AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

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

Introduction

As a global cybersecurity company, we firmly believe that data protection rules are critical for the EU Digital Single Market as they essentially guarantee the fundamental right of EU citizens to the protection of personal data, as well as enable trusted digital transformation for building a data-driven economy in the EU – as the global norm setter in this field.

Following the general approach taken by the European Commission in Article 25 and Recital 78 of the General Data Protection Regulation (GDPR), as well as further in the 2019 Communication[1] where it highlights the necessity of flexibility of the data protection by design and by default principle, and taking into account the 2019 ENISA recommendations on shaping technology according to GDPR provisions[2], we are grateful for the opportunity to share our views, below, on practical guidance to achieve the data protection by design and by default as prescribed by Article 25.

We sincerely hope that our comments will be of interest and may contribute to the finalization of the guidelines. Below we share them in two parts: methodological and contextual comments.

Methodological comments

1. Data protection by design and by default should remain a single, uniform concept, as per the definition expressed in Article 25 and Recital 78 of the GDPR.

1.1. In paragraph 1, the draft guidelines introduce an abbreviation 'DPbDD', which stands for 'Data Protection by Design and by Default', thus highlighting the inseparability of the two parts ('by design' and 'by default') of the concept. This approach is in line with Article 25 of the GDPR, and therefore contributes to greater consistency and consensus in the industry-and-expert community, which is crucial for implementation of the concept.

1.2. However, further, DPbDD concept is split into two separate sections (2.1. and 2.2.), with obligations and principles for controllers outlined for each section. Following the text, the fundamental difference between these sections and, therefore, the two parts of the abbreviation, remains unclear to a reader. Could data protection by design be implemented without data protection by default, and vice versa? How could an SME differentiate these parts of similar meaning? What is the practical value in splitting these parts for achieving the required level of data protection and privacy?

1.3. Practically speaking, there are some obligations for controllers that have been attributed to one of the parts of DPbDD only. For instance, the obligation for controllers to take into account the period of storage of data and any retention of data in paragraph 52 directly relates to the principle of storage limitation (Article 5(1)(e)), and these requirements are set as default in the processing; i.e., 'the controller must have systematic procedures for data deletion embedded in the processing'. At the same time, given the definition in the executive summary that 'data protection by design must be implemented both at the time of determining the means of processing and at

[1] COM(2019) 374 final https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf
[2] https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

the time of processing itself', it is not clear why the obligation to limit the period of storage of data has not been attributed to data protection by design. We believe this requirement needs to be prescribed for implementing both data protection by design and by default as a single concept.

1.4. Thus, the division in DPbDD in the guidelines seems counterintuitive in both essence and structurally, and therefore we recommend keeping the methodological consistency and to highlight that data protection by design and by default is a single, uniform concept, which has to be applied by controllers in its entirety.

2. The scope of the draft guidelines needs to be extended to cover not only Article 25, but also Article 5, since Section 3 in the guidelines explicitly refers to the implementing principles relating to processing of personal data.

2.1. In Section 3, the draft guidelines outline the data protection principles that need to be implemented by controllers to achieve data protection by design and by default. These principles include: transparency, lawfulness, fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. These principles are also outlined in Article 5 and Recital 39 of the GDPR.

2.2. However, while explicitly stating in Section 1 (Scope) that the draft guidelines focus on "controllers' implementation of DPbDD based on the obligation in Article 25 of the GDPR", the document remains silent as to whether or how Article 5 should be read together with Article 25, and therefore mixes up appropriate technical and organizational measures (such as pseudonymisation) and principles leading to methodological uncertainty.

2.3. From a practical point of view, this also makes the situation for controllers ambiguous – especially for SMEs who often have less human and financial resources for compliance with the GDPR. If both security measures and principles compose data protection by design and by default, why do the guidelines not cover Article 5 of the GDPR, and why does the GDPR not mention their essential unity as well? It is important to clarify and provide clear commentaries for controllers, and we recommend expanding the scope of the draft guidelines by explicitly covering Article 5 of the GDPR.

