15 January 2020

Ecommerce Europe's contribution to the EDPB Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default

1. Introduction

These Guidelines give a very detailed general guidance on the obligation of controllers to provide in all their operations where data-processing is part of for Data Protection by Design of this operation and by Default set forth in Art. 25 GDPR (DPbDD), where the core obligation is the effective implementation of the data protection principles and data subjects' rights and freedoms by **design** and by **default**.

This requires that controllers implement, and are able to demonstrate, appropriate technical and organizational measures and necessary safeguards, designed to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects. Controllers must be able to demonstrate the effectiveness of the implemented measures.

Data protection by design must be implemented both at the time of determining the means of processing and at the time of processing itself. It is at the time of determining the means of processing that controllers shall implement measures and safeguards designed to effectively implement the data protection principles. To ensure effective data protection at the time of processing, the controller must regularly review the effectiveness of the chosen measures and safeguards. The EDPB encourages early consideration of DPbDD when planning a new processing operation.

The Guidelines cover elements that controllers must take into account when designing the processing. The criteria of "state of the art" requires controllers to stay up to date on technological progress in order to secure continued effective implementation of the data protection principles. The "cost of implementation" requires the controller to take into account the cost and resources required for the effective implementation and continued maintenance of all of the data protection principles throughout the processing operation. Other elements controllers must take into account are the nature, scope, context and purpose of the processing, and the risk of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Furthermore, Article 25 requires **data protection by default**, meaning that by default, only personal data which are necessary for each specific purpose of the processing is processed. Thus, the default settings must be designed with data protection in mind. Default settings include both parameters that can be set by controllers and data subjects.

The Guidelines also contain practical guidance on how to effectively implement the data protection principles in Art. 5(1) GDPR, listing key design and default elements as well as practical cases for illustration. The possibilities of certification in accordance with Article 42 and supervisory authorities' enforcement of Article 25 are also addressed.

In closing, the EDPB provides recommendations on how controllers, processors and technology providers can cooperation to achieve DPbDD and how DPbDD can be used as a competitive advantage.

2. Ecommerce Europe's feedback on the Guidelines

In general, Ecommerce Europe can basically agree with the very detailed principle based guidelines that certainly will contribute to a clear insight for controllers to be compliant on one of to their core obligations of the GDPR which is to deliver to privacy and data protection by design and by default.

The guidance provides for a clear and extensive checklist for controllers and processors how to be compliant and how to set up their operations respecting the principles of privacy and data protection at the very start of the design of it and provides also for a clear checklist on how to establish optimal privacy and data protection by default settings.

Ecommerce Europe supports the conclusion of the EDPB in par. 16 that KPIs might be an appropriate means to demonstrate compliance, but it must however be absolutely clear that it is not a mandatory obligation to demonstrate compliance by using appropriate KPIs, as it is at the discretion of the controller to choose the means for demonstrating compliance.

However, in the view of Ecommerce Europe, the guidelines are in some ways too strict, as they do not offer the necessary solution for all contexts.

As regard to the processing of **Big Data** (par. 52) it seems to Ecommerce Europe that the EDPB - in its statement that if personal data is not needed after its first processing, then it shall by default be deleted or anonymized - implies that gathering and retention of Big Data as such is impossible under all circumstances and in every context. We are of the opinion that, especially in those cases where unlimited gathering of Big Data is the main purpose of the processing and in those cases where personal data are provided as a counter-prestation or payment for certain services, the obligation to delete data after first processing is not realistic and not based on the articles of the GDPR. In that perspective, Ecommerce Europe urges the EDPB to adjust his statement accordingly.

As regard to providing information to the data subjects on how their personal data is processed, the EDPB, in the example under par. 61, seems to imply that controllers in any way have to provide for **video clips** to explain the most important points of the information. Ecommerce Europe certainly agrees that video clips can be very helpful to provide for the essential information in an easy way, but it should in our view not be mandatory and not seen as always essential to provide for this information. Depending on the context and the medium used for communication (for instance voice-controlled ordering), also other forms and formats of information than video clips should be recognized as compliant and efficient. In that perspective, Ecommerce Europe asks the EDPB to express explicitly that video clips are as such not a mandatory means of information on privacy and data protection.

The same applies to the statement of the EDPB (example under par. 61) that in all circumstances and contexts the privacy policy should be accessible on all internal pages by maximum one click. In the view of Ecommerce Europe, this obligation is too rigid and not realistic in the context of Apps and devices with limited space and does not take into account that traders, besides the mandatory information of the GDPR, also have to provide for mandatory information based on other legislation, like the Consumers Right Directive, the Directives on the sales of goods and digital content, the e-Privacy Directive and the e-Commerce Directive. Considering the fact that there is no legal hierarchy for information obligations and as such GDPR information has no priority, it seems logic to Ecommerce Europe that consumers/data subjects evidently are referred for all this information to a general menu that also contains, as a sublayer, information on privacy and data protection which, at least in the end, needs two clicks to access this information. It should be clear from the guidance that under such circumstances or in such contexts, more than one click to access the essential privacy information is also compliant.

In an equal way, we have doubts on the statement under par. 71, example 1. In our interpretation of this statement, the EDPB seems to imply that certain data are not **essential to perform the contract** for the sale of goods, services or digital content, like birthday, phone number and e-mail address and the processing of them cannot be based on the legal ground "necessary for the performance of the contract". Based on the principle of data minimalization such data should, in the vision of the EDPB, by default, not be processed. Ecommerce Europe doubts this position. In our view, the contract also covers the precontractual and post contractual stage and also the obligation for the trader to provide for safe and secure access and payment methods and necessary communication in case of defects or recalls. This means that, depending on the contract and the context, necessary data to perform the contract also include data for identification (date of birth, address), confirmation (e-mail address) and after sales service in case of defective products/recalls (telephone number). That is why Ecommerce Europe asks the EDPB to explicitly state that these personal data mentioned can, depending on the context and the purpose of the processing, effectively be considered as essential to perform contractual obligations other than just delivery of the sold good or service.

About Ecommerce Europe

Ecommerce Europe is the sole voice of the European Digital Commerce sector. As a result of joining forces with EMOTA, Ecommerce Europe now represents, via its 23 national associations, more than 100,000 companies selling goods and services online to consumers in Europe. Ecommerce Europe acts at European level to help legislators create a better framework for online merchants, so that their sales can grow further.