The Norwegian
Tax Administration

Return address:
P.O.Box 9200 Grønland, N-0134 OSLO

Our date 16. Januar 2020	Your date	Inquiries to Kevin McGillivray
+47	Your reference	Telephone +47
	Our reference	Postal address N-

Re: Public consultation reply to the EDPB's "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"

Introduction:

The Norwegian Tax Administration[1] submits the following comments to "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" (hereinafter 'the Opinion') published by the European Data Protection Board (EDPB).

The Norwegian Tax Administration's primary function and obligation is to secure financing for the Norwegian welfare state through effective taxation. In that capacity, the Norwegian Tax Administration is also responsible for administering a significant portion of the personal data processed in the Norwegian public sector including the National Registry of Persons. Thus, data protection and privacy are of the upmost importance for the Norwegian Tax Administration and affect a great deal of day-to-day agency operations.

As a point of departure, the Norwegian Tax Administration would like to thank the EDPB for the opportunity to comment on this very important area of data protection. The Norwegian Tax Administration also appreciates the amount of effort that has gone into the Opinion and provides comments with the goal of improving the overall quality of the Opinion. Therefore, the focus of the following comments are on areas for improvement rather than the positive aspects of the Opinion. The following comments are organized as follows: (1) general comments, (2) specific sections or points that should be addressed and (3) additional information The Norwegian Tax Administration would like to see in a final revised opinion.

(1) General comments

The concept of privacy by design has been discussed globally as a central aspect of meeting data protection obligations and protecting data subjects. [2] However, implementing the principles of privacy by design is a significant challenge. Thus, much of privacy by design's potential has yet to be realized.[3] Article 25 of the General Data Protection Regulation (GDPR) takes an important step in placing a direct—albeit qualified—duty on data controllers to implement Data Protection by Design and by

Default (DPbDD) measures. However, the relative vagueness of Article 25 is a potential limiting factor to creating effective privacy by design obligations and in creating clear guidance. Unlike certain other areas of the GDPR such as Article 28, which provides a relatively specific recipe for compliance, the obligations in Article 25 are much less clear.

With the aforementioned limitations in mind, in its current form, the Opinion does not provide a particularly useful tool for explaining the application of Article 25 or for meeting the overarching goals of DPbDD more generally. Instead of clarifying the application of and implications of Article 25, the opinion uses Article 25 as a lens to explain central GDPR obligations. This lack of focus makes it difficult to understand how DPbDD fits into the many general compliance obligations referenced throughout the opinion. In other words, the Opinion is framed as more of an overview of compliance rather than specific guidance on implementing the DPbDD obligations of Article 25. Rather than providing specific guidelines on article 25, the Opinion reads more as an explanatory note to Article 24. The result is that the guidance is not specific enough to formulate clear or implementable requirements.

Much of the argument for requiring the technological implementation of privacy obligations remains centred on privacy laws' dependence on the design of software and systems.[4] That is, the notion that software, hardware, and other systems should not only be secure, they should also safeguard privacy. A secure system may well violate a data subject's privacy if not designed properly. Therefore, a greater focus on technical measures that should be applied to meet the requirements of Article 25 is necessary if the Opinion is to obtain its desired effect.

[1] The Norwegian Tax Administration or "Skatteetaten" in Norwegian <https://www.skatteetaten.no/en/person/>

[2] Lee Bygrave, 'Hardwiring Privacy' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds.) *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017) 754-62. Providing a history of the concept of PbD dating back to work in the mid1990s. See generally Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (2011). Available at <https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>.

[3] Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 International Journal of Law and Information Technology 151, 152.

[4] Ibid. However, even if software and systems are seen as crucial, much of privacy by design's potential has yet to be realized.

From a practical perspective, it is difficult to give the Opinion to the Information and Technology (IT) department and point out concrete technical requirements or measures that must be put in place to obtain compliance. Given the central role that the IT department must play in implementing DPbDD requirements, this aspect is particularity problematic. The Opinion should—at some level—speak more directly to those responsible for implementing technical measures and designing systems (e.g. software engineers, applications developers, system architects) along with project management. As it stands, the Opinion appears to be directed at the legal department.

