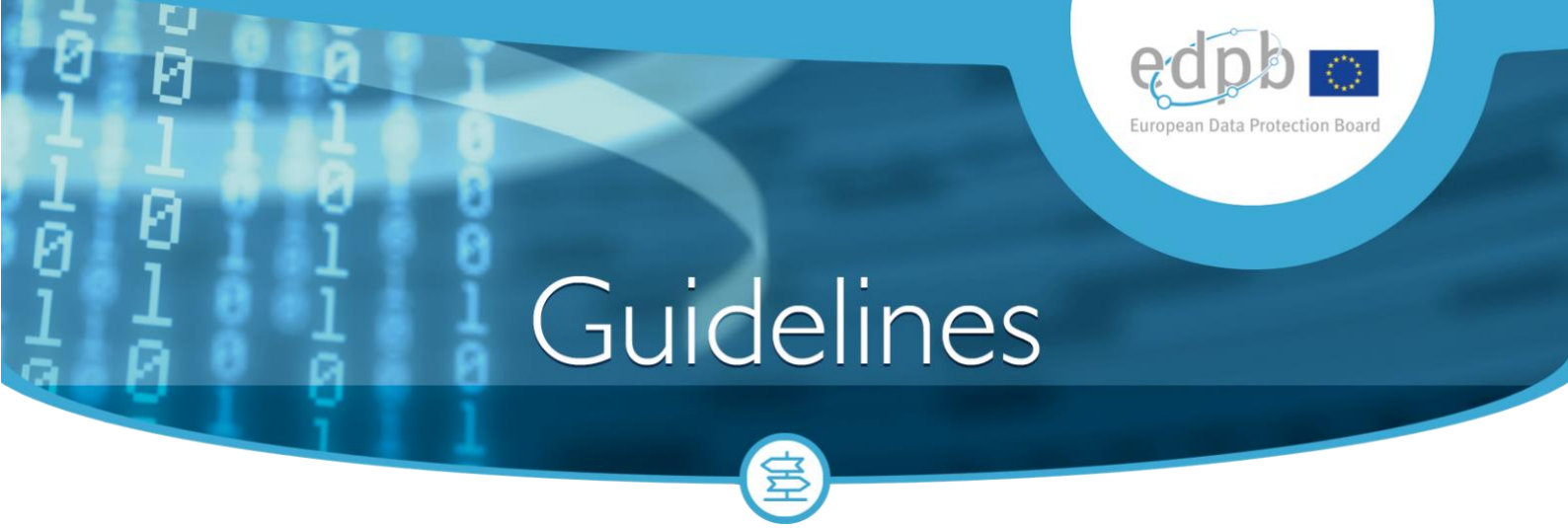

EDPB Plenary meeting, 12-13 November 2019

Guidelines 4/2019 on Article 25

Data Protection by Design and by Default

Adopted on 13 November 2019

Version history

Version 1.0	13 November 2019	Adoption of the Guidelines for public consultation

Table of contents

The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC], (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018, as last amended on 12 November 2019

HAS ADOPTED THE FOLLOWING GUIDELINES

Executive summary

These Guidelines give general guidance on the obligation of Data Protection by Design and by Default (henceforth "DPbDD") set forth in Art. 25 GDPR, where the core obligation is the *effective implementation* of the *data protection principles and data subjects' rights and freedoms by design and by default*. This requires that controllers implement appropriate technical and organisational measures and necessary safeguards, designed to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects. Controllers must be able to demonstrate the effectiveness of the implemented measures.

Data protection by design must be implemented both at the time of determining the means of processing and at the time of processing itself. It is at the time of determining the means of processing that controllers shall implement measures and safeguards designed to *effectively* implement the data protection principles. To ensure effective data protection at the time of processing, the controller must regularly review the effectiveness of the chosen measures and safeguards. The EDPB encourages early consideration of DPbDD when planning a new processing operation.

The Guidelines cover elements that controllers must take into account when designing the processing. The criteria of "state of the art" requires controllers to stay up to date on technological progress in order to secure continued *effective* implementation of the data protection principles. The "cost of implementation" requires the controller to take into account the cost and resources required for the *effective* implementation and continued maintenance of all of the data protection principles throughout the processing operation. Other elements controllers must take into account are the nature, scope, context and purpose of the processing, and the risk of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Furthermore, Article 25 requires data protection by default, meaning that by default, only personal data which are necessary for each specific purpose of the processing is processed. Thus, the default settings must be designed with data protection in mind. Default settings include both parameters that can be set by controllers and data subjects.

The Guidelines also contain practical guidance on how to effectively implement the data protection principles in Art. 5(1) GDPR, listing key design and default elements as well as practical cases for

illustration. The possibilities of certification in accordance with Article 42 and supervisory authorities' enforcement of Article 25 are also addressed.

In closing, the EDPB provides recommendations on how controllers, processors and technology providers can cooperation to achieve DPbDD and how DPbDD can be used as a competitive advantage.

1 SCOPE

1. The Guidelines focus on controllers' implementation of Data Protection by Design and Default (hereinafter "DPbDD") based on the obligation in Article 25 of the GDPR.[1] Other actors, such as processors and technology providers, who are not directly addressed in Article 25, may also find these Guidelines useful in creating GDPR-compliant products and services that enable controllers to fulfil their data protection obligations.[2] Recital 78 of the GDPR points out that DPbDD should be taken into consideration in the context of public tenders. Despite all controllers having the duty to integrate DPbDD into their processing activities, this provision fosters the adoption of the principles, where public administrations should lead by example.

2. The requirement is for controllers to have data protection designed into and as a default setting in the processing of personal data. The core of the provision is to ensure *effective* data protection both by *design* and by *default,* which means that controllers must be able to demonstrate that they have in place the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.

3. Chapter two of the Guidelines focuses on an interpretation of the requirements set forth by Article 25 and explores the legal obligations introduced by the provision. Operational examples on how to apply DPbDD in the context of specific data protection principles are provided in Chapter three.

4. The Guidelines also address the possibility to establish a certification mechanism to demonstrate compliance with Article 25 in Chapter four, as well as how the Article may be enforced by supervisory authorities in Chapter five. Finally, the Guidelines provide stakeholders with recommendations on how to successfully implement DPbDD.

