Position Paper

Bitkom views on EDPB Guidelines 4/2019 on Data Protection by Design and by Default

16/01/2020
Page 1

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Introduction

Bitkom welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines on Data protection by Design and by Default. We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

We therefore appreciate that the EDPB published the draft Guidelines to provide clarity for scope and interpretation of Article 25 GDPR. We welcome that the Guideline show that the Principles of Data Protection by Design and by Default embody, above all, the principles of Art. 5 and 6 GDPR and the risk based approach.

Also, the distinction between Art. 25 (1) and Art. 25 (2) is helpful as it clarifies that para 1 addresses the procedural consideration of data protection in the development and implementation of new data processing systems, whereas Art. 25 (2) describes a substantive legal requirement (data minimisation) and refers to a specific application, namely that of the setting options for users. It is our understanding that para 2 can be seen as an explanation or specification of Art. 5 (1) lit. c).

The given interpretation of Art. 25 (1) deserves closer examination though: while the distinction between the actual measures for implementing data protection principles and the rights of data subjects on the one hand and the measures for ensuring their effective functioning on the other helps all controllers who think and work in risk management structures, security control systems work on a different level than measures taken for data protection. At the level of operational processes certain measures are implemented to reduce risk (or to ensure compliance) (so-called 1st line of defense/assurance), while at a security level, additional mechanisms must be implemented to ensure the functionality of the aforementioned measures (2nd line of assurance). In the context of an internal control system this would be referred to as "controls". The difference between Privacy by Design and such a control system, however, is that assurance must be carried out at the level of processes (as with an internal control system), while data protection must consider the needed measures at much more granular level, f.i. for an application, a data flow or a functionality/feature. In large companies, entire structures exist for these assurance levels. For data protection, this describes a core area of the activities of data protection officers in companies, who have a monitoring function. In our view, Art. 25 (1) addresses tools which, although they are to be implemented by the data controller, at the same time help the DPO to fulfil his or her tasks. However, where the Guidelines propose granular specifications for the scope of such monitoring, many will find them difficult or impossible to manage in practice.

In addition, the EDPB seems to weaken a legislative differentiation between certain processing operations with regard to Art. 35 GDPR: In itself, more comprehensive risk assessments should only be necessary where, according to a (standardised) overall view, there is a particular risk from the perspective of the data subject. Where the EDPB calls for an implementation strategy for both "measures" and "controls" that differentiates according to risk levels, the specific scope of Art. 35 GDPR becomes blurry and the risk based approach is weakened. Thus, by arguing for a risk assessment for each procedure, not only an initial assessment is required (Does the procedure reach the threshold of Art. 35 GDPR?), but also requires the controller to draw up sophisticated catalogues of measures, detached from this question and below the Art. 35 threshold. Here, too, the question of feasibility arises because such an assessment would not be limited to the documentation of requirements, but these requirements would have to be converted into technical measures (and these must be operated and kept up to date "state of the art"), which are then built into processing procedures as modules.

In our view, the EDPB should take greater account of the normative statements of Art. 35 GDPR and should read its intention into the requirements of Art. 25 (1) GDPR.

In addition and while the guidelines are certainly very helpful to shed some light on the structure of Art. 25 GDPR, some interpretations of the EDPB go beyond the legal requirements.

We would therefore like to highlight two aspects as part of our comments on the given interpretation: the Guidelines should take greater account of common, well established practice and should not go beyond the legal requirements of the GDPR in its interpretation. We will go into further detail in the following parts by commenting on certain paragraphs of the Guidelines.

2. Interpretation of Data Protection by Design and by Default

2.1 Scope

With regard to the scope the wording remains unclear with regard to “best practices”. Within official documents of the EU “shall” is often understood as a substantial requirement so that it might be confusing if the same wording is used within a best practices part of a guideline. (e.g.: „Universal design – Information shall be accessible to all, include use of machine readable languages to facilitate and automate readability and clarity.” This cannot be a prerequisite of the GDPR as it is not within its wording)

2.2 Analysis of Article 25

Para 10:

Safeguards act as a second tier to secure data subjects’ rights and freedoms in the processing. Having implemented the data protection principles effectively means that the controller has integrated the safeguards that are necessary to ensure their effectiveness throughout the life-cycle of the personal data being processed. Enabling data subjects to intervene in the processing, providing automatic and repeated information about what personal data is being stored, or having a retention reminder in a data repository may be examples of necessary safeguards. Another may be implementation of a malware detection system on a computer network or storage system in addition to training employees about phishing and basic “cyber hygiene”.

Bitkom Comment:

Automation might be desirable and give the data subjects easier access to their personal data and better possibilities to intervene but to call this a safeguard seems like an overinterpretation. Besides, this could be seen as inconsistent with Art 15 (3) (2) GDPR. The GDPR does not entail any provision that allows data subjects to consistently make use of its right of access. Finally automation is quite hard to achieve within many companies; the Guidelines should reflect that and take a more balanced approach

Para 14:

Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must be able to demonstrate that they have implemented dedicated measures to protect these principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of data subjects. It is therefore not enough to implement generic measures solely to document DPbDD-compliance; each implemented measure must have an actual effect. This observation has two consequences.

