EUROPEAN DATA PROTECTION BOARD

ON GUIDELINES 4/2019 ON ARTICLE 25 DATA PROTECTION BY DESIGN AND BY DEFAULT

Confederation of Finnish Industries ("EK") is the leading business organization in Finland. EK represents the entire private sector and companies of all sizes. It serves over 15,300 member companies across all business sectors.

The European Data Protection Board ("EDPB" or the "Board") has invited public consultation on its Guidelines captured in the topic ("Guidelines"). EK thanks for the opportunity to participate in the consultation and presents the following remarks.

GENERAL COMMENTS

- As an editorial suggestion, in the parts 1 - 2 we would encourage to focus on the *rationale* of the law such as why data protection by design and by default ("PbDD") is considered a necessity (instead of simply relying on privacy principles, etc). The readership is likely professionals, and section 1-2 reads at times as repetition of the regulation without adding much new information. Part 3 is more practicable and actionable, with bullet-points, check-lists and examples. Nevertheless, lengthy checklists come across rather aspirational, and do not help to prioritize privacy design work.

- For legacy software "PbDD" can be a considerable challenge, and it may take a while before new systems operationalize "PbDD" from the start. Proportionality principle and risk-based approach is key, weighed based on most used or riskiest parts of the system.

- The difference between anonymous and pseudonymous data is crucial, and this Guideline refers to these concepts several times without going into detailed conditions for true anonymity. The EDPB is encouraged to update the WP28 Guidelines and practical examples would be highly appreciated.

SPECIAL NOTES

- **State of the art** (p. 8): most controllers rely on service and expertise of others for technical security. The Guidelines should give more concrete examples on what "due regard" means in choosing e.g. software or security system (with special

Confederation of Finnish Industries EK
EU transparency register 1274604847-34
PO Box 30 (Eteläranta 10), FI-00130 Helsinki, Finland
Telephone +358 9 420 20
firstname.lastname@ek.fi · www.ek.fi · BusinessId 1902799-1 · Domicile Helsinki

consideration given to SMEs), as in parts it reads as if controllers themselves must become experts themselves[1].

- **Lawfulness:** Banking example (p.15-16): banking sector is a heavily regulated and the example seems to run contradictory to EU and national credit and risk management rules and regulations. Banks will need information from both the potential customer but also from public source such as the tax authority (which, may also in some Member States be provided in the national legislation). Wording referring to all and any public source information seems unintentionally broad.

- **Fairness**: "consumer-choice" language is confusing and the search engine and "free choice" examples are unclear. These do not seem to add clarity to interpretation of GDPR.

- **AI credit application example** (p. 21-22): it should be clarified that AI can be used in credit approval if processing fulfills conditions of Art 22.

- **Data Minimization** (para 71): consider introducing data masking alongside pseudonymization. Pseudonymization's requirement of separate core data makes unfeasible solution in the context of multiple processing situations (would practically require unnecessary data replication without added value). Also, the EDPB view on "necessary data for the fulfillment of the contract" is too narrow and would make impractical and unnecessary limitations for example for use of date of birth, which can be key info for determining age (for age-restricted services) or combatting fraud.

- **Accuracy** (para 74): Consider introducing less-accurate data as a type of privacy protection. It would be welcome to note that non-accurate data use is permissible for the purposes of protecting individual's privacy (akin to example 2 from p. 20).

[1] For example: "controllers must have knowledge of and stay up to date on technological advances, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape." *p. 8*

Confederation of Finnish Industries EK
EU transparency register 1274604847-34
PO Box 30 (Eteläranta 10), FI-00130 Helsinki, Finland
Telephone +358 9 420 20
firstname.lastname@ek.fi · www.ek.fi · BusinessId 1902799-1 · Domicile Helsinki