2 ANALYSIS OF ARTICLE 25

5. The aim of this chapter is to explore and provide guidance on the requirements to data protection by *design* in Article 25(1) GDPR and to data protection by *default* in Article 25(2) GDPR respectively.
6. DPbDD is a requirement for all controllers, independent of their size, including small local associations and multinational companies alike. The EDPB brings to the reader's attention that the complexity of implementing DPbDD will vary based on the individual processing operation.

[1] The interpretations provided herein equally apply to Article 20 of Directive (EU) 2016/680, and Article 27 of Regulation 2018/1725.

[2] Recital 78 GDPR clearly states this need : "*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*".

2.1 Article 25(1) GDPR: Data protection by design

2.1.1 Controller's obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing

7. The controller shall (1) implement *appropriate* technical and organisational *measures* which are designed to implement the data protection principles and (2) integrate the *necessary safeguards* into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. Both appropriate measures and necessary safeguards are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing.

8. The term *measures* can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be *appropriate*, meaning that they must be suited to achieve the intended purpose, i.e. they must be fit to implement the data protection principles *effectively*[3] by reducing the risks of infringing the rights and freedoms of data subjects. The requirement to appropriateness is thus closely related to the requirement of effectiveness.

9. A technical or organisational measure can be anything from the use of advanced technical solutions to the basic training of personnel, for example on how to handle customer data. There is no requirement to the sophistication of a measure as long as it is appropriate for implementing the data protection principles effectively.

10. Safeguards act as a second tier to secure data subjects' rights and freedoms in the processing. Having implemented the data protection principles effectively means that the controller has integrated the safeguards that are necessary to ensure their effectiveness throughout the life-cycle of the personal data being processed. Enabling data subjects to intervene in the processing, providing automatic and repeated information about what personal data is being stored, or having a retention reminder in a data repository may be examples of necessary safeguards. Another may be implementation of a malware detection system on a computer network or storage system in addition to training employees about phishing and basic "cyber hygiene".

11. An example of a technical measure or safeguard is pseudonymization of personal data.[4] Such a measure may be used to implement a number of principles, such as the integrity and confidentiality and data minimisation.

2.1.2 Designed to implement the data protection principles in an effective manner and protecting data subjects' rights and freedoms

12. The *data protection principles* are in Article 5 GDPR (hereinafter "the principles"), the *data subjects' rights* are found in Articles 12 to 22, the *data subjects' freedoms* are found in Recitals 4 and in the EU Charter of Fundamental Rights (hereinafter "the rights"). It is essential for the controller to have an understanding of the meaning of *the principles* and *the rights.*

13. When implementing the appropriate technical and organisational measures, it is with respect to the effective implementation of each of the aforementioned principles, rights and freedoms that the measures and safeguards shall be *designed*.

[3] "Effectiveness" is addressed below in subchapter 2.1.2
[4] Defined in Article 4(5) GDPR, examples of which are hashing or encryption

Addressing effectiveness

14. Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must be able to **demonstrate** that they have implemented dedicated measures to protect these principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of data subjects. It is therefore not enough to implement generic measures solely to document DPbDD-compliance; each implemented measure must have an actual effect. This observation has two consequences.

15. First, it means that Article 25 does not oblige controllers to implement any prescribed technical and organizational measures or safeguards, as long as the chosen measures and safeguards are in fact appropriate at implementing data protection into the processing. It should be noted that the measures and safeguards should be designed to be robust and be able to be scaled up in accordance with any increase in risk of non-compliance with the principles.[5] Whether or not measures are DPbDD-compliant will therefore depend on the contexts of the particular processing in question and an assessment of the Article-25 elements that must be taken into account when determining the means of processing. The aforementioned elements are addressed below in pt. 2.1.3.

16. Second, controllers must be able to demonstrate that they have implemented measures and safeguards to achieve the desired effect in terms of data protection. To do so, the controller may determine appropriate key performance indicators to demonstrate compliance. Key performance indicators may include *metrics* to demonstrate the effectiveness of the measures in question. Metrics may be *quantitative*, such as level of risk, reduction of complaints, reduction of response time when data subjects exercise their rights; or *qualitative*, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively, controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.

2.1.3 Elements to be taken into account

17. Article 25 lists elements that the controller has to take into account when determining the measures of a specific processing operation. In the following, we will provide guidance on how to apply these elements in the design process.

"state of the art"

18. The concept of "state of the art" is present in various EU acquis, e.g. environmental protection and product safety. In the GDPR, reference to the "state of the art"[6] is made not only in Article 32, for

[5] "Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable." Article 29 Working Party. "Statement on the role of a risk-based approach in data protection legal frameworks". WP 218, 30 May 2014, p3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[6] See German Federal Constitutional Court's "Kalkar" decision in 1978: https://germanlawarchive.iuscomp.org/?p=67 may provide the foundation for a methodology for an objective definition of the concept. On that basis, the "state of the art" technology level would be identified between the "existing scientific knowledge and research" technology level and the more established "generally accepted rules of technology". The "state of the art" can hence be identified as the technology level of a service or technology or product that exists in the market and is most effective in achieving the objectives identified.

security measures,[7] but also in Article 25, thus extending this benchmark to all technical and organisational measures embedded in the processing.

19. In the context of Article 25, the reference to "state of the art" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, **to take account of the current progress in technology** that is available in the market. This means that controllers must have knowledge of and stay up to date on technological advances, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape.

20. The "state of the art" is a dynamic concept that cannot be statically defined at a fixed point in time, but must be assessed continuously in the context of technological progress. In the face of technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25.

21. The "state of the art" criterion does not only apply to technological measures, but also to organisational ones. Lack of adequate organisational measures can lower or even completely undermine the effectiveness of a chosen technology.

22. Existing standards and certifications may play a role in indicating the current "state of the art" within a field. Where such standards exist, controllers should take these into account in the design and implementation of data protection measures.

"cost of implementation"

23. When taking into account the cost of implementation, cost is not only meant in terms of money or economic advantage. Cost, in this context, refers to resources in general, including time and human resources. The EDPB reminds the reader that the *cost of implementing data protection* into the processing is a part of the *business costs*, and it is the former that is addressed in Article 25. Implementation and maintenance of the "state of the art" may also be of significance when considering the cost of implementation.