To a large extent, Article 25 is based on the principle of privacy by design, developed by the Information and Privacy Commissioner of Ontario. The guidelines could elaborate the practice and examples that stem from this work, if the purpose of article 25 is to formalize this principle. In that case, the Opinion could be based on the seven foundational principles of privacy by design and give practical guidance on how to fulfil these principles in the context of the GDPR. The EDPB issued a preliminary opinion on privacy by design that outlining how DPbDD might be implemented providing examples of methodologies. The preliminary opinion provides that "An effective implementation of the principle of privacy by design and by default can represent an outstanding milestone towards a human values based technology design." A realization of this value will heavily depend on a concrete guideline that will guide controllers implementing the principle and contribute to a more standardized approach in the market.

Part 3 "Implementing Data Protection Principles in the Processing of Personal Data Using Data Protection by Design and by Default" provides more specific "Key design and default elements". However, these are at a very general level allowing for a wide range of interpretations. Although the opinion needs to be dynamic and retain a measure of flexibility, as provided "clarity", "semantics" and "accessibility" are so broad that they will give those implementing the elements—including software, outsourcing, and cloud service providers—almost unlimited room in their interpretation.

Guidance that provides even a few specific core obligations is preferable over the generally malleable terms provided in the current Opinion. Concrete elements, such as the "no-robot-textfile" in paragraph 56, will allow for application that adds clear protection for data subjects. An additional point might include further evaluating the role of specific technical means of compliance with Article 25. For instance, this could be achieved by expanding and providing more specific examples to the "key design and default elements" in paragraph 71 and further explaining those elements in paragraph 80 of the Opinion.

Additionally, explaining how any technical obligations under Article 25 are different from the security of processing requirements under Article 32 would help to differentiate these areas. For instance, providing concrete examples of logical and physical security that would bolster DPbDD requirements.[5] Examples of such measures might include:

- Secure storage of passwords
- Create profiles with access and appropriate privilege limits
- Limit access to personal data using accepted authentication requirements
- Protect internal networks and secure servers
- Delete data when no longer needed
- Do not expose more data than needed in GUI and APIs
- Implement functionality for data export

In some areas, the Opinion might also benefit by providing "negative" examples of DPbDD. That is, provide clear examples or instances where processing activities clearly violate the obligations of Article 25. For example, if a controller builds a system without the functionality to delete personal data or provide access requests, the processing will not meet the baseline requirements of Article 25 and *de facto* violates core obligations of DPbDD. Another example of a clear violation of a baseline requirement of DPbDD might be storing sensitive personal data in clear text at rest. In other words, failing to take even minor steps to protect data subjects.

Additionally, instead of providing such general descriptions of elements of compliance including transparency, lawfulness, fairness, provide an example of the importance of these concepts in the context of DPbDD. That is, what is unique, important or relevant to Article 25 for each of these principles? The Opinion provides only a brief overview or cross reference to the principles without

[5] See CNIL, Security of Personal Data' Report/Guidance (2018) 1-24. Available at <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.

detailing how they fit within the core subject matter. Where possible, provide a methodology or specific guidance on how an organization might meet a specific challenge (i.e. transparency or fairness in the DPbDD process).

Further, is a risk analysis focused on DPbDD a necessary element for building an IT system? Should this be documented in the same manner as a DPIA? What other specific steps should be taken to meet the technical requirements of Article 25?

The Opinion would also benefit from additional guidance on organizational measures including managerial obligations and business processes that go beyond training requirements.[6] Further, the Opinion should more clearly separate organizational elements of DPbDD from technical measures. That is, what specific organizational measures does DPbDD require? How might developing business practices or internal policies promote DPbDD and help organizations meet the requirements of Article 25?

An additional concern with the level of generality in the guidance is that it gives technology providers too much discretion in determining what DPbDD requires and how it is implemented. Clearer obligations through more specific guidance will also provide controllers with much needed negotiating leverage in obtaining real and effective DPbDD measures from major providers including US-Based Cloud Service Providers (CSPs) that dominate both the European and American markets.

