Article 36 [41] of the GDPR.

Performing a risk analysis and when applicable, a data protection impact assessment together with the documentation on decisions taken with regard to the results, is a good beginning to establish the privacy requirements that must be implemented in applications and systems as part of privacy by design, as well as to fully document how personal data is processed, and follow the principle of accountability. Other resources for demonstrating the controller's fulfilment of their obligations is their adherence to codes of conduct and certifications as optional instruments for implementing this strategy.

PRIVACY DESIGN STRATEGY		DESCRIPTION AND TACTICS	DESIGN CONTROLS AND PATTERNS
Data oriented strategies	Minimise	Limit the processing of personal data as much as possible. TACTICS: **select**, **exclude**, **strip** and **destroy**	Anonymisation Pseudonymisation Block correlation in federated identity management systems
	Hide	Avoid making personal data public or known TACTICS: **restrict**, **obfuscate**, **dissociate** and **mix**)	Encryption Mix networks Attribute Based Credentials
	Separate	Keep personal datasets separate. TACTICS: **isolate** and **distribute**	Anonymous black lists Homomorphic encryption Physical and logical separation
	Abstract	Limit the level of detail used in personal data processing as much as possible. TACTICS: **summarise**, **group** and **perturb**	Time-based group K-anonymity Added noise measurement obfuscation Dynamic location granularity Differential privacy

41Article 36. "Prior consultation" General Data Protection Regulation (EU) 2016/679https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3210-1-1

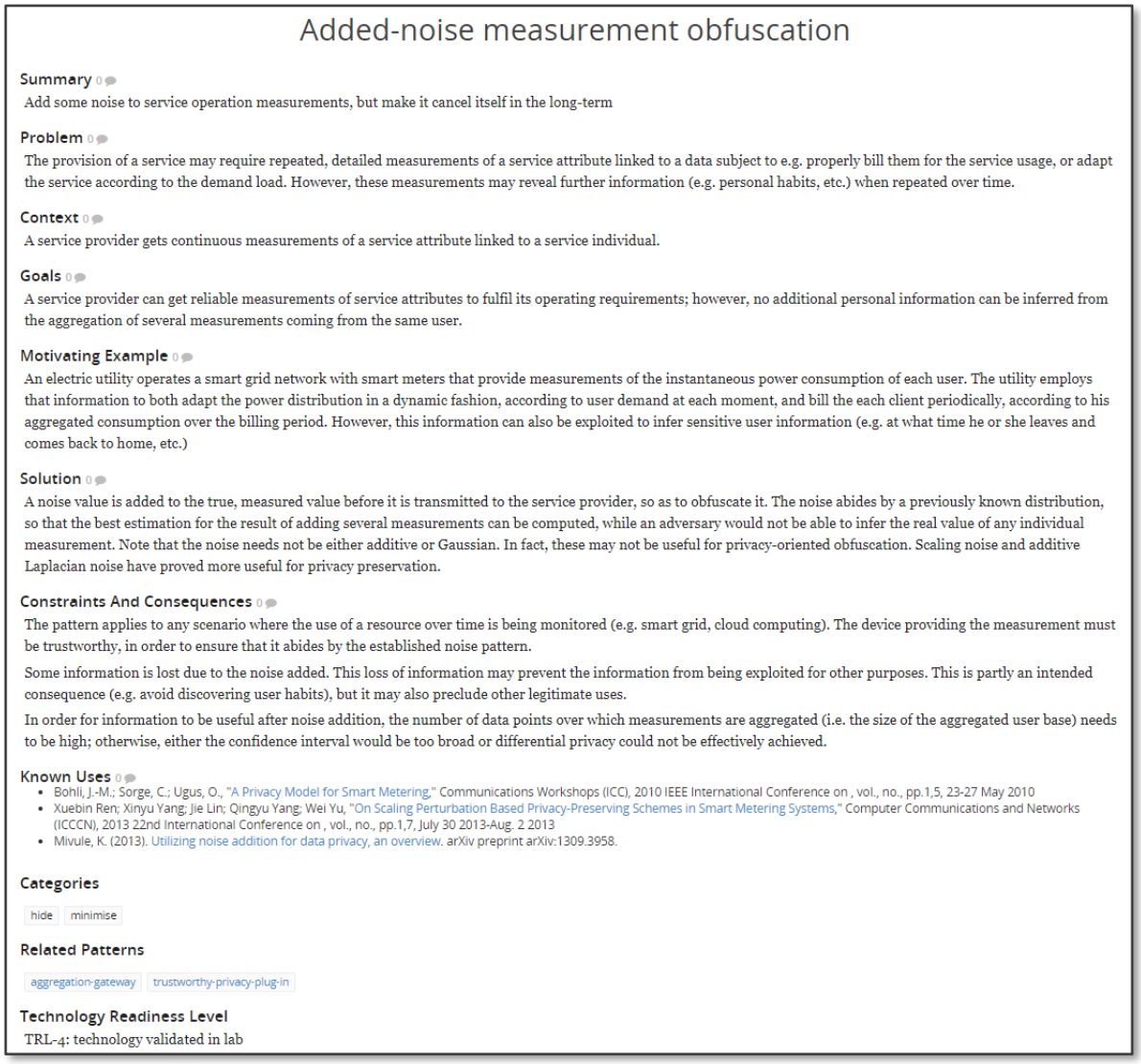
PRIVACY DESIGN STRATEGY		DESCRIPTION AND TACTICS	DESIGN CONTROLS AND PATTERNS
Process oriented strategies	Inform	Keep data subjects informed of the nature and conditions of processing. TACTICS: **supply**, **explain** and **notify**	Security breach notifications Dynamic visualisation of privacy policy Privacy icons Ambient notices
	Control	Provide data subjects with effective control over their personal data. TACTICS: **consent**, **alert**, **choose**, **update**, **retract**	Privacy dashboard Active broadcast of presence Credential selection Informed consent
	Enforce	Respect and promote the fulfilment of the obligations set by current regulations and the data protection policy itself. TACTICS: **create**, **maintain**, **uphold**	Privacy impact assessment in federated identity management solutions Access control. Obligation management Adherence to policies
	Demonstrate	To be able to demonstrate that data processing is respectful of privacy. TACTICS: **record**, **audit** and **report**.	Audit Logs