Bitkom Comment:

The wording "actual effect" would lead to a requirement, where for example training measures need to be effective.

Para 19:

In the context of Article 25, the reference to "state of the art" imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market. This means that 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.

Bitkom Comment:

State of the art cannot be understood as being a requirement to always use the newest available technology. State of the art is what is widely accepted throughout an industry and can be adopted.[1] This should be clarified as the "state of the art" is a dynamic concept that cannot be statically defined at a fixed point in time, but must be assessed continuously in the context of technological progress. In the face of technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25.

Para 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.

Bitkom Comments on 20 and 21:

Following the draft paper the term "state of the art" can be understood in the light of (e.g.) "ENISA, Privacy and Data Protection by Design – from policy to engineering, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport; S. 22 ff.

Within Germany, the equivalent term "Stand der Technik" has a much wider scope (see e.g. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html). Therefore, further clarification would be desirable.

Para 22:

Keeping in mind the goal of effective implementation of the principles into the processing, the controller must take into account the cost of such implementation under the design process. This means that the controller shall plan for and expend the costs necessary for the effective implementation of all of the principles. In doing so, the controller may assess the risks to the rights and freedoms of data subjects that the processing entails and estimate the cost of implementing the appropriate measures into the processing to mitigate such risks to a level

[1] See: Lang in: Taeger/Gabel, DS-GVO, Art. 25, Rn. 47. "[…] wenn die zugrunde liegende Technologie zum relevanten Zeitpunkt auf einem neuesten, aber gesicherten Erkenntnisstand von Wissenschaft und Technik beruht und in der Praxis bereits in ausreichendem Maß zur Verfügung steht.[…]"

where the principles are effectively implemented. The controller must manage the costs to be able to effectively implement all of the principles. Incapacity to bear the costs is no excuse for non-compliance with the GDPR.

Bitkom Comment:

In our view, the requirements are not balanced enough and would lead to undue burdens on many controllers. We recommend introducing at least some practical examples and more guidance on this matter. In our view, the EDPB should acknowledge that cost is a relevant factor in determining what measures are appropriate. The draft guidelines currently only emphasise that controllers must factor in Data protection by Design and by Default as a business cost. However, the inclusion of cost in Article 25 and 32 GDPR make clear that cost is a factor in assessing proportionality. Therefore, when determining which measures are required, this has to be taken into account.

Para 31:

The risk based approach does not exclude the use of baselines, best practices and standards. These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing). Nevertheless, the obligation in Article 25 (as well as Articles 24, 32 and 35(7)(c) GDPR) to take into account "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" remains. Therefore, controllers, although supported by such tools, must always carry out an assessment of data protection risks for the processing activity at hand and verify the effectiveness of the measures and safeguards proposed.

Bitkom Comment:

This seems to introduce an obligation to conduct a DPIA-like Assessment for every data processing (see also our comments in our introductory remarks).

Para 52:

If personal data is not needed after its first processing, then it shall by default be deleted or anonymized.

Anonymization of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of re-identification, is regularly assessed.

Bitkom Comment:

It should be pointed out, that this doesn't apply to personal data that is affected by a retention obligation. We welcome the clear statement that anonymization and deletion of data are considered equal measures.

Para 53:

Article 25(2) further states that personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. The controller must by default limit accessibility and consult with the data subject before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons.

Bitkom Comment:

These requirements cannot be fulfilled in everyday features of open platforms in the internet. We therefore urge the EDPB to consider the effects such requirements would have on innovative business models, platforms and websites that millions of users use in their daily lives.

Para 55:

Depending on the legal grounds for processing, the opportunity to intervene could either mean to ask for consent to make the personal data publicly accessible or to provide information about the public accessibility in order to enable data subjects to exercise their rights in Articles 15 to 22. Either way, the extent of the public accessibility of the personal data should be made transparent to the data subject at the time of "intervention", which is the moment for the data subject's intervention.

Bitkom Comment:

This goes beyond the requirements of the GDPR as other legal ground than consent could also be applicable (f.i. Art. 6 (1)(b) GDPR). The paragraph should therefore be amended.

Para 61:

Key design and default elements may include:

• Clarity – Information shall be in clear and plain language, concise and intelligible.

• Semantics – Communication shall have a clear meaning to the audience in question.

• Accessibility - Information shall be easily accessible for the data subject.

• Contextual – Information shall be provided at the relevant time and in the appropriate form.

• Relevance – Information shall be relevant and applicable to the specific data subject.

• Universal design – Information shall be accessible to all, include use of machine readable languages to facilitate and automate readability and clarity.

• Comprehensible – Data subjects shall have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.