(2) Specific sections/points

Paragraphs 23 and 24 on the "cost of implementation". The distinction between cost in terms of money and cost in terms or resources does not follow for most organizations. That is, applying "resources in general, including time and human resources" requires a monetary investment as professionals providing such services require remuneration. In other words, the Opinion should more clearly acknowledge that creating systems that meet DPbDD requires an investment. Simply assigning existing

[6] Lee A Bygrave, ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 2 Oslo Law Review 105, 113-14. Explaining that privacy by design goes beyond the technical aspects also applies to managerial and business processes.

staff with additional DPbDD tasks, without providing additional resources, will most likely only result in "check-box" compliance.

In some aspects, the opinion seems to blur the lines between a DPIA and DPbDD. Does DPbDD expand or increase the requirements to conduct a DPIA?

Where the Opinion interprets Article 25, some of the explanations read into the GDPR-text elements or aspects that are not evident. For example, paragraph 7 provides:

> 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.

However, it does not follow from the text of the GDPR that these are two separate elements. Rather, the legislative text provides a list of obligations of which necessary safeguards are an element. The text of the GDPR provides:

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

In short, the text of the Opinion does not add much in the way of guidance and interprets the legislation in a manner that does not naturally flow from the original legislation.

In Part 3 "Implementing Data Protection Principles in the Processing of Personal Data Using Data Protection by Design and by Default" there are several elements (transparency, lawfulness, fairness, etc.) used as headings with a brief explanation of the concept followed by "Key design and default elements". However, it is not specified whether these "Key design and default elements" are part of the main element described in the section or regarding DPbDD more generally. For example at Paragraph

61, instead of "Key design and default elements may include" the opinion should specify, "Key design and default elements for transparency may include"—if that is the intent.[7]

§ 54 discussion freedom of information requirements and the role of DPbDD should be more clearly explained. As it currently reads, the Opinion could be interpreted to suggest that Article 25 may significantly limit legislation giving the right to access documents in the public sphere, even when a clear legal basis exists.

The executive summary should more clearly reflect the scope of the guidance in the opinion.
As a minor editorial point, the Opinion should be consistent with use of US or UK spellings. For instance, the opinion uses both spellings "minimization" and "minimisation."

(3) A revised opinion should include

Additional examples from the public sector. Although the lawfulness of processing pursuant to Article 6 of the GDPR is often based on specific national legislation, the issues facing the public sector are similar across member states. How public administrations might implement DPbDD principles while also meeting data sharing obligations, access requirements, open data requirements, and the "once only principle" would have a wide reaching impact.

What is the practical effect of DPbDD? Set a baseline of obligations. Even with the caveat that these requirements will be dynamic, this will provide readers—many of which do not have a dedicated privacy team—with specific obligations that they can aspire to meet.

The 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” included a flow chart that provided a graphical overview of application and obligations. A similar outline of Article 25 would be helpful. A good starting point is the representation created by the Norwegian Data Protection Authority in their guidance on privacy by design.[8]

[7] Emphasis added.
[8] Graphic from the Norwegian DPA’s Guidance available in full here <https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/>

Existing literature: How does this opinion evaluate or fit into existing guidance and literature on privacy by design?[9] Many organizations have relied on existing guidance from the UK ICO, the Norwegian Data Protection Authority, ENISA, ISO, CNIL, among others. These sources could be evaluated or at least referenced much more actively within the Opinion.

Conclusion:

Even if there is no 'one-size-fits-all' method for achieving the requirements of Article 25, in its current form the Opinion is too general. Although data controllers must analyse their data processing operations and make individualized assessments regarding the necessary and appropriate measures they must put in place to meet Article 25 obligations, the Opinion should provide a more concrete framework to assist in that analysis.

With Best Regards,

/s/
Erling Solberg
Senior Data Protection Advisor
The Norwegian Tax Administration

/s/
Kevin McGillivray
Case Manager
The Norwegian Tax Administration

[9] For example, the European Data Protection Supervisor, 'Opinion 5/2018 Preliminary Opinion on privacy by design' (2018) <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf>. The Norwegian Data Protection Authority: Software development with Data Protection by Design and by Default <https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/>. ENISA's PETs Maturity Assessment Repository <https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository>. NIST, 'An Introduction to Privacy Engineering and Risk Management in Federal Systems' (2017) <https://doi.org/10.6028/NIST.IR.8062>. Michael Veale, Reuben Binns, Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) International Data Privacy Law.