Table 4 – Privacy design strategies along with tactics and privacy patterns for implementation

V. PRIVACY DESIGN PATTERNS

Once the privacy goals and strategies to be included in the product, system, application or service as part of its definition are established, it is necessary to integrate them in its design. For this, privacy design patterns are used as reusable solutions to solve common and reiterated problems of privacy that repeatedly appear in a specific context during product and systems development.

Typically, the description of the design pattern contains at least its name, its purpose, its context of application, objectives, structure, implementation (relation to other patterns), the consequences of its application and known uses.



Added-noise measurement obfuscation

Summary

Add some noise to service operation measurements, but make it cancel itself in the long-term

Problem

The provision of a service may require repeated, detailed measurements of a service attribute linked to a data subject to e.g. properly bill them for the service usage, or adapt the service according to the demand load. However, these measurements may reveal further information (e.g. personal habits, etc.) when repeated over time.

Context

A service provider gets continuous measurements of a service attribute linked to a service individual.

Goals

A service provider can get reliable measurements of service attributes to fulfil its operating requirements; however, no additional personal information can be inferred from the aggregation of several measurements coming from the same user.

Motivating Example

An electric utility operates a smart grid network with smart meters that provide measurements of the instantaneous power consumption of each user. The utility employs that information to both adapt the power distribution in a dynamic fashion, according to user demand at each moment, and bill the each client periodically, according to his aggregated consumption over the billing period. However, this information can also be exploited to infer sensitive user information (e.g. at what time he or she leaves and comes back to home, etc.)

Solution

A noise value is added to the true, measured value before it is transmitted to the service provider, so as to obfuscate it. The noise abides by a previously known distribution, so that the best estimation for the result of adding several measurements can be computed, while an adversary would not be able to infer the real value of any individual measurement. Note that the noise needs not be either additive or Gaussian. In fact, these may not be useful for privacy-oriented obfuscation. Scaling noise and additive Laplacian noise have proved more useful for privacy preservation.

Constraints And Consequences

The pattern applies to any scenario where the use of a resource over time is being monitored (e.g. smart grid, cloud computing). The device providing the measurement must be trustworthy, in order to ensure that it abides by the established noise pattern.

Some information is lost due to the noise added. This loss of information may prevent the information from being exploited for other purposes. This is partly an intended consequence (e.g. avoid discovering user habits), but it may also preclude other legitimate uses.

In order for information to be useful after noise addition, the number of data points over which measurements are aggregated (i.e. the size of the aggregated user base) needs to be high; otherwise, either the confidence interval would be too broad or differential privacy could not be effectively achieved.

Known Uses

- Bohli, J.-M.; Sorge, C.; Ugus, O., "A Privacy Model for Smart Metering," Communications Workshops (ICC), 2010 IEEE International Conference on , vol., no., pp.1,5, 23-27 May 2010
- Xuebin Ren; Xinyu Yang; Jie Lin; Qingyu Yang; Wei Yu, "On Scaling Perturbation Based Privacy-Preserving Schemes in Smart Metering Systems," Computer Communications and Networks (ICCCN), 2013 22nd International Conference on , vol., no., pp.1,7, July 30 2013-Aug. 2 2013
- Mivule, K. (2013). Utilizing noise addition for data privacy, an overview. arXiv preprint arXiv:1309.3958.