24. Keeping in mind the goal of effective implementation of the principles into the processing, the controller must take into account the cost of such implementation under the design process. This means that the controller shall plan for and expend the costs necessary for the effective implementation of all of the principles. In doing so, the controller may assess the risks to the rights and freedoms of data subjects that the processing entails and estimate the cost of implementing the appropriate measures into the processing to mitigate such risks to a level where the principles are effectively implemented. The controller must manage the costs to be able to effectively implement all of the principles. Incapacity to bear the costs is no excuse for non-compliance with the GDPR. At the same time, effective implementation of principles must not necessarily lead to higher costs. Spending more on technology does not necessarily lead to more effective implementation of the principles. In

[7] As an example of how to define the "state of the art" for IT security measures, see the guidelines to define the "state of the art" in IT security from TeleTrusT - IT Security Association Germany, published in English in cooperation with the European Union Agency for Network and Information Security (ENISA): "State of the art", www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/. Accessed 12 November 2019

some instances there may be simple low-cost solutions that can be just as or even more effective than their costly counterparts.

"nature, scope, context and purpose of processing"

25. Controllers must take into consideration factors such as the nature, scope, context and purpose of processing when determining the appropriate technical and organisational measures that effectively implement the principles into the processing.

26. The concept of these factors reflect the understanding of these terms as they appear in other provisions of the GDPR, such as Articles 24, 32 and 35. The difference in the context of Article 25 is that these factors must be taken into account when designing and integrating technical and organisational measures into the processing operations so that they effectively implement principles that meet GDPR obligations and protect the rights of data subjects.

27. In short, the concept of **nature** can be understood as the inherent characteristics of the processing. The **scope** refers to the size and range of the processing. The **context** relates to the circumstances of the processing, which may influence the expectations of the data subject, while the **purpose** pertains to the aims of the processing.

"risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"

28. The GDPR adopts a coherent risk based approach throughout its provisions, in Articles 24, 25, 32 and 35 with a view to identify appropriate technical and organisational measures to protect individuals, their personal data and comply with the requirements of the GDPR. The risk and the assessment criteria are the same: the assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights and freedoms), taking into account the same conditions (nature, scope, context and purposes of processing).

29. When performing the risk analysis for compliance with Articles 24 and 25 the controller has to identify the risks and determine their likelihood and severity.

30. The "EDPB Guidelines on Data Protection Impact Assessment (DPIA)",[8] which focus on determining whether a processing operation is likely to result in a high risk or not, also provide guidance on how to assess data protection risks and how to carry out a data protection risk assessment. These Guidelines may also be useful during the risk assessment in all the Articles mentioned above, including Article 25.

31. The risk based approach does not exclude the use of baselines, best practices and standards. These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing). Nevertheless, the obligation in Article 25 (as well as Articles 24, 32 and 35(7)(c) GDPR) to take into account "*risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*" remains. Therefore, controllers, although supported by such tools, must always carry out an assessment of data protection risks for the processing activity at hand and verify the effectiveness of the measures and safeguards proposed.

[8] Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". WP 248 rev.01, 4 October 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 - endorsed by the EDPB

2.1.4 Time aspect

At the time of the determination of the means for processing

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

33. The "*means of processing*" ranges from the abstract to the concrete detailed design elements of the processing, such as the architecture, procedures, protocols, layout and appearance.

34. The "*time of determination*" of such means is when the controller is in the process of determining which means to incorporate into the processing. It's in the process of making such decisions that the controller must assess the appropriate measures and safeguards to effectively implement the principles and rights of data subjects into the processing, and take into account elements such as the "state of the art", cost of implementation, nature, scope, context and purpose, and risks.

35. Controllers must be able to demonstrate that such assessments have been made for all of the means that are part of the processing.

36. Early consideration of DPbDD is crucial for a successful implementation of the principles. From a cost-benefit perspective, it would be in controllers' interest to take this into account sooner rather than later, as it could be challenging and costly to make changes to plans that have already been made and processing operations that have already been designed.

At the time of the processing itself

37. Once the processing has started the controller has a continued obligation to maintain DPbDD, i.e. continued effective implementation of the rights and principles. The nature, scope and context of processing operations may change over the course of processing, which means that the controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards.

38. This obligation also extends to any processing carried out by data processors. Processors' operations should be regularly reviewed and assessed to ensure that they enable continual compliance with the DPbDD principles and support the data controller's obligations in this respect.

2.2 Article 25(2): Data protection by default

Default

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

40. Hence, "data protection by default" refers to the choices made by a controller regarding any pre-existing configuration value or processing option that is assigned in a software application, computer program or device that has the effect of adjusting , in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

41. If there were no default settings, data subjects would be overwhelmed by options that he or she may not have the ability to grasp. Thus, in many cases, controllers must decide on these options on behalf

of the data subjects, and in doing so they have to ensure that only the personal data that is necessary to achieve the purpose of the processing is enabled. Here, controllers must rely on their assessment of the necessity of the processing with regards to the legal grounds of Article 6(1). If the controller uses third party software or off-the-shelf software, it is vital that functions that do not have coverage in the legal grounds or are not compatible with the intended purposes are switched off.

42. The values and processing options should be universal to all instances of the device, service or model, and should minimise the processing of personal data "out of the box".

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

Technical and organisational measures

44. "Technical and organisational measures" in the context of data protection by default is understood in the same way as discussed above in section 2.1.1, but applied specifically to the principle of data minimisation. The measures applied must be appropriate, meaning they must be suitable, adequate, relevant and limited to achieve the intended purpose.

45. The controller is required to predetermine for which specified, explicit and legitimate purposes the personal data is collected and processed.[9] The measures must by default be appropriate to ensure that only personal data which are necessary for each specific purpose of processing are being processed.

46. The EDPS guidelines to assess necessity and proportionality of measures that limit the right to data protection can be useful also to decide which data is necessary to process in order to achieve a specific purpose.[10] [11]

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

2.2.1 Required application of data protection by default

48. The aforementioned obligation to only process personal data which are necessary for each specific purpose applies to the following elements:

"amount of personal data collected"

49. In accordance with the principle of data minimisation, by default, only the amount of personal data that is *necessary* for the processing shall be processed.