3. Principles and security measures (technical and organizational ones) should be separated in the guidelines for greater structural and methodological consistency.

3.1. While we support the view that both principles and security measures (both technical and organizational ones) compose the guidelines on achieving data protection by design and by default, we consider that principles and security measures have different roles for controllers. Specifically, principles provide overall guidance and set the mind-set explaining the reasoning and logic behind the DPbDD concept, while security measures serve as practical steps for controllers to implement the required level of privacy and security.

3.2. We read Section 3 as the section with practical steps for controllers to implement data protection principles, and in this regard, to us, the inclusion of certain principles – such as the principle of fairness or the principle of transparency – seems counterintuitive: the draft guidelines explain each principle with detailed key design and default elements, but do not give practical instruction to data controllers on implementing the principles, and each element is read here as an improvement order or direction for a desired action, but not as a practical guide.

3.3. To support our argumentation, we believe the requirement to implement a technical measure such as pseudonymisation cannot be grouped together with the principle of fairness, which is not considered as a security measure.

3.4. Therefore, we recommend to frame principles as a separate section to demonstrate them as intentions that establish the mind-set for controllers for implementing data protection by design

and by default. The current Section 3 needs to focus solely on the practical steps (meaning security measures) that controllers need to implement for compliance with the GDPR.

4. The guidelines introduce a definition of technology providers not given in the GDPR.

4.1. In the Executive Summary (Scope) and thereinafter, the draft guidelines introduce a definition of technology providers, while in the GDPR there is neither a definition nor mention of any such providers. This inevitably leads to methodological ambiguity and inconsistency as the guidelines recognize them as additional 'key enablers for DPbDD' (paragraph 85) – distinguishing them from both processors and controllers – but at the same time the document does not clearly define who is implied under these providers or how different their legal status, obligations or roles are from those of processors and controllers.

4.2. To avoid unnecessary confusion for readers of the guidelines and, therefore, to contribute to their easier application, we recommend not having any additional definitions that are not prescribed by the GDPR, unless they are accompanied with explanations as to the critical importance for such.

Contextual comments

These comments directly refer to particular lines in the draft guidelines, and for convenience we list them in the below table:

Line No.	Sentence	Point for improvement
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. […]'	We believe that the draft guidelines need to clarify what key performance indicators demonstrating compliance would be deemed appropriate and sufficient by regulators. Perhaps separate discussion and study of this question might be necessary.
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.'	We deem it necessary to clarify in the draft guidelines which 'adequate organizational measures' are implied here.
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.'	While referring to 'existing standards and certifications' as an orienting point, the draft guidelines are silent on exactly which standards and certification are implied here. Perhaps separate discussion and study of this question might be necessary to finalize the guidelines.
24	'In some instances there may be simple low-cost solutions that can be just as or even more effective than their costly counterparts.'	The draft guidelines highlight that controllers have to keep in mind the goal of effective implementation, and take into account 'the cost of such implementation'. The document also mentions that 'effective implementation of principles must not necessarily lead to higher costs', but does not give any hint, especially to

		SMEs, as to what those low-cost solutions may be.
61, 63, 65, 67, 71, 74, 77, 80	'Key design and default elements may include: […]'	For each principle, the draft guidelines list key design and default elements, which are read in line with the name of Section 3, as practical steps and instructions for implementing each principle and achieving DPbDD. However, this is only how we read it; we may be mistaken here. We recommend adding clarity as to what 'key design and default elements' are, how mandatory they are, and whether all of them must be implemented at once.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies, helping 270,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com.

Contact

For more information, or to discuss the contents of this submission in more detail, please contact Anastasiya Kazakova, Public Affairs Manager (+7 968 648 60 05; anastasiya.kazakova@kaspersky.com), or Igor Kumagin, Cybersecurity expert (+32 474 80 09 28; igor.kumagin@kaspersky.com).