Categories

hide minimise

Related Patterns

aggregation-gateway trustworthy-privacy-plug-in

Technology Readiness Level

TRL-4: technology validated in lab

Figure 7 – Example of privacy design pattern

As we have mentioned before, a design pattern can be used to implement more than one privacy strategy, and therefore these are not closed and exclusive solutions, rather we must look at privacy strategies from a combined and overall focus. For example, the '*Added noise measurement obfuscation*' pattern displayed in Figure 7, which adds noise to real measurements taken during the operation of a service so that additional information cannot be extrapolated, lets us implement 'abstract', 'hide' and 'minimise' strategies simultaneously.

DESIGN PATTERN CATALOGUES

There are different collections or catalogues of privacy design patterns where we can find comprehensive definitions, their goals and information on how to use them. The PRIPARE (*Preparing Industry to Privacy by design by supporting its Application in*

Research), [42] project funded by the European Union has developed a catalogue of 26 privacy design patterns [43].

Another similar initiative is the result of a project [44][45] carried out at the Vienna University of Economics and Business, which creates an interactive repository of solutions [46] which classifies 40 privacy design patterns by the 11 principles of protection defined by the ISO/IEC 29100:2011 [47] standard.

There is another collaborative initiative among various centres and universities that maintains a pattern catalogue [48] in order to operationalise legal requirements in specific solutions, standardise the language of privacy, document and compile common solutions to concrete problems and help systems and applications designers to identify privacy problems and respond to them.

Annex 1 lists these patterns in the form of a table with links to each entry; a total of 54 privacy design patterns that have been published on websites as a result of the aforementioned initiatives, with a brief summary of the purpose of each pattern and the privacy design strategy or strategies that they seek to implement.

VI. PRIVACY ENHANCING TECHNOLOGIES (PETS)

Once the prospective product, system, application or service's privacy strategies are defined and privacy patterns designed, we come to its implementation at the development stage by using a specific technological solution.

Privacy Enhancing Technologies or PETs are an organised and coherent group of ICT solutions that reduce privacy risks by implementing the previously defined strategies and patterns.

Due to the changing technological context, their effectiveness, in terms of privacy protection changes from one PET to another based on time, it being complicated to provide an updated classification and typology [49]. A PET may be an independent tool bought and installed by the end user on their personal computer or a complex information systems structure.

---

42 ATOS, Inria, Gradiant, Trilateral and UPM. *Privacy and Security by Design Methodology Handbook* , Dec 2015 http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

43 Online - *privacypatterns.eu - collecting patterns for better privacy* https://privacypatterns.eu/

44 Olha Drozd, Sabrina Kirrane, Sarah Spiekermann – Vienna University of Economics and Business. *Towards an Interactive Privacy Pattern Catalog*. 12th Symposium on Usable Privacy and Security (SOUPS 2016), Jun 2016, Denver CO. https://www.researchgate.net/publication/305811615_Towards_an_Interactive_Privacy_Pattern_Catalog

45 Olha Drozd – Vienna University of Economics and Business. *Privacy Pattern Catalog: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into Software Development Process*., Julio 2016, https://www.researchgate.net/publication/304995300_Privacy_Pattern_Catalogue_A_Tool_for_Integrating_Privacy_Principles_of_ISOIEC_29100_into_the_Software_Development_Process

46 Online – *privacypatterns* http://privacypatterns.wu.ac.at:8080/catalog/

47 Technical Committee ISO/IEC JTC 1 /SC 27. *ISO/IEC 29100:2011 Information Technology - Security techniques – Privacy Framework,* Dec 2011 https://www.iso.org/standard/45123.html

48 Online – *Privacy patterns* https://privacypatterns.org/

49 COM(2007)228 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on promoting data protection by Privacy Enhancing Technologies (PETs) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0228&from=EN

CLASSIFICATION OF PETs.

There are multiple classifications of PETs, most of them based on technical characteristics [50]. Another possible classification of these tools is that which is offered in this guide, and is based on the goals that they pursue [51]. Therefore, they shall be classified according to whether they are meant to protect privacy or manage it, thus maintaining a focus consistent with the classification of strategies that have been discussed earlier. The first group combines tools and technologies that actively protect privacy during the processing of personal data (for example, hiding personal data or eliminating the need for identification). The second group deals with tools and technologies that support procedures related to privacy management but do not actively operate on the data.

CATEGORY	SUBCATEGORY	DESCRIPTION
Privacy protection	Pseudonymisation tools	Allow transactions without asking for personal information
	Anonymisation products and services	Provide access to services without requiring the data subject' identification.
	Encryption tools	Protect documents and transactions from being viewed by third parties
	Filters and blockers	Avoid undesired emails and web content
	Anti-trackers	Eliminate the user's digital footprint
Privacy management	Information tools	Create and verify privacy policies
	Administrative tools	Manage user identity and permissions

Table 4 – One possible classification of PETs (*META Group Report*)

PET CATALOGUE

Similar to privacy design patterns, there is no single unified catalogue of PET tools and technologies, although there are different initiatives.

