Comment

of the German Insurance Association (GDV)
ID-number 6437280268-55

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

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
Data Protection/Basic Issues

E-Mail: **data-protection@gdv.de**

www.gdv.de

Data protection by design and default is one of the central principles of the GDPR.

While further guidance on the implementation of Art. 25 GDPR is welcome in general, the guidelines 4/2019 prove too restrictive in certain points. Some deliberations go far beyond the text of the GDPR. Others require additional clarification.

The aspects we consider problematic are the

- definition of “state of the art”,
- interpretation of “cost of implementation”,
- requirements on transparency and to disclose the balancing of interests,
- obligation to gather data directly from the data subject,
- examples for the fairness of data processing,
- unclear statements on usage of AI for decision-making,
- tendency for overly high requirements on technical and organizational measures and safeguards and
- absence of statements on how to ensure that processors and technology providers shall be encouraged to support the controllers.

1. Definition of „state of the art“

The guidelines contain mostly general remarks on how to determine the „state of the art“ in their paragraphs 18-22 (pages 7-8). On their own, these remarks do not pose a problem. However, in footnote 6 on page 7 the guidelines identify „state of the art“ as „the technology level of a service or technology or product that exists in the market and is most effective in achieving the objectives identified.“ The EDPB does not make it clear whether it considers the definition to be the correct one according to the GDPR. If that were the case, controllers would be overly burdened by the financial and organisational obligation to always scout the market for the most effective technology. Such a requirement seems excessive. An appropriate technological level that ensures effective protection should be sufficient.

2. Cost of implementation

According to Art. 25 GDPR, when determining the appropriate technical and organisational measures the cost of implementation should be taken into account. The EDPB holds the view that the provision is to be understood in such a way that the controller must always plan for and expend the costs necessary for the implementation of all principles in advance (page 8, paragraph 24). It is far more likely though that the European lawmaker intended for this element of the provision to be an expression of the principle of proportionality. We believe it means that the legislator did explicitly not want controllers to spend excessive amounts of money just in order to achieve a marginally higher level of data protection. As such, we perceive the EDPB`s interpretation as critical.

3. Transparency

Furthermore, the guidelines state that necessary information must be provided in the right context, at the appropriate time. Thus, according to the EDPB a privacy policy on the website alone is generally not sufficient for the controller to meet the requirements of transparency (page 14, paragraph 61). The explanation for this statement is sorely lacking. The EDPB does not state why and how it arrives at this conclusion. In our opinion, it is sufficient if a notice is displayed immediately when opening a website and thus before or with the beginning of the data processing. In this case, there is no reason to assume that the information is not presented in the right context and at the appropriate time.

4. Disclosure of the balancing of interests

In case the processing of data is carried out on the basis of Art. 6 (1) (f) GDPR, the guidelines state that the controller should disclose his assessment of the balancing of interests. The GDPR does not contain such a requirement. According to Art. 13-15 GDPR controllers merely have to disclose the legitimate interests they pursue to the data subject, but not their assessment of the balancing of interests.

5. Necessary in order to take steps at the request of the data subject prior to entering into a contract

In the example on pages 15 and 16 (paragraph 63) the EDPB expresses the view that necessary data for entering into a contract must be gathered directly from the data subject if the controller plans on using Art. 6 (1) (b) GDPR as the legal basis for the data processing. If the controller intends to collect the data from a third party, he will have no other option than do it on the basis of consent.

This too is a requirement not constituted by the GDPR. If the data itself and the act of its collection are necessary for entering into a contract, it makes no difference if the data is collected directly from the data subject or from a third party. A principle of generally having to gather data directly from the data subject is alien to the GDPR. Thus, consent is not the only possible legal basis for gathering data from a third party. Art. 6 (1) (b) GDPR is also applicable. Additionally, legitimate interests would also serve as an appropriate legal basis in the example as described in the guidelines.

6. Fairness

Under the headline „Fairness“ the guidelines request that processing should correspond with the data subjects‘ expectations. Moreover, whenever a service or a good is personalized or proprietary, it may create a lock-in to the service. If it is difficult for the data subject to change controllers due to this, it may not be fair.

The guidelines should specify that the processing should correspond with the data subject’s **reasonable** expectations since unreasonable expecta-

tions cannot and should not be required to be fulfilled. Finally, the question remains unanswered why it may be unfair if a personalized product or service meets the data subject's specific needs and makes it difficult for a data subject to change controllers.

7. Automatic individual decision-making

On page 22 (Example 1 on Accuracy) the guidelines determine that the bank "will never solely rely on the AI to decide whether to grant loans". While the example merely showcases one possible situation wherein the controller is fulfilling his obligations on data protection by default and design, it may be misconstrued as automatic individual decision-making never being allowed under any circumstances. As such we propose to add that the controller "should not rely on the AI to decide whether to grant loans, **unless the decision is made in accordance with the exemptions in Art. 22 (2) GDPR**".

8. Specific Measures

The EDPB proposes several measures and safeguards that shall provide effective data protection. The proposals include among others:

- Providing automatic and repeated information about what personal data is being stored (para. 10)
- Determination of key performance indicators to demonstrate compliance (para. 16)
- Multi-channel information of the data subjects (para. 61)
- Highest degree of autonomy for the data subjects (para. 65)

While these proposals are presented as examples of possible technical and organisational measures, a tendency for overly high prerequisites is clearly visible. This conclusion is punctuated by the fact that the EDPB considers these measures „**key design and default"** elements or examples of safeguards. This may pose a problem for controllers if all measures and safeguards must necessarily be of similar standard or level.

9. Obligations only for controllers, but not for technology providers

It is highly problematic that only controllers are held accountable for ensuring data protection by design and default. As the guidelines themselves

correctly state, producers of products, services and applications shall be encouraged to take into account the right for data protection during the development and design in order to make sure that controllers are able to fulfil their obligations (recital 78). While the guidelines refer to recital 78, they make no mention of how the EDPB intends to ensure that technology providers are encouraged to support the controllers. In the current situation most technology providers possess such market power that controllers are dependent on their product and do not have the standing to influence them or bargain with them for a higher data protection standard. Furthermore many controllers do not have the technical knowledge and personal capacity to control the products and all updates appropriately. In this case the controllers would be forced to forego the use of even standard products.

Berlin, 14 January 2020