VAN BAEL & BELLIS

CLIENT ALERT MEMORANDUM

3 December 2019

EDPB Guidelines on Data Protection by Design and by Default

On 13 November 2019, the European Data Protection Board (***EDPB***) published draft guidelines (the ***Guidelines***) on the principle of "Data Protection by Design and by Default" set out under Article 25 of the General Data Protection Regulation (***GDPR***). The Guidelines explain how controllers must ensure that they effectively implement the "*data protection principles and data subjects' rights and freedoms by design and by default*" during the design and life cycle of processing activities.

The EDPB underlines that Data Protection by Design and Default is a requirement for all controllers, independent of their size. The examples contained in the Guidelines illustrate the broad range of processing activities to which this principle applies: from setting up membership administration to buying customer relationship management (CRM) software; designing online order forms; improving effectiveness of deliveries (through tracking employees); deciding on loan applications as a financial institution; or using artificial intelligence to profile customers. However, the complexity of implementing this principle will vary based on the individual processing operation. In this regard, the principle of Data Protection by Design and Default is coherent with the "risk-based approach" underlying the GDPR.

Data protection by design

Under the principle of "Data Protection by Design", data controllers are obliged to implement "appropriate technical and organisational measures" and "necessary safeguards" to implement data protection principles, such as lawfulness and data minimisation, in an effective manner and to protect the rights and freedoms of data subjects. The Guidelines explain these measures and safeguards and list elements that must be considered to determine which measures are "appropriate" or which safeguards are "necessary".

The EDPB clarifies that measures and safeguards must be implemented both at the time of determining the means of processing data <u>and</u> at the time of processing the data itself. A regular review of the effectiveness of the chosen measures and safeguards is required in order to ensure effective data protection at the time of processing.

The Guidelines furthermore explain that there is no requirement as to the sophistication of a technical or organisational measure so long as it is appropriate for implementing the data protection principles effectively. Such a measure can be anything, from the use of advanced technical solutions to the basic training of personnel (*e.g.*, on how to handle customer data).

Necessary safeguards are, for example, 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.

The *effective* implementation of the data protection principles means that controllers must be able to demonstrate that they implemented dedicated measures to protect these principles and that specific necessary safeguards were put in place. This compliance may be demonstrated by appropriate key performance indicators, which may include quantitative or qualitative metrics. Alternatively, controllers may provide the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.

Article 25 lists some elements that the controller has to take into account when determining the appropriate technical and organisational measures of a specific processing operation:

- The concept of "*state of the art*" imposes an obligation on controllers 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: (i) technological advances, (ii) how technology can present data protection risks to the processing operation and (iii) 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. Taking into account technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Existing standards and certifications may play a role in indicating the current "state of the art" within a field.

- The controller must consider the "*cost of implementation*" under the design process meaning that the costs necessary for the effective implementation of all the principles should be planned and expended. 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 where the principles are effectively implemented. According to the Guidelines, spending more on technology does not necessarily lead to more effective implementation of the principles. In some instances, simple low-cost solutions can be just as or even more effective than their costly counterparts.

- Controllers must take into consideration factors such as the "*nature, scope, context and purpose"* of processing.

- Article 25 obliges controllers to take into account "*risks of varying likelihood and severity for rights and freedoms of natural persons"* posed by the processing. Controllers must therefore 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. This also applies if controllers are supported by useful tools to tackle similar risks in similar situations such as the use of baselines, best practices and standards.

Data Protection by Default

In addition, Article 25 of the GDPR requires "Data Protection by Default", which means that, by default, only personal data which are necessary for each specific purpose of the processing can be processed. This principle refers to the choices made by a controller regarding any pre-existing configuration value or processing option that is assigned in a software application, computer programme or device that has the effect of adjusting, in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Default settings must thus be designed with data protection in mind. Some key aspects of the Guidelines relating to this principle are the following:

- If there were no default settings, data subjects would be overwhelmed by options that he or she may not have the ability to grasp. Thus, in many cases, controllers must decide on these options on behalf of the data subjects and, in doing so, they have to ensure that only the personal data that is necessary to achieve the purpose of the processing is enabled.

- Technical and organisational measures in the context of data protection by default is understood in the same way as explained above under the principle of "Data Protection by Design" but is applied specifically to the principle of data minimisation. The measures must, by default, be appropriate to ensure that only personal data which are necessary for each specific purpose of processing are being processed. This includes that controllers must take into account the amount of personal data collected (*i.e.*, the volume of personal data, types, categories and level of detail of personal data required for the processing purposes), the extent of their processing, the period of their storage (*i.e.*, if personal data is not needed after its first processing, then it shall by default be deleted or anonymised) and their accessibility (*i.e.*, access to personal data must be limited based on an assessment of necessity but they must be accessible to those who need it when necessary, for example in critical situations).

Implementation of Basic Data Protection Principles

The EDPB explains that Data Protection by Design and Default is a critical step to effectively implement the data protection principles in Article 5(1) of the GDPR, such as transparency, lawfulness of processing and purpose limitation. The Guidelines contain practical guidance by listing key design and default elements as well as practical cases for illustration.

For instance, to illustrate how to implement the principle of "transparency" by design and by default, the Guidelines explain that, in general, providing a privacy policy on the website alone is not enough for the controller to meet the requirements of transparency. Data subjects should be enabled to understand, and if necessary, make use of their rights in Articles 15 to 22 of the GDPR. The controller can therefore design a privacy policy, but the necessary information must be provided in the right context and at the appropriate time. This implies that the controller should inform the data subject, when asking him/her to enter personal data, of how the personal data will be processed and why these personal data are necessary for the processing. To give another example, when relying on legitimate interests as the legal basis for processing data, the controller should disclose their assessment of the balancing of interests. This is considered in the Guidelines as a key design and default element that helps in meeting the requirements of "lawfulness".

The Guidelines also address the possibilities of certification in accordance with Article 42 of the GDPR and supervisory authorities' enforcement of Article 25 of the GDPR. Finally, the EDPB provides recommendations on how controllers, processors and technology providers can cooperate to achieve "Data Protection by Design and by Default" and how they can turn this into a competitive advantage.

A copy of the EDPB's draft Guidelines can be found here. Stakeholders can submit comments on these draft Guidelines until 16 January 2020.

Authors

Thibaut D'hulst	tdhulst@vbb.com
Justine Van Den Bon	jvandenbon@vbb.com

Get in touch

If you have any questions concerning this memorandum, please call us at	+32 2 647 73 50
or send us an e-mail at	brussels@vbb.com