The Technology Analysis Division of the Office of the Privacy Commissioner of Canada has developed a general overview of PETs based on their functionality and given some concrete examples of solutions [52].

50 Lothar Fritsch, Norwegian Computing Center Report, No 1013. *State of the art of Privacy-enhancing Technology (PET),* Nov 2007 https://www.nr.no/publarchive?query=4589

51 Ministry of Science, Technology and Innovation, Denmark. *Privacy Enhancing Technologies – META Group Report v1.1,* Mar 2005 https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf

52 The Technology Analysis Division of the Office of the Privacy Commissioner. *Privacy Enhancing Technologies – A review of Tools and Techniques*, 2017 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

The Center for Internet and Society (CIS) at Stanford University's Law Faculty (California) have published a database of PET tools and technologies as an open-source wiki, so that users can have better control over their personal data [53].

In Europe, the European Data Protection Supervisor (EDPS) has developed IPEN *(Internet Privacy Engineering Network)*[54], in order to support developers in using privacy design patterns and other reusable blocks that aim to protect and improve privacy in a more efficient and effective manner.

In 2015, ENISA carried out the study *"Online privacy tools for the general public"* [55] which analysed PET tools for online privacy protection and compiled a list of web portals that promote the use of this technology. Although the tools suggested in the portals displayed in Table 5 are generally software applications aimed at end users to improve their personal data protection, their analysis and study is also useful for data controllers as examples of privacy requirements that must be included in services, products, an applications to be developed. If these solutions (secure communications encryption, anonymisers, anti-trackers, etc.) are serially integrated in systems, they will prevent end users from being left unprotected or having to add an unimplemented privacy layer to to a later installation of third party tools.

From this initial study, ENISA has published several reports [56][57][58][59] on the evolution of PET tools and the development of a methodology for comparing PET maturity. It is working on developing a platform provides support as well as a centralised repository on solutions that are best suited to intended privacy goals [60].

WEBSITE	ORGANISATION	URL	DESCRIPTION
Secure Messaging Scorecard	Electronic Frontier Foundation (EFF)	https://www.eff.org/deeplinks/2018/03/secure-messaging-more-secure-mess	A presentation and evaluation of secure messenger applications and tools, using a list of predefined criteria.
PRISM Break	Nylira (Peng Zhong)	https://prism-break.org/en/	A selection of tools to prevent tracking and

53 The Center for Internet and Society Stanford University. *Ciberlaw PET wiki*, https://cyberlaw.stanford.edu/wiki/index.php/PET

54 https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

55 European Union Agency for Cybersecurity (ENISA). *Online privacy tools for the general public*, Dec 2015 https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public/at_download/fullReport

56 European Union Agency for Cybersecurity (ENISA). *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, Mar 2016 https://www.enisa.europa.eu/publications/pets/at_download/fullReport

57 European Union Agency for Cybersecurity (ENISA). *PETs control matrix – A systematic approach for assessing online and mobile privacy tools*, Dec 2016 https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools/at_download/fullReport

58 European Union Agency for Cybersecurity (ENISA). *Privacy Enhancing Technologies: Evolution and State of the Art*, Mar 2017 https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art/at_download/fullReport

59 European Union Agency for Cybersecurity (ENISA). *A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment*, Mar 2018 https://www.enisa.europa.eu/publications/pets-maturity-tool/at_download/fullReport

60 UNIPI Workshop on Privacy Enhancing Technologies. Evgenia Nikolouzou - ENISA Data Security and Standardization Unit. *PETs Repository Community Building and Evaluation*, Nov 2018 https://www.enisa.europa.eu/events/personal-data-security/pets-maturity

WEBSITE	ORGANISATION	URL	DESCRIPTION
			mass surveillance, such as encryption tools, anonymisers, etc.
Security in-a-box	Tactical Technology Collective and Front Line Defenders	https://securityinabox.org/en/	A security website for general use which includes privacy protection tools, such as encryption tools.
EPIC Online Guide to Practical Privacy Tools	Electronic Privacy Information Center (EPIC)	https://www.epic.org/privacy/tools.html	It offers lists of privacy tools arranged according to different areas (browser add-ons, anonymisers, etc.).
The Ultimate Privacy Guide	BestVPN (4Choice Ltd)	https://proprivacy.com/guides/the-ultimate-privacy-guide	A security website for general users which offers lists of commercial VPNs. The privacy guide provides a list of tools classified according to area.
Free Software Directory	Free Software Foundation (FSF)	https://directory.fsf.org/wiki/Main_Page	A website for general users with information on security and privacy freeware, focusing mainly on encryption.
Privacytools.io	Privacytools.io	https://www.privacytools.io	It offers lists of tools to safeguard privacy such as VPNs, browser add-ons, etc.
Me & My Shadow	Tactical Technology Collective	https://myshadow.org	A website focusing mainly on digital footprints and online tracking. Offers recommendations on various relevant tools.