50. "Amount" refers to quantitative as well as qualitative considerations. Controllers must consider both the volume of personal data, as well as the types, categories and level of detail of personal data

[9] Art. 5(1)(b), (c), (d), (e) GDPR

[10] EDPS. "Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection". 25 February 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[11] For more info on necessity, see Article 29 Working Party. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC". WP 217, 9 April 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

required for the processing purposes. Their design choices should take into account the increased risks to the principles of security, data minimisation and storage limitation when collecting large amounts of detailed personal data, and compare that against the reduced risks of collecting less finely detailed information about data subjects. In any case, the default setting must not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data is unnecessary or if detailed data isn't needed because less granular data is sufficient, then any surplus personal data shall not be collected.

"the extent of their processing"

51. Processing[12] operations performed on personal data shall be limited to what is necessary. As noted above, many processing operations may contribute to a processing purpose, but just because personal data is needed to fulfil a purpose does not mean that all types of, and frequencies of, processing operations may be carried out on the data. Controllers should also be careful not to extend the boundaries of "compatible purposes", and have in mind what processing will be within the reasonable expectations of data subjects.

"the period of their storage"

52. If personal data is not needed after its first processing, then it shall by default be deleted or anonymized. Any retention should be objectively justifiable and demonstrable by the data controller in an accountable way. Anonymization[13] of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of re-identification, is regularly assessed[14]. Further guidance is available in Opinion 05/2014 of the Art. 29 Working Party. For both deletion and anonymization process, the controller shall limit the retention period to what is strictly necessary. This obligation is directly related to the principle of storage limitation in Article 5(1)(e), and it is a requirement that storage limitation is default in the processing, i.e. the controller must have systematic procedures for data deletion embedded in the processing.

"their accessibility"

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

Article 25(2) further states that personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. The controller must by default limit accessibility and consult with the data subject before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons.

[12] According to art. 4(2) GDPR, this includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
[13] Article 29 Working Party. "Opinion 05/2014 on Anonymisation Techniques". WP 216, 10 April 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[14] Please see Art. 4(1) GDPR, Recital 26 GDPR, Article 29 Working Party "Opinion 05/2014 on Anonymisation Techniques". Please also see the subsection on "storage limitation" in section 3 of this document, referring to the need for the controller to ensure the effectiveness of the implemented anonymisation technique(s).

54. This provision applies, irrespective of the legal grounds for processing and of national legislation on freedom of information. Limiting intended or unintended dissemination is to limit possible situations where data subjects may experience a negative impact from the processing stemming from a lack of control over personal data.

55. Depending on the legal grounds for processing, the opportunity to intervene could either mean to ask for consent to make the personal data publicly accessible, or to provide information about the public accessibility in order to enable data subjects to exercise their rights in Articles 15 to 22. Either way, the extent of the public accessibility of the personal data should be made transparent to the data subject at the time of "intervention", which is the moment for the data subject's intervention.

56. Making personal data available to an indefinite number of persons may result in even further dissemination of the data than initially intended, this is particularly relevant in the context of the Internet and search engines. Even though the recipient controller is accountable for the legality of the further processing, there is still an obligation on the original controller not to make the personal data unduly accessible in the first place. This can be done using technical tools and protocols to limit search engines from indexing the data. For example a controller using a website to publish personal data can make use of a "no-robot-textfile" to give a message to search engines not to crawl the webpage. In this case, it is also vital that the controllers responsible for the search engines respect these protocols, although they aren't binding.

57. Even in the event that personal data is made available publicly with the permission and understanding of a data subject, it does not mean that any other controller with access to the personal data may freely process it themselves, for their own purposes – they must have a separate legal basis.[15]

3 IMPLEMENTING DATA PROTECTION PRINCIPLES IN THE PROCESSING OF PERSONAL DATA USING DATA PROTECTION BY DESIGN AND BY DEFAULT

58. In all stages of design of the processing activities, including tenders, outsourcing, development, support, maintenance, testing, storage, deletion, etc., the controller must take into account and consider the various elements of DPbDD which will be illustrated by the examples in this chapter, set in the context of implementing the principles.[16]

59. When presenting the examples of how to operationalize DPbDD we have made lists of **key DPbDD elements** for each of the principles. The examples, while highlighting the specific data protection principle in question, may overlap with other closely related principles as well.

[15] See Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland no. 931/13

[16] More examples can be found in Norwegian Data Protection Authority. "Software Development with Data Protection by Design and by Default". 28 November 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

Transparency[17]

60. The controller must be clear and open with the data subject from the start about how they will collect, use and share personal data. Transparency is about enabling data subjects to understand, and if necessary, make use of their rights in Articles 15 to 22. The principle is embedded in Articles 12, 13, 14 and 34. Measures and safeguards put in place to support the principle of transparency should also support the implementation of these Articles.

61. Key design and default elements may include:

- Clarity – Information shall be in clear and plain language, concise and intelligible.
- Semantics – Communication shall have a clear meaning to the audience in question.
- Accessibility - Information shall be easily accessible for the data subject.
- Contextual – Information shall be provided at the relevant time and in the appropriate form.
- Relevance – Information shall be relevant and applicable to the specific data subject.
- Universal design – Information shall be accessible to all, include use of machine readable languages to facilitate and automate readability and clarity.
- Comprehensible – Data subjects shall have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.
- Multi-channel – Information should be provided in different channels and media, beyond the textual, to increase the probability for the information to effectively reach the data subject

Example[18]

A controller is designing a privacy policy in order to comply with the requirements of transparency. The privacy policy cannot contain a lengthy bulk of information that is difficult for the average data subject to penetrate and understand, it must be written in clear and concise language and make it easy for the user of the website to understand how their personal data is processed. The controller therefore provides information in a multi-layered manner, where the most important points are highlighted. Drop-down menus and links to other pages are provided to further explain the concepts in the policy. The controller also makes sure that the information is provided in a multi-channel manner, providing video clips to explain the most important points of the information.

The privacy policy cannot be difficult for data subjects to access. The privacy policy is thus made available and visible on all internal web-pages of the site in question, so that the data subject is always only one click away from accessing the information. The information provided is also designed in accordance with the best practices and standards of universal design to make it accessible to all.

Moreover, necessary information must also be provided in the right context, at the appropriate time. This means, that generally a privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency. The controller therefore designs an information flow, presenting the data subject with relevant information within the appropriate contexts using e.g. informational snippets or pop-ups. For example, when asking the data subject to enter personal data,

[17] Elaboration on how to understand the concept of transparency can be found in Article 29 Working Party. "Guidelines on transparency under Regulation 2016/679". WP 260 rev.01, 11 April 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 - endorsed by the EDPB

[18] The French Data Protection Authority has published several examples illustrating best practices in informing users as well as other transparency principles: https://design.cnil.fr/en/

the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing.

