Comments on EDPB Guidelines 4/2019 on Article 25 GDPR

By Eike Wolf

These comments could be published with my name

0 Introduction

It has to be thanked to the EDPB for having taken the effort to give a thorough judgment to Article 25 of the GDPR. As a technician and a jurist specialized in civil rights and data protection since 40 years I attempt to underline some additional items which I miss in your excellent and necessary guidelines in the following. As far as possible some of these comments seem to me as very important due to the impact of the GDPR on contracts and warranty and indemnification.

1 Scope

The scope addresses mainly the controller based on the obligation in Article 25 of the GDPR. It mentions the **technology providers** but only as indirect addressed in Art 25. Due to my experience it should be necessary to put more emphasize on the technology providers or better manufacturers due to the fact that they deliver the system which could or should process personal data must be designed and built according to Art 25 GDPR. This is not a simple possibility but an obligation due to the fact that GDPR is law in all EU member states. However, if a law establishes a compelling requirement for systems, then each purchaser of those systems has a legitimate expectation that the system acquired will meet the requirement of the law. These expectations results in civil rights as a positive interest before take over the system and after take over as warranty interest. The acquirer in not obliged to express this claim explicitly, because it is a legal obligation. Taking this into account the Art 25 requests not only indirect but direct to manufacturers the fulfillment of DPbDD. Consider for this standpoint the EC Mandate M/530 (“Privacy and security management for product and services”) which asks CEN and CENELEC for development of several standards based on Art 25.

Additionally one has to consider that the average acquirer for instance a small enterprise has less knowledge and even no possibility to implement the requests of GDPR into a an acquired system. He must trust that the acquired system meets the requirements of the GDPR. How he then deals with the acquired system and uses it is mainly his responsibility as controller. Never the less he should have regress to the manufacturer based on warranty and indemnification if he is charged with claims based on not fulfilling the GDPR.

The guideline itself emphasizes in Section 6 paragraph 85 and 86 that the technology provider named here shortly manufacturer of the system delivered to controllers play a major role at implementation of DPbDD. This is obvious if the EDPB takes into account that most controllers in the EU are SMEs. That means that 90% of all enterprises have employees below 150. These small enterprises have seldom the opportunity to build their own systems and taking care of the GDPR. Most of them depend on manufacturers delivering systems that are GDPR compliant.

Considering this dependency the Guideline should include the manufacturer much more and even substitute the controller by the manufacturer where necessary or take both into account when it is obvious that the requested conditions by GDPR could not be provided or implemented by the controllers due to their lack of right (Copyright law on software) or lack of knowledge or influence on development for systems processing personal data. The Guideline concentrates too much responsibility and liability on the controllers. It is clear that the controllers have the liability and responsibility for violations of GDPR and they could not be released, however, in most cases the original systems are designed by manufacturers serving the market with their applications. If the manufacturer has not delivered the product or service which fulfills the GDPR and has not even warned in advance the controller about some lack or total lack all of the conditions requested by GDPR then the manufacturer is liable according to all civil rights of the EU member states ("*culpa in contrahendo*"). Even if a system is imported from outside the EU the importer is liable according to civil right at least to product liability by analogy.

It is recommended to use the term manufacturer instead of the more vague term "technology provider" and it is shorter and has a common understanding. However, to clear the understanding the term "manufacturer" should be defined for this Guideline.

2 Analysis of Article 25

To Paragraph 6:
DPbDD is not only for all controllers a requirement but taking into account the above arguments the manufacturer has to take at least the but same even more responsibility, because he has much more impact on the system then the controller. Therefore the manufacturer has more obligations to implement appropriate measures and necessary safeguards into the processing. Certainly the controller has then the obligation to use the system in the right manner and to implement appropriate organizational measures and necessary safeguards into the processing.

2.1 Article 25(1) GDPR: Data protection by design

To Paragraph 7:
In this paragraph the controller has to be substituted by manufacturer, because only he has the possibility and knowledge and therefore the obligation to implement appropriate technical and organizational measures which should be designed to implement the data protection principles and integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. Most controllers are due to their possibilities and knowledge as SMEs incapable to implement the requirements.

