Spolek pro ochranu osobních údajů

# Comments on the EDPB's proposal of "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"

Prague, January 15, 2020

First of all, we would like to express our sincere thanks for the opportunity to provide comments on the EDPB's proposed "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" (hereinafter "the Guidelines"). Spolek pro ochranu osobních údajů (The Data Protection Association) is the largest organization bringing together DPOs and other professionals in the field of personal data protection in the Czech Republic.

**Below are our comments to the draft Guidelines:**

We welcome the Guidelines provide controllers with the detailed guidance. However, we would like to point out that, especially for smaller controllers, these requirements may be too complex to be practically met.

We would like to add and also emphasize that, in the context of the implementation of security measures, it is clear that, in addition to linking the proportionality (necessity) requirements and the effectiveness of concrete measures, it is absolutely crucial to link GDPR measures correctly with cyber security measures to create a robust and comprehensive system (see point 9 and related points to specific security measures). This can be correlated with point 15 since it is not enough (proven in practice) to implement general measures solely to prove compliance with DPbDD, seeing that the decisive factor always becomes the context and environment in which the organization operates (see point 15).

Considering the cost of such implementation in the design process, it is necessary to say that the financial issue is a major factor in the decision-making and appropriation of individual measures - especially for smaller controllers (see point 24). That is why it is so important to have well-managed management and delegation for small businesses that are often exposed to the same risks, - but with different opportunities - that large companies (controllers) have faced too.

We must also confirm that prompt consideration of the costs and benefits of concrete measures and correct timing is essential for the successful implementation of the principles, but on the other hand, it may be difficult for small businesses to regularly review these measures as this may assume rapid adaptation to changes in conditions or external environment (see point 36-38). Otherwise, it may be true that the rigor of large controllers and sometimes the tough institutional character also undermines the efforts to regularly monitor the effectiveness of individual measures. So, this could be for both controllers the same question to be solved.

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

We could certainly agree that information security should permeate all levels of the organization's system, but it is necessary to evaluate each level of the organization separately - as a wide-ranging security measure (in default manner) could entail unnecessary or additional financial costs on the controllers or its business partners (see point 47).

Regarding the published data (see point 53 and 54), we believe that the obligation to always consult the data subject prior to the publication of the data or making available does not arise from any provision of the GDPR. Typically, for example, in the case of the exercise of freedom of expression, this requirement could be at the edge of constitutionality.

Multi-channel information in point 61 – we believe that this requirement (for example to provide the videoclip) could be too demanding especially for smaller controllers. This approach is not common even for large and financially more disponible controllers.

We would like to point out that we respectfully disagree with the idea that if the withdrawal of the consent is not as easy as giving, consent is not valid (probably - as we understand - this point it is meant that in such a case the consent is invalid from the beginning and even if the problems with the possibility to withdraw consent only occurred later). From the point of view of basic legal principles, it is very unusual to retroactively invalidate a legal action that has been duly conducted. We believe that such a consequence is not justified even by the recitals 42 and 43 of the GDPR. Of course, the impossibility of easy withdrawing of consent may affect the lawfulness of the processing that occurs after the data subject has taken the intention to withdraw the consent. We believe that the question of the legal consequences of the impossibility of easy withdrawing consent requires further discussion.

The requirement to disclose the assessment of the balancing of interest in point 63 seems to us as disproportionate. This is not usually the case in practice, and would be in some cases an unjustified burden, especially for smaller controllers or for some specific types of business sector, where also this may not be a widespread practice or there may be a risk of breach of security guarantees for these businesses.

Although we agree that the controller should avoid "lock in" of data subjects, the example in point 65 does not seem very appropriate to us. In practice, personalization of services is often demanded and welcomed by data subjects and represents a significant competitive advantage for some controllers. In this respect, it is from our point of view more important that the data subjects have the right to choose whether the personalization should be carried out or not.

In some cases, it seems to us that the requirement to processing being *strictly necessary* (for example in point 71) goes beyond the text of the GDPR. And, it may be reflected in other relevant legislation or processes where it is intended to prevent any other use or abuse of protected information.

The example in paragraph 77 does not seem to be practically constructed. Usually, the controller will process (at least) some of the data even after termination of membership at least for the purpose of the legitimate interest pursued by the controller or a third party (for example during a statutory limitation period to protect against potential legal claims). We understand

that this processing is done for a different purpose, but this example could be confusing for some controllers.

Although we understand the intention which is behind the requirement on data controllers to demand from technology providers information about cost of developing the solution compatible with Art. 25 of GDPR (see page 26), we would like to point out that such information would very often form a business secret of technology provider, which is also never publicly available.

Even though we agree with the criticality and necessity of certification processes on technology providers (see point 86), there should always be an open field for diversification of tools and suppliers across the market regardless of their size or the necessary possession of a specific certification. Especially for small businesses, there may be a risk of the vendor-lock, which could easily occur when targeting the largest providers offering a comprehensive package/box solution (all-in-one solution). Thus, it should be on every controller what he considers as the alternative instruments or guarantees other than certificated products.

We do not believe that GDPR requires to disclose to data subjects how the controllers are assessing effective DPbDD implementation (see page 27) although it could be seen as a best practice example and the strong sign of transparency.

**We are grateful for the opportunity to provide the above-mentioned comments on the Guidelines.**

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat at the address Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562