Lawfulness

62. The controller shall identify a valid legal basis for the processing of personal data. Measures and safeguards put in place to support the principle of lawfulness should support the requirement to make sure that the whole processing lifecycle is in line with the relevant legal grounds of processing.

63. Key design and default elements may include:
- Relevance – The correct legal basis shall be applied to the processing
- Differentiation[19] – The controller shall differentiate between the legal basis used for each processing activity
- Specified purpose - The appropriate legal basis must be clearly connected to the specific purpose of processing.[20]
- Necessary – Processing must be necessary for the purpose to be lawful. It is an objective test which involves an objective assessment of realistic alternatives of achieving the purpose.
- Autonomy – The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data.
- Consent withdrawal – The processing shall facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid.
- Balancing of interests – Where legitimate interests is the legal basis, the controller must carry out an objectively weighted balancing of interests. There shall be measures and safeguards to mitigate the negative impact on the data subjects, and the controller should disclose their assessment of the balancing of interests.
- Predetermination – The legal basis shall be established before the processing takes place.
- Cessation – If the legal basis ceases to apply, the processing shall cease accordingly.
- Adjust – If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis.
- Default configurations – Processing must be limited to what the legal basis strictly gives grounds for.
- Allocation of responsibility – Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject

Example

A bank plans to offer a service to improve efficiency in the management of loan applications. The idea behind the service is that the bank, by requesting permission from the customer, can be able to retrieve data from public authorities about the customer. This may be, for example, tax data from the tax administration.

Initially, this personal data is necessary in order to take steps at the request of the data subject prior to entering into a contract.[21] However, this specific way of processing the personal data is not necessary for entering into a contract, because a loan may be granted without obtaining data directly

[19] EDPB. "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects". Version 2.0 , 8 October 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[20] See section on purpose limitation below

[21] See Article 6(1)(b) GDPR

from public authorities. The customer is able to enter into a contract by providing the information from the tax administration herself.

When implementing the principle of lawfulness, the controller realizes that they cannot use the "necessary for contract-"basis for the part of the processing that involves gathering personal data directly from the tax authorities. The fact that this specific processing presents a risk of the data subject becoming less involved in the processing of their data is also a relevant factor in assessing the lawfulness of the processing itself. The bank concludes that this part of the processing must rely on consent.

The bank therefore presents information about the processing on the online application platform in such a manner that makes it easy for data subjects to understand what processing is mandatory and what is optional. The processing options, by default, do not allow retrieval of data directly from other sources than the data subject herself, and the option for direct information retrieval is presented in a manner that does not deter the data subject from abstaining. Any consent given to collect data directly from other controllers is a temporary right of access to a specific set of information.

Any given consent is processed electronically in a documentable manner, and data subjects are presented with an easy way of controlling what they have consented to and to withdraw their consent.

The controller has assessed these DPbDD requirements beforehand and includes all of these criteria in their requirements specification for the tender to procure the platform. The controller is aware that if they do not include the DPbDD requirements in the tender, it may either be too late or a very costly process to implement data protection afterwards.

Fairness

64. Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes).

65. Key design and default elements may include:
    - Autonomy – Data subjects shall be granted the highest degree of autonomy possible with respect to control over their personal data.
    - Interaction – Data subjects must be able to communicate and exercise their rights with the controller.
    - Expectation – Processing should correspond with data subjects' expectations.
    - Non-discrimination – The controller shall not discriminate against data subjects.
    - Non-exploitation – The controller shall not exploit the needs or vulnerabilities of data subjects.
    - Consumer choice – The controller should not "lock in" their users. Whenever a service or a good is personalized or proprietary, it may create a lock-in to the service or good. If it is difficult for the data subject to change controllers due to this, which may not be fair.
    - Power balance – Asymmetric power balances shall be avoided or mitigated when possible. Controllers should not transfer the risks of the enterprise to the data subjects.
    - Respect rights and freedoms – The controller must respect the fundamental rights and freedoms of data subjects and implement appropriate measures and safeguards to not violate these rights and freedoms.

- Ethical – The controller should see the processing's wider impact on individuals' rights and dignity.
- Truthful – The controller must act as they declare to do, provide account for what they do and not mislead the data subjects.
- Human intervention – The controller must incorporate *qualified* human intervention that is capable of recovering biases that machines may create in relation to the right to not be subject to automated individual decision making in Article 22.
- Fair algorithms – Information shall be provided to data subjects about processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements.[22]

Example 1

A controller operates a search engine that processes mostly user-generated personal data. The controller benefits from having large amounts of personal data and being able to use that personal data for targeted advertisements. The controller therefore wishes to influence data subjects to allow extensive collection and use of their personal data.

When implementing the fairness principle, taking into account the nature, scope, context and purpose of the processing, the controller realizes that they cannot present the options in a way that nudges the data subject in the direction of allowing the controller to collect more personal data than if the options were presented in an equal and neutral way. This means that they cannot present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data, or make it difficult for the data subjects to adjust their privacy settings and limit the processing. The default options for the processing must be the least invasive, and the choice for further processing must be presented in a manner that does not deter the data subject from abstaining.

Example 2

Another controller processes personal data for the provision of a streaming service where users may choose between a regular subscription of standard quality and a premium subscription with higher quality. As part of the premium subscription, subscribers get prioritized customer service. With regard to the fairness principle, the prioritized customer service granted to premium subscribers cannot discriminate other data subjects' rights according to the GDPR Article 12. This means that although the premium subscribers get prioritized service, such prioritization cannot result in a lack of appropriate measures to respond to request from regular subscribers without undue delay and in any event within one month of receipt of the requests.

Prioritized customers may pay to get better service, but all data subjects shall have equal and indiscriminate access to enforce their rights and freedoms according to the GDPR.

[22] See recital 71 GDPR

Purpose Limitation[23]

66. The controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected.[24] The design of the processing should therefore be shaped by what is necessary to achieve the purposes. If any further processing is to take place, the controller must first make sure that this processing has purposes compatible with the original ones and design such processing accordingly. Whether a new purpose is compatible or not, shall be assessed according to the criteria in Article 6(4).

