Opinion on the draft Guidelines 4/2019 of the European Data Protection Board

This opinion only reflects the views of its author.

On 20 November 2019, the European Data Protection Board published its draft Guidelines 4/2019[1] *"on Article 25 Data Protection by Design and by Default"* (hereinafter referred to as Draft Guidelines).

The Draft Guidelines focus on the interpretation of the requirements set forth by Article 25 of the GDPR and explores the legal obligations introduced by the provision. The Draft Guidelines also provide some operational examples on how to apply Data Protection by Design and by Default (DPbDD) in the context of specific data protection principles (i.e. the principles in Article 5 of the GDPR).

Despite some positive statements, the Draft Guidelines are, generally speaking, quite theoretical and less practical in terms of some still open questions concerning the consequences of application of the guidelines in case they become final.

I. Positive statements of the Draft Guidelines

1. Paragraphs 52 and 71 of the Draft Guidelines confirm that anonymisation can be considered as alternative to deletion (provided, of course, that the anonymisation criteria are meet).

2. Paragraph 55 of the Draft Guidelines gives an acceptable interpretation of the last sentence of Article 25(2)[2] instead of following a restrictive interpretation which could cause further difficulties and an administrative burden on data controllers.

II. Issues to be reconsidered

In addition to the above-mentioned positive statements of the Draft Guidelines, some other points should be further elaborated or reconsidered by the EDPB.

1. First of all, the Draft Guidelines are too theoretical (academic) and less practical. The text does not give, on one hand, too much guidance on the *practical implementation* of the theoretical explication. On other hand, however, the examples in Chapter 3 do not clarify whether they are

[1] See at the following link https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[2] *"In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*

only examples (best practices) or the only acceptable solutions for the situations described there. Some examples, namely the ones after points 61 and 74, contain statements that would function better in the body of the Draft Guidelines because of their nature[3] (i.e. if the said statements—especially the obligations that they impose—are of general nature and are to be applied in cases other than the example). The latter, i.e. moving some explanations from the footnotes to the main body of the Draft Guidelines, applies to the definition of the "state of the art" in footnote 6.

2. Further, the Draft Guidelines should clarify which of their provisions are mandatory ("must", "shall") and which ones are just recommendations ("should"). In some cases, this is not clear enough,[4] and if any statement/provision in the Draft Guidelines (e.g. use of "informational snippets or pop-ups"[5]) is mandatory, it may force a lot of data controllers to redesign their websites even if that redesigning would not be vital taken into account the concrete circumstances of a given data processing activity. In this regard, it should be taken into consideration that Article 25 of the GDPR does not specify any particular measure (just contains very general obligations) to be taken; the Draft Guidelines are, therefore, just one possible interpretation of Article 25, which is not (necessarily) confirmed by court decision(s). In sum, the provisions of the Draft Guidelines should be considered as recommendations rather than binding rules.

3. a) It comes from the theoretical nature of the Draft Guidelines that, although acknowledging that *"the complexity of implementing DPbDD will vary based on the individual processing operation"*[6], the Draft Guidelines follow a single approach without taking properly into account the differences either of data controllers (in terms of their size, i.e. SMEs or big companies) and their possibilities or of the different characteristics of different data processing activities.

Namely—although it is true, at least theoretically—that *"DPbDD is a requirement for all controllers, independent of their size, including small local associations and multinational companies alike"*, other requirements detailed in the Draft Guidelines (e.g. the *"controllers must have knowledge of and stay up to date on technological advances"*[7], and *"the controller shall plan for and expend the costs necessary for the effective implementation of all of the principles"*[8], as well as the fact that *"the processors and technology providers, who are not directly addressed in Article 25, [are also encouraged to take into consideration the Draft Guidelines when] creating*

[3] E.g. in Example after point 61 declares that *"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, the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing."*

[4] E.g. in points 42 and 61 the same issue ("universal design") are considered differently ("should" vs. "shall").

[5] See example after paragraph 61.

[6] See paragraph 6.

[7] See paragraph 19.

[8] See paragraph 24.