To Paragraph 8:
The controller has to be substituted by manufacturer because only he has usually the means and the methods to employ them in the processing.

To paragraph 11:
The pseudonymization of personal data is usually a mean which the manufacturer has to implement as a tool into the system, which the controller could or should use. However, the controller is usually not allowed to interfere in the acquired system to install pseudonymization. Therefore this condition is impossible to be performed by the controller. The statement has to be cleared that if the system has included a tool for pseudonymization the controller is liable to use it as appropriate.

To paragraph 12:
Every manufacturer designing systems which process personal data have to take care of the whole GDPR including especially the Art 5 and Art 12 to Art 22, because if these design principles are not incorporated in his system he has to explain expressively to his customers that the system is not fulfilling the conditions for processing personal data. If he misses this

explanation for a system which is normally used to process personal data he is fully liable for the faulty system (“*culpa in contrahendo*”).

Addressing effectiveness

To paragraph 14:
In this paragraph the controller has to be substituted by manufacturer, because he has the potential to demonstrate that the system is compliant with GDPR. The controller has only the opportunity to check whether or not his acquired system is compliant with GDPR. This is an obligation that can be imposed on the controller.

To paragraph 15:
The controllers should be substituted by manufacturers, as they are the originators of the systems and could and should control their design.

To paragraph 16:
The controllers should be substituted by manufacturers, as they are able to demonstrate that they have implemented measures and safeguards. The last sentence should be changed to “Alternatively, manufacturers and controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.”

Elements to be taken into account

To paragraph 17:
The controller should be substituted by manufacturer, because he determines the measures of a specific processing operation.

“state of the art”

To paragraph 19:
The reference to “state of the art” imposes an obligation on **manufacturers**, when determining the appropriate technical and organizational measures, to take account of the current progress in technology that is available on the market. This means that **manufacturers** 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. Any small enterprise will be overloaded by these requests.

To paragraph 21:
The “state of the art” criterion is also in the responsibility of the controller and does not only apply to technological measures, but also to organizational ones. Lack of adequate organizational measures can lower or even completely undermine the effectiveness of a chosen technology, which is outside of control for the manufacturer.

To paragraph 22:
The controller should be substituted by manufacturer, because he could and should take these into account in the design and implementation of data protection measures. The controller is based on his reduced knowledge (SME) seldom able to take these into account.

“cost of implementation”

To paragraph 24:
In the first four sentences the controller should be substituted by manufacturer.

“nature, scope, context and purpose of processing“

To paragraph 25:
The controllers should be substituted by manufacturers, because only they have the experience and the ability to implement these factors.

“risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing”

To paragraph 29:
This statement should be replaced by the following: “When performing the risk analysis for compliance with Articles 24 and 25 the manufacturer and the controller independently of each other have to identify the risks and determine their likelihood and severity.”

To paragraph 31:
The second sentence should be replaced by the following: “These might provide a useful toolbox for manufacturers and controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing).”

At the time of the determination of the means for processing

To paragraph 32:
The sentence should be enhanced to: “Data protection by design must be implemented by the manufacturer *“at the time of determination of the means for processing”*, because he has to select the right means of processing. The controller has seldom the possibility to make such a choice.

To paragraph 34:
This paragraph should be enhanced by the following sentence at the beginning due to the fact that the manufacturer has to provide the appropriate measures and safeguards : “The manufacturer has to provide the appropriate measures and safeguards in his offered system to support the controller so that the controller could use the means to reach the requirements of the GDPR.” …….

To paragraph 35:
Enhance the paragraph by: “The manufacturer has to provide the means so that the controllers must be able to demonstrate that such assessments have been made for all of the means that are part of the processing.”

To paragraph 36:
The second sentence should be enhanced to : “From a cost-benefit perspective, it would be in manufacturers’ and controllers’ interest to take this into account sooner rather than later, as it could be challenging and costly to make changes to plans that have already been made and processing operations that have already been designed.”

2.2 Article 25(2): Data protection by default

Default

To paragraph 39:
In order to give the controller the possibility to select the preferred values at the end of the paragraph the following sentence should follow: “The manufacturer of the delivered system is obliged to implement in the system the possibility for the controller to select the right values out of configurable presetting.”