67. Key design and default elements may include:
    - Predetermination – The legitimate purposes must be determined before the design of the processing.
    - Specificity – The purposes must be specific to the processing and make it explicitly clear why personal data is being processed.
    - Purpose orientation – The purpose of processing should guide the design of the processing and set processing boundaries.
    - Necessity – The purpose determines what personal data is necessary for the processing.
    - Compatibility – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
    - Limit further processing – The controller should not connect datasets or perform any further processing for new incompatible purposes.
    - Review – The controller must regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.
    - Technical limitations of reuse – The controller should use technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.

Example

The controller processes personal data about its customers. The purpose of the processing is to fulfil a contract, i.e. to be able to deliver goods to the correct address and obtain payment. The personal data stored is the purchase history, name, address, e-mail address and telephone number.

The controller is considering buying a Customer Relationship Management (CRM) product that gathers all the customer data such as sales, marketing and customer service in one place. The product gives the opportunity of storing all phone calls, activities, documents, emails and marketing campaigns to get a 360-degree view of the customer. Ultimately the CRM automatically analyses the customers' purchasing power by using public information. The purpose of the analysis is to target the advertising better but is not a part of the original lawful purpose of the processing.

To be in line with the principle of purpose limitation, the controller requires the provider of the product to map the different processing activities using personal data with the purposes relevant for the controller. Another requirement is that the product shall be able to flag which kind of processing activities using personal data that is not in line with the legitimate purposes of the controller.

[23] The Article 29 Working Party provided guidance for the understanding of the principle of purpose limitation under Directive 95/46/EC. Although the Opinion is not adopted by the EDBP, it may still be relevant as the wording of the principle is the same under the GDPR. Article 29 Working Party. "Opinion 03/2013 on purpose limitation". WP 203, 2 April 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[24] Art. 5.1.b GDPR

After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are within the contractual purposes or if they need another legal ground for this processing. Alternatively the controller could choose to not make use of this functionality in the product.

Data Minimisation

68. Only personal data that is adequate, relevant and limited to what is **necessary** for the purpose shall be processed.[25] As a result, the controller has to predetermine which features and parameters of processing systems and their supporting functions are permissible. Data minimisation substantiates and operationalises the principle of necessity. In the further processing, the controller should periodically consider whether processed personal data still is adequate, relevant and necessary, or if the data shall be deleted or anonymized.

69. Controllers must first of all determine whether they even need to process personal data for their relevant purposes. They should verify whether technology, processes or procedures exist that could make the need to process personal data obsolete. Such verification could take place, in a particular point of the processing activity or even throughout the processing lifecycle. This is also consistent with Article 11.

70. Minimising can also refer to the degree of identification. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the controller shall anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights.

71. Key design and default elements may include:
    - Data avoidance - Avoid processing personal data altogether when this is possible for the relevant purpose.
    - Relevance – Personal data shall be relevant to the processing in question, and the controller shall be able to demonstrate this relevance.
    - Necessity – Each personal data element shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.
    - Limitation – Limit the amount of personal data collected to what is necessary for the purpose
    - Aggregation – Use aggregated data when possible.
    - Pseudonymization – Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately.
    - Anonymization and deletion – Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.
    - Data flow – The data flow shall be made efficient enough to not create more copies, or entry points for data collection than necessary.
    - "State of the art" – The controller should apply available and suitable technologies for data avoidance and minimisation.

Example 1

[25] Art. 5(1)(c) GDPR

A bookshop wants to add to their revenue by selling their books online. The bookshop owner wants to set up a standardised form for the ordering process. To prevent that customers don't fill out all the necessary information the bookshop owner makes all of the fields in the form a required field (if you don't fill out all the fields the customer can't place the order) using a standard contact form. The webshop owner initially uses a standard contact form, which asks the customer's date of birth, phone number and home address. However, not all the fields in the form are strictly necessary for the purpose of buying and delivering the books. The data subject's date of birth and phone number are not necessary for the purchase of the product. This means that these cannot be required fields in the web form to order the product. Moreover, there are situations where an address will not be necessary. For example, when ordering an eBook the customer can download the product and his or her address does not need to be processed by the webshop.

The webshop owner therefore decides to make two web forms: one for ordering books, with a field for the customer's address and one web form for ordering eBooks without a field for the customer's address.

Example 2

A public transportation company wishes to gather statistical information based on travellers' routes. This is useful for the purposes of making proper choices on changes in public transport schedules and proper routings of the trains. The passengers must pass their ticket through a reader every time they enter or exit a means of transport. Having carried out a risk assessment related to the rights and freedoms of passengers' regarding the collection of passengers' travel routes, the controller establishes that it is possible to identify the passengers based on the ticket identifier. Therefore, since it is not necessary for the purpose of optimizing the public transport schedules and routings of the trains, the controller does not store the ticket identifier. Once the trip is over, the controller only stores the individual travel routes so as to not be able to identify trips connected to a single ticket, but only retains information about separate travel routes.

In cases where there can be a risk of identifying a person solely by their travel route (this might be the case in remote areas) the controller implements measures to aggregate the travel route, such as cutting the beginning and the end of the route.

Example 3

A courier aims at assessing the effectiveness of its deliveries in terms of delivery times, workload scheduling and fuel consumption. In order to reach this goal, the courier has to process a number of personal data relating to both employees (drivers) and customers (addresses, items to be delivered, etc.). This processing operation entails risks of both monitoring employees, which requires specific legal safeguards, and tracking customers' habits through the knowledge of the delivered items over time. These risks can be significantly reduced with appropriate pseudonymization of employees and customers. In particular if pseudonymization keys are frequently rotated and macro areas are considered instead of detailed addresses, an effective data minimization is pursued, and the controller can solely focus on the delivery process and on the purpose of resource optimization, without crossing the threshold of monitoring individuals' (customers' or employees') behaviours.

Accuracy

72. Personal data shall be accurate and kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[26]

73. The requirements must be seen in relation to the risks and consequences of the concrete use of data. Inaccurate personal data could be a risk to the data subjects' rights and freedoms, for example when leading to a faulty diagnosis or wrongful treatment of a health protocol, or an incorrect image of a person can lead to decisions being made on the wrong basis either manually, using automated decision-making, or through artificial intelligence.