• Multi-channel – Information should be provided in different channels and media, beyond the textual, to increase the probability for the information to effectively reach the data subject

Example: Moreover, necessary information must also be provided in the right context, at the appropriate time. This means, that generally a privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency. The controller therefore designs an information flow, presenting the data subject with relevant information within the appropriate contexts using e.g. informational snippets or pop-ups. For example, when asking the data subject to enter personal data, the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing.

Bitkom Comment:

More elaborations on these examples would be helpful and we recommend that the EDPB collects examples from all member states to build a best practice catalogue on this issue. This would deepen the understanding and could lead to more practicability. The given example goes way beyond what is legally required under the GDPR and should therefore be amended to better reflect practical examples of established transparency measures. In our view some of the interpretations are also too broad and go beyond what is legally required. For instance, the elaborations on the semantic element could lead to a requirement where a controller needs to provide several different data protection notices. The guidance on "relevance" introduces impractical obligations on the controllers as such specific information can hardly be given by larger service providers as the audience is too diverse, too broad to always determine the specific user. This could also lead to a requirement where a controller needs to provide several different data processing information notices. The same is true for the elaborations on "comprehensible" key features made by the EDPB in this paragraph. We ask the EDPB to consider the practical consequences such requirements would have.

Para 63:

- Withdrawal shall be as easy as giving consent. If not, any given consent is not valid.
- Cessation – If the legal basis ceases to apply, the processing shall cease accordingly.
- Necessary – Processing must be necessary for the purpose to be lawful. It is an objective test which involves an objective assessment of realistic alternatives of achieving the purpose.

Bitkom Comment:

The interpretation that consent should be invalid if the withdrawal is not as easy as giving consent goes way beyond GDPR requirements. The question whether consent is valid or not has to be decided by solely by the requirements of Art 7/ 8 GDPR. We ask the EDPB to amend that paragraph. The same is true for the elaborations on "Cessation" as the processing can be based on several legal bases and does not automatically become unlawful if one of the legal bases ceases to apply. This should be reflected in the paragraph. We also recommend amending the Guidelines with regard to the interpretation of "necessary" processing of data as it seems to narrow. The proposed interpretation could lead to a completely redundant Art 6(1)(b), as one might always find a way to perform a contract without processing certain data. That, however, is not the intention of the GDPR which stipulated that the processing has to serve the intended purpose without asking the controller to consider other means to achieve the purpose. This argument should also be considered with regard to para 69 and 71 of the Guidelines.

Para 65:

- Consumer choice – The controller should not "lock in" their users. Whenever a service or a good is personalized or proprietary, it may create a lock-in to the service or good. If it is difficult for the data subject to change controllers due to this, which may not be fair.

- Human intervention – The controller must incorporate qualified human intervention that is capable of recovering biases that machines may create in relation to the right to not be subject to automated individual decision making in Article 22.
- Fair algorithms – Information shall be provided to data subjects about processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements.

Example: A bookshop wants to add to their revenue by selling their books online. The bookshop owner wants to set up a standardised form for the ordering process. To prevent that customers don't fill out all the necessary information the bookshop owner makes all of the fields in the form a required field (if you don't fill out all the fields the customer can't place the order) using a standard contact form. The webshop owner initially uses a standard contact form, which asks the customer's date of birth, phone number and home address. However, not all the fields in the form are strictly necessary for the purpose of buying and delivering the books. The data subject's date of birth and phone number are not necessary for the purchase of the product. This means that these cannot be required fields in the web form to order the product. Moreover, there are situations where an address will not be necessary. For example, when ordering an eBook the customer can download the product and his or her address does not need to be processed by the webshop.
The webshop owner therefore decides to make two web forms: one for ordering books, with a field for the customer's address and one web form for ordering eBooks without a field for the customer's address.

Bitkom Comment:
Linking personalization of services to "unfair processing" is an interpretation that is not in line with the intention of the GDPR and goes well beyond its legal requirements. The freedom to conduct business, offer services that are tailored to the user and using data to achieve such a purpose should not be forbidden by conserving every such processing unfair. The transparency requirements and user rights serve as effective safeguards for the rights of the user and ensure a high level of data protection. We urge the EDPB to reconsider its interpretation and amending this paragraph.

With regard to the given example we recommend an amendment as it should be reflected that data might be collected for other purposes than just the book delivery (security reasons, e.g. telephone number, or having enough information about the customer to enforce possible future claims against the client, e.g. if he/she does not pay. Above that the date of birth might be necessary information for the service provider to assess whether the customer is old enough to conduct business at all/ old enough to buy a specific product with an age restriction.

Para 77:

Effectiveness of anonymization/deletion - The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible.

Bitkom Comment:

We welcome that anonymization and deletion are considered as being equal.
We would, however, recommend amending the paragraph with regards to necessary backups in the context of "deleted or anonymized data". Practical guidance and best practice examples would be helpful in this regard.

Bitkom represents more than 2,700 companies of the digital economy, including 1,900 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.