Technical and organizational measures

To paragraph 45:
The paragraph should be enhanced at the beginning by the sentence: “In order to support the controller for the predetermination of legitimate purposes the manufacturer has to take care of this obligation of the controller and provides the measures by default.”

“the period of their storage”

To paragraph 52:
The paragraph should start with the following sentence:
“In order to fulfill the request of storage limitation the manufacturer has to provide the means that for different cases different storage limitations are possible by default, so that the controller has the possibility to limit the retention period for different cases.”

“their accessibility”

To paragraph 53:
The first paragraph should start with the following sentence:
“For the request of limitation of access to personal data the manufacturer has to provide in his system means that for different use cases different rights of accessibilities are implemented and could be more or less freely selected by the controller.”

The second paragraph should start with:
“The manufacturer has to prevent in his delivered system that personal date could not be accessible by an indefinite number of persons without the free consent of the concerned data subject and according to paragraph 56 that even for the case the data subject has given his free consent for publishing his personal data. The data shall not be searchable by robot crawlers.”

3 IMPLEMENTING DATA PROTECTION PRINCIPLES IN THE PROCESSING OF PERSONAL DATA USING DATA PROTECTION BY DESIGN AND BY DEFAULT

The Guideline uses 8 headlines to support the DPbDD. It is recommended to extend these headlines to 10 principles and extract important rules out of the 8 headlines in order to emphasize important viewpoints. These 10 recommended rules or principles are

(1) Avoidance of personal data as far as possible

(2) Transparency of processing

(3) Lawfulness of processing

(4) Fairness of processing

(5) Purpose limitation

(6) Data minimization

(7) Accuracy of data

(8) Storage Limitation

(9) Integrity and confidentiality

(10) Deletion of personal data

Only the first and the last principle are insofar new as they are extracted from the already mentioned principles in the Guideline.

Avoidance of personal data has been extracted from Data Minimization (paragraph 69) in order to put much more emphasizes on this principle. The reason is simple, because personal data not collected and not processed could not abused, not by negligence be revealed to third parties or to public. It causes no additional cost for processing, storage, organizational efforts and it causes no risk by any criminal acts (hacking, stealing, etc). It is obvious that this principle requests at design of a system much more effort and possible change the design of a business model, however, this effort reduces the subsequent development due to omission of any safeguarding and processing efforts and adaptation of the process which by experience takes only a fraction of the following adaptation costs. This makes any system more secure and saves the rights and freedom of the data subjects by absence of his data.

It is obvious that this avoidance could not be taking into account for online purchasing of goods, because the address of the receiver of the good is necessary. However, for digital data the avoidance is possible because the payment in return could already be anonymous for the seller.

Deletion of personal data has been extracted from Storage Limitation (paragraph 77) also in order to put much more attention to this principle. The experience shows that personal data are retained much more then allowed and considered useful with the attitude "*it could be useful in the future and for advertising*". But this retention violets the rule of Art 5 paragraph 1 (e) that personal data has to be deleted, if the purpose is completely fulfilled. There are some lawful obligations to retain it. However, for such cases special arrangements have to be implemented to reduce the access and correct implemented pseudonymization to prevent possible abuse or negligence or the data are blocked such that nobody even not the administrator of the system have access to it. It could then be deleted by the next clearance of the system or at rearranging the data base.

To paragraph 58:
This paragraph treats features which are important to be considered in a very early stage of development and they are therefore to be taken into account by the manufacturer. And so the controller should be substituted by manufacturer.

Transparency

To paragraph 60:
Due to the fact that transparency is a design principle the controller should be attended by the manufacturer, because at the end the controller makes use of the system supported by the means incorporated in the system.

To paragraph 61:
The key design and default elements may include the mentioned functionality. However, some of them request the support of the system designed by the manufacturer which has to implement it in the system delivered:

- 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, which has to be prepared by the manufacturer
- Contextual – Information shall be provided at the relevant time and in the appropriate form, the appropriate form is part of the obligations of the manufacturer
- 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, which is under the obligation of the manufacturer
- 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, which even the manufacturer has to prepared them in a useful and understandable form
- 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.