WEBSITE	ORGANISATION	URL	DESCRIPTION
Gizmo's Freeware	Gizmo's Freeware	http://www.techsupportalert.com/content/free-windows-desktop-software-security-list-privacy.htm	Website on general use freeware, which also proves a list of open-source privacy tools.
Best Privacy Tools	Best Privacy Tools	http://bestprivacytools.com/	It offers a list of privacy tools,. especially messenger apps, VPN, secure browsing, etc.
Internet Privacy Tools	Internet Privacy Tools	http://privacytools.freeservers.com	It offers a list of privacy tools,. especially email filters, browser-based encryption, etc.
Reset The Net Privacy Pack	Fight for the Future and Center for Rights	https://pack.resetthenet.org	It offers a list of free privacy tools and pertinent advice (for example, secure communications, anonymous browsing, etc.).

Table 5 – Websites that promote the use of online privacy tools
to the general public according to the ENISA study *Online privacy tools for the general public*

VII. CONCLUSIONS

Within a context where every day organisations and companies are developing services based on an intensive use of personal data and whose impact on privacy is visibly strengthened by the use of disruptive technologies, it becomes necessary to adopt effective and efficient technical and organisational measures that ensure that the rights and freedoms of persons are respected with regard to the processing of their personal data.

Ensuring privacy and establishing a framework of governance that guarantees personal data protection does not represent an obstacle to innovation. On the contrary, it offers advantages and opportunities for the different participants:

- for organisations it means improved efficiency, optimised processes, establishing a cost-reduction strategy and obtaining a competitive edge

- for the market it means the development of long-term sustainable economic models
- for society as a whole, it means being able to access the benefits of technological advances without having to compromise on individual freedoms and independence.

Ensuring privacy is indeed innovation in itself and it introduces a new technological discipline: privacy engineering.

The efficient and effective implementation of privacy principles requires them to be an integral part of the nature of products and services and to achieve this, they must be taken into account from the initial stages of concept development, design and development themselves as another part of the group of specifications, both functional and non-functional. This approach is known as Privacy by Design.

Privacy by design involves the use of a methodological focus centred on risk management and accountability that lets us determine privacy requirements by means of practices, procedures and tools. For this:

- The risk analysis will establish the specific objectives of data protection (unlinkability, transparency and intervenability) as well as security goals from the perspective of privacy (confidentiality, availability and integrity) that guarantee the basic principles established in Article 5 [61] of the GDPR.
- Next, the data-oriented and process-oriented privacy strategies that specify the requirements of each privacy goal are to be studied. These strategies are: 'minimise', 'hide', 'separate', 'abstract', 'inform', 'control', 'enforce' and 'demonstrate', and for each of them, the protection tactics that implement these strategies effectively are to be defined.
- In the design stage, the selected tactics shall be integrated by means of available solutions, that is to say, privacy design patterns that deal with common and reiterated problems, by accessing available catalogues, of which a selection is given in this document.
- Finally, in the development stage, these patterns shall be implemented. This implementation shall be carried out by development teams either by programming the code with the necessary functionality or whenever possible, by using existing ICT solutions, i.e., Privacy Enhancing Technologies.

In any case, data protection by design is the data controller's obligation and they must work to guarantee it by any possible means of development, acquisition or subcontracting of systems, products or services, without delegating completely to third parties (manufacturers and processors) the responsibility of implementing this principle.

As a part of fulfilling their duty, they must actively participate in privacy engineering tasks by defining the requirements that must be taken into account, continually monitoring its correct implementation and verifying its full operability before the system production, so that the privacy of individuals whose data are to be processed is guaranteed.

61 Article 5. "Principles relating to processing of personal data" General Data Protection Regulation (EU) 2016/679https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e1873-1-1