74. Key design and default elements may include:
    - Data source – Data sources should be reliable in terms of data accuracy.
    - Degree of accuracy – Each personal data element shall be as accurate as necessary for the specified purposes.
    - Measurably accurate - Reduce the number of false positives/negatives.
    - Verification – Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing.
    - Erasure/rectification – The controller must erase or rectify inaccurate data without delay.
    - Accumulated errors – Controllers must mitigate the effect of an accumulated error in the processing chain.
    - Access – Data subjects should be given an overview and easy access to personal data in order to control accuracy and rectify as needed.
    - Continued accuracy – Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.
    - Up to date – Personal data shall be updated if necessary for the purpose.
    - Data design - Use of technological and organisational design features to decrease inaccuracy, e.g. drop down lists with limited values, internal policies, and legal criteria.

Example 1

A bank wishes to use artificial intelligence (AI) to profile customers applying for bank loans as a basis for their decision making. When determining how their AI solutions should be developed, they are determining the means of processing and must consider data protection by design when choosing an AI from a vendor and when deciding on how to train the AI.

When determining how to train the AI, the controller must have accurate data to achieve precise results. Therefore, the controller must ensure that the data used to train the AI is accurate.

Granted they have the legal basis to train the AI using personal data from a large pool of their existing customers, the controller chooses a pool of customers that is representative of the population to also avoid bias.

Customer data is gathered from their own systems, gathering data about the existing loan customers' payment history, bank transactions, credit card debt, they conduct new credit checks, and they gather data from public registries that they have legal access to use.

[26] Art. 5(1)(d) GDPR

To ensure that the data used for AI training is as accurate as possible, the controller only collects data from data sources with correct and up-to date information.

Finally, the bank tests whether the AI is reliable and provides non-discriminatory results. When the AI is fully trained and operative, the bank uses the results as a part of the loan assessments, and will never rely solely on the AI to decide whether to grant loans.

The bank will also review the reliability of the results from the AI at regular intervals.

Example 2

The controller is a health institution looking to find methods to ensure the integrity and accuracy of personal data in their client registers.

In situations where two persons arrive at the institution at the same time and receive the same treatment, there is a risk of mistaking them if the only parameter to separate them is by name. To ensure accuracy, the controller needs a unique identifier for each person, and therefore more information than just the name of the client.

The institution uses several systems containing personal information of clients, and need to ensure that the information related to the client is correct, accurate and consistent in all the systems at any point in time. The institution has identified several risks that may arise if information is changed in one system but not another.

The controller decides to mitigate the risk by using a hashing technique that can be used to ensure integrity of data in the treatment journal. Immutable hash signatures are created for treatment journal records and the employee associated with them so that any changes can be recognized, correlated and traced if required.

Storage limitation

75. The controller must ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.[27] It is vital that the controller knows exactly what personal data the company processes and why. The purpose of the processing shall be the deciding criteria in how long personal data shall be stored.

76. Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure, the right to object and profiling.

77. Key design and default elements may include:
    - Deletion – The controller must have clear internal procedures for deletion
    - Automation – Deletion of certain personal data should be automated
    - Storage criteria – The controller must determine what data and length of storage is necessary for the purpose.
    - Enforcement of retention policies – The controller must enforce internal retention policies and conduct tests of whether the organization practices its policies.

[27] Art. 5(1)(c) GDPR

- Effectiveness of anonymization/deletion - The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible
- Disclose rationale – The controller must be able to justify why the period of storage is necessary for the purpose, and disclose the rationale behind the retention period
- Data flow – Controllers must beware of and seek to limit "temporary" storage of personal data
- Backups/logs – Controllers must determine which personal data and length of storage is necessary for back-ups and logs

Example

The controller collects personal data where the purpose of the processing is to administer a membership with the data subject, the personal data shall be deleted when the membership is terminated.

The controller makes an internal procedure for data retention and deletion. According to this, employees must manually delete personal data after the retention period ends. The employee follows the procedure to regularly delete and correct data from any devices, from backups, logs, e-mails and other relevant storage media.

To make deletion more effective, the controller instead implements an automatic system to delete data automatically and more regularly. The system is configured to follow the given procedure for data deletion which then occurs at a predefined regular interval to remove personal data from all of the company's storage media. The controller reviews and tests the retention policy regularly.

Integrity and confidentiality

78. The principle of security includes the well-known information security properties – confidentiality, integrity and availability – which strengthen data processing resilience. The security of personal data shall both prevent data breach incidents as well as facilitate the proper execution of data processing tasks, independent of individuals, to reinforce principles and allow individuals to exercise their rights in a seamless manner.

79. Recital 78 states that one of the DPbDD measures could consist of enabling the controller to *"create and improve security features"*. Along with other DPbDD measures, Recital 78 suggests a responsibility on the controllers to continually assess whether it is using the appropriate means of processing at all times and to assess whether the chosen measures actually counter the existing vulnerabilities. Furthermore, it should be understood that controllers must conduct regular reviews of the information security measures that surround and protect the personal data, and the procedure for handling data breaches.

80. Key design and default elements may include:
    - Information security management system (ISMS) – Have an operative means of managing policies and procedures for information security. For some controllers, this may be possible with the help of an ISMS.
    - Risk analysis – Assess the risks against the security of personal data and counter identified risks
    - Resilience – The processing should be robust enough to withstand changes, regulatory demands, incidents and cyber attacks
    - Access management – Only authorized personnel shall have access to the data necessary for their processing tasks

- Secure transfers – Transfers shall be secured against unauthorized access and changes
- Secure storage – Data storage shall be secure from unauthorized access and changes
- Backups/logs – Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control
- Special protection – Special categories of personal data should be protected with adequate measures and, when possible, be kept separated from the rest of the personal data
- Pseudonymization – Personal data and back-ups/logs should be pseudonymized as a security measure to minimize risks of potential data breaches, for example using hashing or encryption
- Security incident response management – Have in place routines and procedures to detect, handle, report and learn from data breaches
- Personal data breach handling - Integrate management of notification (to the supervisory authority) and information (to data subjects) obligations in the event of a data breach into security incident management procedures
- Maintenance and development – Regular review and test software to uncover vulnerabilities of the systems supporting the processing

Example

A controller wants to extract personal data from a medical database to a server in the company. The company has assessed the risk for routing the extracts to a server that is accessible to all of the company's employees as likely to be high for data subjects' rights and freedoms. There is only one department in the company who needs to process these patient data. The extracts will also have a high value to the company.

