EDPB Guidelines 4/2019 on Article 25: Data Protection by Design and by Default
Comments on these Guidelines as of January 16, 2020.

Overall assessment of the Guidelines

The EDPB Guidelines 4/2019 on Article 25: Data Protection by Design and Default (DPbDD) (Guidelines) provide a very comprehensive overview on aspects of compliance with the data protection principles of the GDPR. We appreciate that the Guidelines make it clear that DPbDD is by no means limited solely to the security setup of data processing systems, but should also aim at implementing the data protection principles defined in Art. 5 GDPR both before processing commences and throughout its entire duration.

Hereby we acknowledge that the concept of DPbDD is very difficult to grasp in its entirety. It requires a radical shift in the mindset of everyone dealing with personal data – potentially even all service interactions – such that they adopt data protection thinking as a habit. Starting point and measure of this habit is a deep, ingrained understanding of the data protection principles such that the commercial considerations or functional considerations of any service are bounded by the thinking, rather than separate from the thinking. At the same time, the concepts within data protection are constructs that are not fully formed or agreed, let alone understood, so that embeddedness is difficult to achieve. The guidelines are a very good start to address this desire in the GDPR to make what is not even a business but a societal shift.

Consequently, a considerable part of the Guidelines is taken up by its explanation of the data protection principles. This makes for a good overview of the requirements for GDPR compliance in general, but specific emphasis on how these considerations influence the DESIGN of data processing and its tools and how aspects of DEFAULT approaches can become relevant are opaque to the layperson in most of its sections. Much more emphasis seems to have been placed on recommendations primarily related to other GDPR principles such as accountability (Art. 5(2)). We would have expected to instead find such specific recommendations on individual data protection principles in guidelines on those specific principles and we would indeed like to encourage the EDPB to draw up guidelines on the principle of “accountability”.

At this point we would like to emphasise that with respect to “appropriateness” as discussed in the Guidelines, we cannot endorse an interpretation of this term solely in close connection with “effectiveness”. The method by which measures are derived, in particular those arising as a result of balancing the cost of implementation with the nature, scope, context and purposes of processing as well as the risks—of varying likelihood and severity—to rights and freedoms of natural persons posed by processing, unambiguously indicates that “appropriateness” should instead be interpreted with the help of the idea of proportionality, as also clearly suggested by the EDPB Guidelines of 25th February 2019, (see in detail below).

Furthermore, we would like to encourage the EDPB to devote more detail to the roles of data controllers and data processors, the assessment of the state of the art and the definition of “ethical” in the context of DPbDD. Finally, sector-specific guidance on technical and organisational measures would be welcomed gladly by various communities, particularly those in the area of scientific research.

Recommendations

1. *Provide more concrete guidance on how to comply with the principles of data protection “by design” and “by default”, as related to different aspects of data processing and in connection with the principles defined in Art. 5 GDPR*

The current version of the Guidelines illustrates extensively how compliance with the data protection principles according to Art. 5 GDPR can be achieved in general. However, instead of explaining how to implement these principles by design and/or by default, the focus seems to be on a general interpretation of the Art. 5 principles themselves, with a strong focus on documentation and risk analysis related to the suitability of implementing measures. The approaches for "by design" or "by default" planning and realisation of data processing and the illustration of how to address the Art. 5 principles by design and by default are only implied (cf. the connection between data minimisation, Art. 5(1)c and Art. 25(1) GDPR).

In our view, the EDPB should provide – as far as possible at this stage of thinking – more information that highlights the factors that actually ensure that measures that are to be taken by the controller (and possibly by the processor, e.g. upon instructions by the controller) when implementing the Art. 5 principles duly respect the principles of data protection by design and by default.

2. *Provide clarification of potential measures as technical or as organisational*

Even though technical and organisational measures are strongly linked, when implementing the principles of data protection by design and by default there should be a clearer distinction as to which measures count as technical and which as organisational, as these measures will be implemented by different (accountable) entities, such as different actors within one organisation or multiple organisations and their actors all involved in the same data processing chain. Additionally, it would be very much appreciated if the EDPB would elaborate more on organisational measures such as policies, contractual clauses etc., as these measures get a raw deal in the current Guidelines (cf. Guideline 21). Furthermore, it would also be beneficial to create an even clearer separation between technical measures that are part of "by design" planning before the processing begins, and technical measures that are to be implemented throughout the processing to provide data protection "by default" (Guideline 63). One particularly useful example is that the principle of data protection "by design" partly anticipates the obligation of an impact assessment as defined by Art. 35 GDPR. This way, the GDPR extends its scope well before the time of the actual data processing.

3. *Provide sector-specific advice on realising different elements of data protection "by design" and "by default"*

Examples are always helpful to illustrate the implementation of data protection principles. This is particularly important when it comes to DPbDD, as the realisation of the principles of data protection by design and by default must strongly rely on technical and management staff and less on the involvement of legal experts.

Unfortunately, the Guidelines lack any breakdown of examples for different sectoral types of data processing. Because the GDPR provides various derogations from the main data protection rules and the majority of these derogations are related to specific data processing sectors, examples and use cases related to those sectors as regards DPbDD would be extremely helpful.