VIII. ANNEX 1: SELECTION OF PRIVACY DESIGN PATTERNS

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
Added Noise Measurement Obfuscation	Modifies the detailed measurements of use or any other attribute of a service by adding noise values that mask real data in order to avoid the deduction of patterns and behaviours by unauthorised third parties that may intercept the communication.	Abstract Hide Minimise
Aggregation in time	Consists of collecting data from different moments in time and processing information in an aggregated manner to protect privacy.	Abstract
Differential Privacy	This pattern modifies search results by adding new data (noise) randomly extracted from a distribution generated from original data, so that statistically said modification has an insignificant result on the results of the algorithm analysing the data, but it still maintains the privacy of the individuals.	Abstract
Trustworthy Privacy Plug-in	On many occasions, providing a service means taking detailed and repetitive measures that, upon a time-based evaluation, can reveal certain behaviours and put the subject's privacy at risk. This plug-in securely aggregates the detailed values of records at the user side for the intended goal, but hides the detailed disaggregated values.	Abstract
Dynamic Location Granularity	Uses k-anonymity to reduce precision of user location in location-based services (LBS), but maintains a balance with regard to the use of information required to provide the service.	Abstract Minimise
Aggregation Gateway	It implements homomorphic encryption, coding, aggregating and later decoding the processed information. By operating on encrypted information, it is possible to	Abstract Hide Separate

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
	process measurements taken at different moments in time on a user, but without extrapolating patterns of behaviour. It works with aggregated data without accessing individual information.	
Active Broadcast Of Presence	It allows the user to decide when they want to actively share information, especially location-based information. Information broadcast settings must not be holistically applied by default, and when unsure, clarification must always be sought.	Control
Obtaining Explicit Consent	For certain processes, the data controller must obtain the user's informed consent. Implementing this pattern ensures the display of a clear, concise and understandable notice before collecting data and beginning of the processing where, by using the service, the user consents to the processing of required data and is aware of the possible consequences. Complete details must be easily accessible so the user can decide whether to use the service or not.	Control
Private Links	In environments where the controller provides users with a content storage service, these may contain personal data. If the user wishes to share part of the content but in a limited manner, implementing this pattern allows them to send a private link to certain individuals, which provides access to this information, but without making it completely public.	Control
Sticky Policies	They are privacy policies that are automatically read and interpreted, and which accompany data shared with third parties to define their uses, limits and user preferences, thus improving the user's control over their personal data.	Control

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
Enable/Disable Functions	Data controllers often collect more data than is strictly necessary in order to provide additional functionalities related to the main processing goal. This pattern allows users to selectively choose the system functions that they want to use and provide only those data that are required to achieve this.	Control
Selective Access Control	Used in forums, social networks and content-based websites, it provides users with a tool to define the visibility of their posts and the content they share by defining the rules of access and privacy options settings.	Control
Selective Disclosure	Many products and services require the collection of a predetermined quantity of data which can occasionally be excessive, before the user can begin to use them. However, there are people who prefer the freedom to choose what type of information they share. This pattern recommends that services support selective disclosure, adopting the provided functionality to the data that the user is comfortable sharing.	Control
Privacy Dashboard	This pattern allows users to monitor and easily configure permissions and privacy preferences, by offering a central point where they can log in with their password and configure the settings that determine how their data is processed.	Control Inform
Access control	It establishes mechanisms to control access to information on a “need to know” basis, so that data is processed legally and by the authorised parties.	Enforce
Federated Privacy Impact Assesment	Identity management solutions allow the unlinking of functions related to authentication, authorisation and management of user attributes, as well as	Enforce

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
	providing the services accessed by these users, constituting a federated system of complex data flow and user identity sharing between different systems. These data flows are a risk and threat to privacy that must be analysed by means of a data protection impact assessment.	
Obligation Management	This pattern allows the obligations on data sharing, storage and processing to be shared and administered among different parties involved in the processing. This makes it possible to manage the defined privacy policy and user preferences, controlling the exercise of rights or the withdrawal of consent when the data have been communicated or shared by various controllers/processors.	Enforce
Auditing	Carry out periodic audits to examine the effectiveness of the mechanisms for fulfilment.	Demonstrate
Logging	Applying this pattern lets the controller demonstrate their compliance with the principle of accountability and that relevant data protection regulations have been duly implemented.	Demonstrate
Abridged terms and conditions	Its goal is for users to better understand the terms and conditions of a privacy policy (risks, rights, transfers, etc.) by presenting them in a concise and abbreviated fashion that is comprehensible to the user.	Inform
Ambient notice	Provides a discreet but clearly visible notice when personal data is being collected by a sensor system or an individual is being tracked, so that users can have real-time information, should they require it, on the use of their data and thus revoke consent. One alternative to this pattern is Asynchronous Notice.	Inform

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
Appropriate privacy feedback	In order to ensure that the data subject is aware of the scope of processing, a notification is sent in order to confirm that they understand what data is being collected, with whom it will be shared, how it will be used and the involved privacy risks, so that they can accordingly adjust their privacy settings before using the application or service.	Inform
Privacy icons	Privacy policies are often convoluted and difficult to understand. The use of icons, preferably standardised ones, allows sharing information quickly and helps text comprehension, making it a useful tool to increase transparency and the level of information offered by the privacy policy.	Inform
Awareness Feed	Make users aware of the potential consequences of data sharing, informing them of how visible the data is and what are the risks of sharing it. This lets them reconsider their privacy settings and take desired measures.	Inform
Data breach notifications pattern	This pattern ensures that if there is an unauthorised access and processing of personal data, it is detected and the supervisory authority and, when applicable, the affected users, are informed without undue delay.	Inform
Dynamic Privacy Policy Display	Not all environments are suitable for displaying an extensive privacy policy, however the subjects must still be able to consult detailed information regarding a specific point. This pattern provides additional information from the privacy policy in a contextual fashion (by clicking or hovering over a link) adjusted to the context or device where the consultation is made.	Inform