To regulate access and mitigate possible damage from malware, the company decides to segregate the network, and establish access controls to the server and the directory. In addition, they put up security monitoring and an intrusion detection and prevention system. The controller activates access control on the server and isolates it from routine use. An automated auditing system is put in place to monitor access and changes. Reporting and automated alerts are generated from this when certain events related to usage are configured. This security measure will ensure that all users have access on a need to know basis and with the appropriate access level. Inappropriate use can be quickly and easily recognised.

Some of the extracts have to be compared with new extracts, and must therefore be stored for three months. The controller decides to put them into separate directories and encrypt the stored extracts.

Handling the incident makes the system more robust, and reliable, both for the controller and the data subjects. The data controller understands that preventative and effective measures and safeguards should be built into all personal data processing undertakes now and in the future, and that doing so may help prevent future such data breach incidents.

The controller establishes these security measures both to ensure accuracy, integrity and confidentiality, but also to prevent malware spread by cyber-attacks to make the solution robust.

4 CERTIFICATION

81. According to Article 25(3), certification of data protection by design pursuant to Article 42 may be used as an element to demonstrate compliance with DPbDD. This means that where a controller has been awarded a certification, supervisory authorities will take this into account in their global assessment of compliance with the GDPR, specifically with regards to DPbDD. However, supervisory authorities

must still carry out independent assessments of DPbDD compliance based on the criteria set out in Chapter 2 of these Guidelines.

82. When a processing operation is certified according to Article 42, the elements that contribute to demonstrating compliance with Article 25(1) and (2) are the design processes, i.e. the process of determining the means of processing, the governance and organisational compliance approach to the processing operation, the selection of effective measures and safeguards in the context of the processing operation. The data protection certification criteria are determined by the certification bodies or certification scheme owners and then approved by the competent supervisory authority or by the EDPB in case of a European Data Protection Seal. For further information about certification mechanisms, we refer the reader to the EDPB Guideline on Certification.[28]

5 ENFORCEMENT OF ARTICLE 25 AND CONSEQUENCES

83. Supervisory authorities may assess compliance with Article 25 according to the procedures listed in Article 58. The corrective powers are specified in Article 58(2) and include the issuance of warnings, reprimands, orders to comply with data subjects' rights, limitations on or ban of processing, administrative fines, etc.

84. DPbDD is further a factor in determining the level of monetary sanctions for breaches of the GDPR, see Article 83(4).[29] [30]

6 CONCLUSIONS AND RECOMMENDATIONS

85. In an increasingly digital world, adherence to DPbDD requirements play a crucial part in promoting privacy and data protection in society. It is therefore essential that controllers take this responsibility seriously and implement the GDPR obligations when designing processing operations. Although not directly addressed in Article 25, processors and technology providers are also recognized as key enablers for DPbDD. They are in a position to identify the potential risks that the use of a system or service may entail, and are more likely to be up to date on technological developments. When processing on behalf of controllers, or providing solutions to controllers, technology providers should use their expertise and seize the opportunity to build trust and guide their customers in designing solutions that embed data protection into the processing. Processors and technology providers should also be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection.

Recommendations

86. It should be kept in mind when implementing Article 25 that the main design objective is the *effective implementation* of the principles and the rights of data subjects into the processing. In order to facilitate and enhance the adoption of DPbDD, we recommend the following:

---

[28] EDPB. "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation". Version 3.0, 4 June 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

[29] Article 83(2)(d) GDPR stipulates that in determining the imposition of fines for breach of the GDPR *"due regard" shall be taken of "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".*

[30] More information on fines can be found in Article 29 Working Party. "Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679". WP 253, 3 October 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - endorsed by the EDPB

- Controllers should think of DPbDD from the *initial stages* of planning a processing operation, even before the time of determination of the means of processing.
- A processing operation may be *certified* for DPbDD. Such a certification may provide an added value to a controller when choosing between different processing systems from technology providers. A certification seal may also guide data subjects in their choice between different goods and services, such as applications, software, systems, Internet of Things, including wearables and implants. Having a DPbDD-seal can therefore serve as a competitive advantage for both technology providers and controllers, and may even enhance data subjects' trust in the processing of their personal data. Where there is no certification, controllers should seek to have other *guarantees* that technology and service providers comply with the requirements of DPbDD.
- Technology providers should seek to support controllers in complying with DPbDD. Controllers, on the other hand, should not choose providers who do not propose systems enabling the controller to comply with Article 25, because controllers will be held accountable for the lack of implementation thereof.
- Technology providers should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures they have in place. Controllers should include this requirement as a contractual clause to make sure they are kept up to date.
- Controllers should take into account the cost element when choosing a provider or planning a technology or organisational practice or solution, and take into account the potential cost of monetary fines as a result of non-compliance with the GDPR. The controller should assess the factors contributing to the cost of a project, and find the actual costs of data protection, as opposed to the business costs of processing data. Ways to be more cost efficient are for example to simplify the organisation, leverage economies of scale or leverage economies of scope.
- Technology providers should keep in mind that Article 25 requires cost of implementation to be taken into account in the design process. This means that when developing a solution, technology providers should also take cost efficiency into account during the development of that solution and implement principles in an effective manner. Controllers should demand that their technology providers are transparent and demonstrate the costs of developing the solution.
- Controllers should always seek to effectively mitigate risk when observing data protection by design within the nature, scope and context of their processing operations, including when accounting for the related cost and state of the art of their chosen technical and organisational measures and safeguards.
- The EDPB encourages technology providers to take the opportunity to use DPbDD as a competitive advantage in the market.
- The EDPB recommends controllers to require that technology providers demonstrate accountability on how they have complied with DPbDD, for example by using key performance indicators to demonstrate the effectiveness of the measures and safeguards at implementing the principles.
- The EDPB emphasizes the need for a harmonized approach to implement principles in an effective manner and encourages associations or bodies preparing codes of conduct in accordance with Article 40 to also incorporate DPbDD.

- Controllers should be fair to data subjects and transparent on how they assess and demonstrate effective DPbDD implementation, in the same manner as controllers demonstrate compliance with the GDPR under the principle of accountability.

For the European Data Protection Board

The Chair

(Andrea Jelinek)