

European Data Protection Board

Our date	15.1.2020
Our reference	19/00370-32

Your date	
Your reference	

Uploaded to https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

Executive officer: Jon Berge Holden
Witheld from public access due to

Comments on draft EDPB guidelines - art 25

The Norwegian Digitalisation Agency would like to submit the following comments on EDPB's draft [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#) (version for public consultation)

General remarks

We welcome all guidelines from EDPB.

When it comes to the draft regarding Article 25, we think its value and usability would improve if the final version had more legal justifications for the interpretations that the recommendations are based upon.

Specific concerns

- 1) The draft's analysis of Article 25 (1) seems to lack support in the actual text of the article (paragraph 7)

The draft concludes in paragraph 7 that Article 25(1) imposes two duties on the controller: to implement measures, and to integrate safeguards in the processing. This is a reading of the article that seems to lack support in the legal text. If such an interpretation were to be upheld in the final version, the interpretation should be supported by a legal justification. In our view, the references to "in an effective manner" and "to integrate the necessary safeguards" are to be read as guidelines as to what will be considered as "appropriate" measures,, i.e. that the part starting with "and to integrate" does not impose a second set ("a second-tier", ref. paragraph 10) of requirements on the controller. It seems to us that our reading of Article 25 is in line with that of the Danish Data Protection Authorities, as it is expressed in its guidelines of June 2018¹. It seems like the interpretation in the draft requires that the word "to" in the latter part of 25 (1) is disregarded, so the sentence would read "...the controller shall ... implement ... measures ... and [tø] integrate... safeguards..."²

¹ <https://www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf>, e.g. page 23 "

² Article 25 (1) reads (grey and emphasis added): «1. 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

Given this revised understanding of Article 25 (1), more emphasis should be given in the guidelines as to how “appropriate” should be understood (para 8).

2) More guidance on the concept “by default” is requested (paragraphs 39-43)

The term “by default” implies a choice, that there is a choice for someone between a default and a non-default set of data processing. In situations where the legal basis for the processing is consent, this choice is clearly up to the data subject – the user can opt-in for a more intense data processing. But how is the term “default”, and the choice of non-default processing, to be understood when processing has a legal basis in Article 6 (1) (b)-(f)? Is Article 25 (2) at all relevant in those cases, or is it consumed by the requirement that processing be “necessary” in Article 6 or the data principles of Article 5?

3) More guidance regarding the relation between Article 25(2) and Articles 85 and 86.

We suggest that the draft also should include more guidance on the relationship between Article 25 (2) and national law, especially when national law mandates or allows for web publishing of public documents with personal data. How is article 25 (2) to be interpreted in those circumstances?

Best regards
for Norwegian Digitalisation Agency

Nils Medhus
Head of Section

Tone Bringedal
Senior Advisor

This document is approved electronically and sent without signature.

Copy to:

Recipient list:

European Data Protection
Board

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, 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.»