The examples currently provided predominately cover service provision. These examples have only limited validity for other sectors such as scientific research or personnel administration (e.g. Guidelines 43, 53-57). It was very much appreciated to find dedicated discussions of the implications of data protection principles for scientific research scenarios, such as those provided in the guidelines on consent and transparency, and we would like to emphasise the need for more sector-specific discussions and use-case examples in a revised version of the current Guidelines especially with regard to scientific research.

Our position is that this sector has to deal with particular questions such as those related to the relevance of the revision of data processing by ethics committees in the course of their authorisation for DPbDD. In any sector-specific discussion of DPbDD for health research, the role of ethics review prior to commencing data processing could be put forward as a potential safeguard. Ethics review aims to ensure respect for human rights is included in the design of research projects. We would like to refer to the European Data Protection Supervisor's Preliminary Opinion on data protection and scientific research and the discussion of the role of independent ethics committees on page 34 of this Opinion. It would be highly appreciated by many scientific communities carrying out health research if the EDPB could make a clarifying statement on this matter. This way, even though it lies beyond the scope of the opinion, insights into the notion of "ethical" processing could be gained, a notion which is increasingly coming to the fore when applying new technologies such as artificial intelligence in general and machine learning in particular.

4. *Clarify the relation between proportionality, appropriateness, necessity and effectiveness in the context of DPbDD*

As indicated in the introduction, we believe that the EDPB has taken the wrong approach in interpreting the term "appropriate" of Art. 25(1) GDPR and putting it on the level of "effectiveness". Firstly, the GDPR itself explicitly distinguishes between appropriateness and effectiveness (cf., for example, recital 74 GDPR). Secondly, according to Art. 25(1) GDPR, DPbDD has the AIM of EFFECTIVELY implementing data protection principles AND integrating the NECESSARY safeguards into the process to protect the rights of data subjects.

While the requirement of appropriateness as set out in Art. 25 GDPR is closely related to the requirement of effectiveness, as the EDPB rightly states (Guideline 8), they are not identical. In the context of DPbDD, "appropriate" seems to describe a balancing exercise between the criteria listed in Art. 25(1) sentence 1 GDPR, i.e. the nature, scope, context and purpose of the processing, the state of the art and the cost of implementation, alongside an even narrower risk analysis focusing on the assessment of the potential likelihood and severity of the impact of processing on the data subject. These analyses and their results are then taken into account when defining the measures to be taken. The risk analysis also includes a comprehensive balancing of goods and interests in the context of the rights and freedoms of the data subjects (cf. recital 75 GDPR). Taken altogether, the joint link between "appropriate" and "necessary" as indicated in Art. 25(1) GDPR to "proportionality" seems much stronger than the link between "appropriate" and "effective" (cf. also Art. 24(2) GDPR).

We would appreciate seeing the EDPB clarify the relationship between appropriateness, effectiveness and necessity in relation to both narrow and wide meanings of "proportionality" specifically within the context of DPbDD.

In addition, based on recital (77) GDPR, we would like to invite the EDPB to issue guidance on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what technical and organisational measures may be sufficient in such cases to address those risks (e.g. in the form of a use case in the current Guidelines). General assessments of this kind would enable controllers to assess their processing in the relevant individual context in a suitable manner.

5. *Create a more detailed overview of roles and responsibilities of data controllers and data processors by linking Art. 24 and Art. 28 GDPR*

The GDPR defines obligations for both data controllers and processors. Given the growing technological complexity of data processing, it is of the utmost importance that clear obligations are

created for both entities. The GDPR assigns certain obligations to both actors. This is understandable, as in many cases it will be the concrete processing situation that suggests which entity can be obliged to which task in order to provide compliance with data protection rules and principles, especially in the protection of data subjects' rights and freedoms.

The personal scope of application of Art. 25 GDPR is confined to the data controller. However, taking recital 78 GDPR into account, the assignment of obligations related to DPbDD in the Guidelines seems one-way, e.g. Guidelines 37-38. Even on a general and non-sectoral-specific level, and while following the spirit of the GDPR, it seems possible to establish a more streamlined assignment of obligations, as the particular field of DPbDD will inherently include processing activities whereby the processor—under the auspices of the controller—will play an increasingly important role. Thus, we suggest that the Guidelines take into account the ever-stronger role of the processor and the relationship between the controller and the processor in realising DPbDD—as is probably intended but not explicated in Guideline 38. This could be realized by connecting Art. 25(1) measures to those defined in Art. 28 et seq.

Additionally, it is not entirely clear how Art. 25 GDPR relates to Art. 24 GDPR (responsibility of the controller), as it contains partly divergent and partly overlapping factors for determining the appropriateness of measures. Further clarification of the relationship between both articles would be beneficial.

6. *Establish clear suggestions on how to assess the "state of the art"*

We welcome the suggestion to introduce clauses in compliance with state-of-the-art technical and organisational measures to ensure data protection by technology providers. We would appreciate if, in addition, further guidance could be given on criteria and/or methods for establishing said state of the art (Guidelines 8, 22), as the proposed definition is bogged down by vague legal terms (footnote 6 of the Guidelines). Particularly, although "state of the art" is often used in a technological context, as indicated in the guidelines, organisational measures may also be related to a certain state of the art, subject to change according to time as well as legal context and system. Because of this, further guidance is needed on the assessment of the state of the art for both technical and organisational measures.

Regina Becker
Edward Dove
Mark Fillietaz
Fruzsina Molnar-Gabor
Maria Pilar Nicolas
David Townend

for the European GDPR Network for Health-related Research