The **example** contains obligations which are in the duty of the manufacturer:
In the first sentence the controller should be substituted by manufacturer, because this is the duty of him.
The third and forth sentences should be supported in the basic design by the manufacturer.
For the whole second paragraph the manufacturer has to provide the means that the information is presented in the requested manner.
In the third paragraph the controller should be substituted by manufacturer as it is his duty to provide the design of the information flow.

Lawfulness

It is obvious that this section is under the responsibility of the controller, however, the manufacturer is obliged to deliver the means which supports the key design and the default elements.

Fairness

To paragraph 65:
The key design is an obligation of the manufacturer. This means that he has to design the system to be delivered such that all default elements are prepared and designed for the controller in a manner easy to use and understandable for the controller. Especially the algorithms are typical obligation of the manufacturer.

Purpose Limitation

To paragraph 66:
The design of the processing is the obligation of the manufacturer.

To paragraph 66:
The manufacturer has the obligation that he as an expert for design are obliged to foresee the legitimate purposes and the compatibility with further legitimate purposes. The manufacturer has additionally to include the technical limits of reuse because this is a security principle as part of data protection.

Data Minimisation

To paragraph 69:
The avoidance of processing personal data should be the first decision of the controller. For most cases exist a solution, which avoids the collection and processing of personal data. However, this has to be decided at the very beginning even before the decision on privacy by design and it makes necessary a decision on business model. This decision has a great impact on the selection of products. It is recommended to follow the 10 basic rules. The avoidance as already mentioned reduces the cost of processing the personal data and avoids even all risks with it. Thinking about a solution to avoid personal data saves more cost then the process about thinking on it.

To paragraph 71:
The manufacturer is responsible to design the system in the manner that the key design and the default elements of this paragraph could be fulfilled. The controller is then responsible to apply the system accordingly.

Accuracy

Accuracy and the supporting features for performing it request the conforming design by the manufacturer. He is therefore obliged to provide the features to support the controller keeping personal data accurate and up to date.

Artificial intelligence is most based on statistical methods and therefore indeterminate. It should be therefore be avoided as much us possibly. If it is used due to simplification of decisions it requests definitely the beforehand consent of the data subject with explanation of the impact on his rights and freedoms. In order to be compliant with GDPR the manufacturer has to consider all these conditions in his design.

Storage limitation

The paragraphs 75 to 77 request strong support by features and functionalities of the applied software. Therefore the manufacturer is obliged and it is a strong demand to him to implement the supporting features and functionalities.

The manufacturer has additionally to take into account that backup storage is not excluded from the protection of personal data. He has therefore to implement features and functionalities to secure and to delete or to make inaccessible by no means personal data which must be erased by request or by default due to time out or no longer necessary.

Integrity and confidentiality

The paragraphs 78 to 80 request strong support by features and functionalities of the applied software. Therefore the manufacturer is obliged and it is a strong demand to him to implement the supporting features and functionalities to reach the conditions of GDPR.

4 CERTIFICATION

To paragraph 81:
It seems to be out of the economic horizon of most of the European SMEs to apply for certification according to Article 42 because the audits and the requested conditions for these are very expensive. The manufacturer is much more in the economic position to get a certification of offered products and services due to the fact that he could distribute such cost over several products and services. A certified system is than an advantage for the controller if he applies it correctly.

5 ENFORCEMENT OF ARTICLE 25 AND CONSEQUENCES

No additional comment.

6 CONCLUSIONS AND RECOMMENDATIONS

To paragraph 85:
Keeping in mind that most the controllers in Europe are SMEs and as such they are not able and not interested to develop application software which fulfils the condition of this guideline the main focus to get the right systems are on manufactures. They are as experts in software development obliged to develop systems according to GDPR and this guideline. This very important viewpoint should be included in the revision of this guideline.
A further recommendation is that the development of such systems should be according to ISO/IEC 90003 which makes the development more transparent than all the other methods.

Recommendations

To paragraph 86:
Beside the recommendations in paragraph 85 the mentioned “technology provider” should replaced by manufacturer due to the fact, that it is a more common concept and noted. All the other bullets are supported.