GDPR-compliant products and services that enable controllers to fulfil their data protection obligations"[9]) may result in that some companies, especially SMEs with modest resources (or public bodies with similarly modest resources)—in addition to the permanent risk of non-compliance with the GDPR as data controller—will either be excluded from some possibilities to act as data processor (simply because they will not be able to demonstrate that they "stay up to date on technological advances") or the responsibility for compliance will be transferred to the "technology providers" (software or application developers).

b) The Draft Guidelines should elaborate better what "stay up to date on technological advances" means. Does it mean that data controllers must always have the latest version of the software, application they use irrespective of whether the current and supported version does not represent any privacy risk? (For example, does a company have to upgrade from Windows 8.1 to Windows 10 just because the latter has been released?) Or is it enough if the data controller has only the latest update of the supported software/application (i.e. for example the latest updates of Windows 8.1)? Or—taken into account that *"the complexity of implementing DPbDD var[ies] based on the individual processing operation"*—even an unsupported, out-of-date software/application can be accepted under certain circumstances (e.g. without violating the GDPR, may the owner of a small chandlery use his PC still running Windows XP in offline mode with an also offline database of its customers?)? The Draft Guidelines should, therefore, clarify *how* other criteria established in the Draft Guidelines (e.g. in Paragraphs 25-27 and 28-31) affect the two main criteria (i.e. state-of-art and cost).[10]

III. Other remarks

1. a) The Draft Guidelines—as many other previous opinions, guidelines, etc. of the WP29 and the EDPB—still insist on their very strange interpretation of contractual relationship (which interpretation runs counter the age-old logic and rules of civil law).[11] One of its manifestation is paragraph 41 of the Draft Guidelines, where defaults settings are considered as done *"on behalf of the data subjects"*. In my view, defaults settings must be set because of the provisions of the law (i.e. default settings are obligations imposed by law rather than action on behalf of unknown persons).

b) The example after paragraph 77 also ignores the age-old institution of the statute of limitations and the necessary data processing accruing from a legal relationship even after termination.

[9] See paragraph 1.

[10] From the Draft Guidelines one can learn that these criteria affect the implementation of Article 25, but one cannot learn "how".

[11] It is despite the fact that the EDPB was warned and the right interpretation was explained by many in the course of public consultation on Draft 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.

2. a) The example after paragraph 63. is wrong (i.e. if a bank could develop a data processing process to obtain tax data directly from tax administration in the course of evaluation of a loan request): it is very unlikely that—knowing that tax secret is one of the most sensitive private information—tax administration would grant a bank access to its databases unless it is a legal obligation [i.e. regulated by law in accordance with Articles 6(1)c) and (2)-(3) of GDPR] or unless the said public administration database is such that "is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest" [cf. Articles 49(1)g) and (2) of GDPR].

b) Irrespective of the quality of the said example, one can have ambivalent feelings when reading these Draft Guidelines: on the one hand, the EDPB, in a welcoming way, *"encourages technology providers [and data controllers] to take the opportunity to use DPbDD as a competitive advantage in the market"*,[12] but, on the other hand, by declaring any element of a proposed solution (e.g. obtaining data directly from tax administration in the said example) as *"not necessary"*, the Draft Guidelines question the innovations in the said process. In general, as nothing is "necessary" technically (since anything can be done in different ways, even offline), "technology providers" may remain in doubt if any proposed solution may not violate the "necessity" principles as interpreted by data protection supervisory authorities.

3. Among the "key design and default elements" of storage limitation principle, the Draft Guidelines prescribe the following: *"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****"* (emphasis added). However, nothing in Article 13 and Article 14 obliges the data controller to do so. According to the said provisions; data controllers are obliged only to provide *"the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period".*[13] The EDPB is not authorised to supplement the GDPR.

In sum: since DPbDD is one of the key principles of the GDPR, it should be very carefully determined if any requirement laid down in the Draft Guidelines are really compulsory or just recommendations. In this, the Draft Guidelines should very carefully and in detail examine possible scenarios by taking into account that "the complexity of implementing DPbDD will vary based on the individual processing operation".

By Zsolt Bártfai

[12] See the eighth bullet point in paragraph 86. (Conclusions and Recommendations)
[13] See Article 13(2)(a) and Article 14(2)(a).