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
Unusual Activities	Many web services have weak authentication systems based on user id and passwords. It may be worthwhile to identify anomalous activities in the user account, alert the account holders and use multifactor authentication to protect systems from unauthorised access.	Inform
Impactful Information and Feedback	To prevent users from inadvertently sharing or publishing personal information, contextual privacy alerts that notify users based on the level of data disclosure may be used to alert them before the information is definitely published or shared.	Inform
Informed Secure Passwords	The usual means of authentication to access a service involves the use of user id and passwords. Due to the weakness of this security method, the controller must use this pattern to aid users in selecting a strong password and keep them informed of the importance of protecting and safeguarding it.	Inform
Layered Policy Design	Privacy policies tend to be long, complex and difficult to understand, which leads to users not reading them and consequently not being properly informed about data processing. This pattern suggests that controllers arrange privacy policies in nested levels of detail and include the most relevant aspects in a first level which then provides access to successive levels of detail where users can easily and comfortably find the relevant information.	Inform
Minimal Information Asymmetry	Information asymmetry is defined as a situation where one of the parties involved in a transaction has more or better information than the other. For there to be a relation of confidence between the controller and the data	Inform

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
	subject, the latter must be aware of and understand the nature of the processing. The use of this pattern involves minimising the quantity and type of data obtained from the user so that only those personal data that are required to attain desired goal are processed, and clear and concise policies that can be understood by the user are established, thus reducing the controller-subject inequality.	
Personal Data Table	Even in many cases where the controller is not legally obliged to do so, publishing data processing inventories fosters transparency and making them available to users lets them be informed of all the details of the processing: what data is collected, by whom, for what purpose, who is the data shared with, how long is the data stored, etc. Controller can even evaluate the possibility of giving access to raw data that is processed with different levels of detail.	Inform
Privacy Awareness Panel	Certain services and applications have an impact on users' privacy in ways that are not immediately evident to them. If they are not wholly aware of the consequences and act without full information, users may take incorrect decisions on how they use the services, even going so far as to assume that their actions are private and do not identify them. This pattern sends user reminders of who can view the content they publish, what is done with it and how they can be identified.	Inform
Privacy Colour Coding	Used in web environments where personal data is published, such as social networks, it lets users quickly and easily identify the privacy parameters of the shared content by colour-coding them.	Inform

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
Privacy Labels	Due to the effort required, users often do not consult the different privacy policies that they use, leading to disinformation on the possible consequences of giving consent and the configured privacy settings. Defining the basic aspects of processing in tabular format and using labels helps users to easily understand the nature and characteristics of the data processing.	Inform
Privacy Mirrors	Users are frequently unaware of the levels at which a system processes their personal data. Due to this, they sometimes accept the indefinite and uncontrolled use of data while others place greater restrictions than is necessary, leading to a loss of functionality. This pattern provides a high-level feedback of the data known to the system, what access it provides to others and what type of personal data may be deduced, thus providing an interface that allows users to consider their privacy in context and take informed decisions suited to their needs.	Inform
Privacy-Aware Network Client	Website privacy policies are often difficult to read and understand for data subjects. This pattern, which is applicable to web solutions, implements a privacy proxy that analyses and interprets policies and transforms them into a more readable format.	Inform
Informed Credential Selection	In processes that require authentication, to provide exact information to users on their personal data and the metadata obtained by the controller once the transaction is completed, and to implement a mechanism that allows choosing between different options, making for a more granular identification	Inform Control

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
	which provides more or less information as the user chooses.	
Anonymisation	To unlink the sensitive attributes of corresponding identifiers so that data subjects cannot be identified.	Minimise
Select before you collect	Its implementation limits personal data collection to only that which is required for specific goals and for which there exists a legal basis, thus preventing an indiscriminate collection of data and potential deviation in the data processing goal.	Minimise
Strip Metadata	Metadata generated during certain processes (EXIF data in photos, headers in emails or in other types of communication, time stamps, etc.) that are not necessary for the pursued goal and that, if made public, could pose a threat to privacy.	Minimise
Attribute Based Credentials	They allow the flexible and selective authentication of different properties or attributes of an entity or subject, but without disclosing their identity or additional information on them (zero-knowledge property)	Minimise Hide
Protection Against Tracking	This pattern prevents the use of cookies to track persons who visit a website by implementing mechanisms between the browser and the web server which delete them regularly (for example, when starting up the operating system) or disabling them permanently.	Minimise Hide

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
Mix Networks	Mix networks are routing protocols that make communications difficult to trace by using a chain of proxy servers that receive messages from multiple sources randomly, rearrange them and resend them randomly to the next destination (possibly another mix node). This breaks the link between the source of the request and the destination, making it more difficult for someone to eavesdrop on end-to-end communications. This pattern unlinks end-to-end communications making it difficult to establish correlations and track communications.	Hide
Onion routing	This pattern is a specific example of the Mix Networks pattern and it breaks the link between the sender and the receiver of a communication by encapsulating the data in different layers of encryption and thus restricting the knowledge of intermediate nodes on the path, achieving an anonymous routing.	Hide
Pseudonymisation	This pattern allows the processing of personal data but does not attribute it to a specific data subject without additional information, provided said additional information is maintained separately and is subject to technical and organisational measures to guarantee non-attribution.	Hide
Pseudonymous Identity	It is possible to interact anonymously in certain services such as forums by using pseudonyms that hide the real identity of the participants, so that the other users cannot link the pseudonym to the real identity of the data subject.	Hide
Pseudonymous Messaging	It is an improved online messaging service where a trusted third party exchanges the identifiers of the communicating parties by pseudonyms,	Hide

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
	thus maintaining anonymity at both ends.	
Use of Dummies	This pattern hides the actions of a user by adding other false interactions that cannot be distinguished from the real ones. It is used to protect privacy in location services by notifying different locations in order to hide the real location; in anonymous communications by sending false messages to false receivers to protect the user's profile; or in web searches to hide the user's real preferences.	Hide
Anonymity Set	It aggregates multiple occurrences of user records in a single dataset so that a concrete occurrence cannot be identified in isolation from the set, thus preventing actions such as tracking a subject's location, behaviour analysis and other operations that may endanger privacy.	Hide Abstract
Encryption with User-Managed Keys	It protects the confidentiality of personal information by encrypting message contents shared on the Internet or stored via a service provided by unreliable third parties by using encryption algorithms and using keys managed by the user, so that only those who possess the decryption key can recover the contents.	Hide Control
Identity Federation Do Not Track Pattern	Using this pattern in federated identity management systems prevents the correlation of requests between the end user and the service provider that may reach other participants in a federated identity system by means of an orchestrator that runs in the client environment.	Hide Minimise

NAME OF DESIGN PATTERN	OBJECTIVE AND PURPOSE	STRATEGY OR STRATEGIES SUPPORTED
User Data Confinement Pattern	It is customary to develop centralised systems where personal data processing is performed on a single system or entity in which the user is forced to confide and even share sensitive data. This pattern avoids centralised personal data processing by transferring a part of it to environments trusted by users (such as their own devices) allowing them to control the exact data that are shared with service providers.	Separate
Anonymous Reputation Based Black-Listing	To control users who make incorrect use of the service and prohibit them from accessing the service by creating black lists, but without being aware of their identity.	Separate Hide

IX. ANNEX 2: REGULATORY EXTRACTS

In the following section, the relevant articles and paragraphs Recitals of the General Data Protection Regulation (EU) 2016/679 that have been referenced throughout this guide and are related to the concept of privacy by design and by defect are included for the reader's comfort.

RECITAL 39

"Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."

RECITAL78

"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 the data subject 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."

ARTICLE 5 PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

"1. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

ARTICLE 13 INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE COLLECTED FROM THE DATA SUBJECT

"1. 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:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

ARTICLE 14 INFORMATION TO BE PROVIDED WHERE PERSONAL DATA HAVE NOT BEEN OBTAINED FROM THE DATA SUBJECT

"1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the categories of personal data concerned;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e) the right to lodge a complaint with a supervisory authority;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

a) the data subject already has the information;

the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

ARTICLE 24 RESPONSIBILITY OF THE CONTROLLER

"1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller."

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."

ARTICLE 28 PROCESSOR

"1. Where processing is to be carried out on behalf of a controller, the controller shall 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.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required pursuant to Article 32;

d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to

audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

ARTICLE 32 SECURITY OF PROCESSING

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."

ARTICLE 36 PRIOR CONSULTATION

"1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

b) the purposes and means of the intended processing;

c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

d) where applicable, the contact details of the data protection officer;

e) the data protection impact assessment provided for in Article 35; and

f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health."

ARTICLE 83 GENERAL CONDITIONS FOR IMPOSING ADMINISTRATIVE FINES

"1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

b) the obligations of the certification body pursuant to Articles 42 and 43;

c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

b) the data subjects' rights pursuant to Articles 12 to 22;

c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

d) any obligations pursuant to Member State law adopted under Chapter IX;

e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them."