LB&P
LEGAL

**Comments form**

**PUBLIC CONSULTATION:** Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

**Name and address of the institution:**
**Leśniewski Borkiewicz & Partners (LB&P Legal)**
Warsaw, al. Solidarności 119/125, 67; 00-897 Warsaw, PL
Wroclaw, Podwale 83, 11 (OVO Wroclaw); 50-414 Wroclaw, PL

**Contact:**
Mateusz Borkiewicz; +48 663 683 888; mb@lbplegal.com
Grzegorz Leśniewski; +48 531 871 707; gl@lbplegal.com

EDPB's guidelines on the application of 'privacy by design' and 'by default' rules are key to the secure and stable development of the Digital Single Market in the EU. The following commentary points to areas where EDPB should make a clear statement in order to address the key concerns raised by the IT industry in the EU for further technological development.

These guidelines remain the right place for this. Without clarifying the following points – they will not fulfil much of the role that has been assigned to them under Article 70 GDPR.

| No. | page | pt / section no. | the content of the section of the guidelines | reservations / justification / direction of the proposed modification of the content |
|---|---|---|---|---|
| *Reservation area: unexplained technology provider's legal status in fulfilment of obligations under Article 25 GDPR* | | | | |
| **1.** | page 5th | pt 1st | The Guidelines focus on controllers' implementation of Data Protection by Design and Default (hereinafter "DPbDD") based on the obligation in Article 25 of the GDPR. Other actors, such as processors and **technology providers, who are not directly addressed in Article 25**, may also find these Guidelines useful in creating GDPR-compliant | Reservation: EDPB does not explicitly support the acceptance or exclusion of the possibility of controlling technology providers (TP) in terms of compliance with Art. 25 GDPR.<br><br>Currently in the guidelines: |

| | | | | |
|---|---|---|---|---|
| | | | products and services that enable controllers to fulfil their data protection obligations. | - on the one hand: statement in point 1 (page 5th) “[...] technology providers, who are not directly addressed in Article 25 [...]”;<br>- on the other: (I) TP's obligation to directly implement “privacy by design / by default” rules; (II) admission of TP to the certification system in scope of “compliance with the regulation” pursuant to Art. 42 GDPR (parts of the guidelines quoted in the left column);<br><br>Therefore, the guidelines raise doubts about the possibility of controlling and adopting corrective measures / imposing fines against TP for violation of Art. 25 GDPR.<br><br>Despite the fact that Article 83 of the GDPR provides for the possibility of imposing administrative fines only on controller or processor (TP does not act in such role), the potential assumption that TP is obliged to comply with “privacy by design / by default” rules opens the way to (examples show the relevance of the issue):<br>- application of Art. 84 GDPR (introduction of new / use of current national regulations to impose sanctions on TP for violation of Article 25 GDPR);<br>- assessment of solutions created by TP as 'unlawful' in the event of non-compliance with the requirements of Article 25 GDPR (as a result: i.a. placing on the market solutions incompatible with such obligations could be qualified as a ‘unfair competitive practice’ with all the consequences foreseen for such situations, including obligation to withdraw the solution from the market);<br><br>Leaving doubts regarding the possibility of assessing solutions created by TP in terms of art. 25 GDPR will also cause uncertainty in the application of future regulations - including planned changes in scope of liability of digital technology producers (European Commission Report “Liability for Artificial Intelligence and other emerging digital technologies” 2019). |
| **2.** | page 26th | indent 2nd | A processing operation may be certified for DPbDD. **Such a certification may provide an added value to a controller when choosing between different processing systems from technology providers**. A certification seal may also guide data subjects in their choice between different goods and services, such as applications, software, systems, Internet of Things, including wearables and implants. **Having a DPbDD-seal can therefore serve as a competitive advantage for both technology providers and controllers**, and may even enhance data subjects’ trust in the processing of their personal data. Where there is no certification, controllers should seek to have other guarantees that **technology and service providers comply with the requirements of DPbDD.** | |
| **3.** | page 26th | indent 6th | Technology providers should keep in mind that Article 25 requires cost of implementation to be taken into account in the design process. **This means that when developing a solution, technology providers should also take cost efficiency into account during the development of that solution and implement principles in an effective manner**. | |
| **4.** | page 26th | indent 9th | The EDPB recommends controllers to require that **technology providers demonstrate accountability on how they have complied with DPbDD**, for example by using key performance indicators to demonstrate the effectiveness of the measures and safeguards at implementing the principles. | |
| Proposed new wording: | | | Due to the imposition in Art. 25 GDPR obligations explicitly on the "controller", it is proposed to delete parts of the guidelines quoted in points 3rd and 4th above, and to introduce the following position:<br><br>"*Technology providers are not directly addressed in Article 25. This means that the solutions they create cannot be assessed by authorities for compliance with Art. 25. Verification of compliance with DPbDD occurs only at the stage of controlling the controller's activity and is not limited to the specific, individual solution provided by technology provider, but always refers to all technical and organizational measures implemented by the controller, which ‘as a whole’ should implement the principles of DPbDD. This does not exclude the use of DPbDD rules by the technology provider in the event of contractual regulation of such necessity with the controller or in the event of unilateral imposing such an obligation by the technology provider (however, the liability of the technology provider would only be contractual).*” | |

<table>
<tr><td colspan="5">Reservations area: giving the effectiveness requirement a priority over the other requirements</td></tr>
<tr><td>5.</td><td>page 4th</td><td>section 1st</td><td>These Guidelines give general guidance on the obligation of Data Protection by Design and by Default (henceforth “DPbDD”) set forth in Art.25 GDPR, where the core obligation is the effective implementation of the data protection principles and data subjects’ rights and freedoms by design and by default.</td><td rowspan="4">Reservation: the "effectiveness" requirement adopted as a key criterion for assessing compliance with "privacy by design / by default" rules.<br><br>Such an approach seems to be incompatible with the literal wording of Art. 25 GDPR. The provisions precisely indicate the premises that should be taken into account when assessing measures as meeting the requirements of "privacy by design / by default" rules, including: "the state of the art” and „the cost of implementation ".<br><br>Therefore, the controller should not be liable primarily for the effectiveness of implemented measures, as proposed in the guidelines.<br><br>In particular, inability to manage the costs of implementing fully effective technical and organizational measures may, in a specific case, exempt the controller from the obligation “to implement data-protection principles in an effective manner”.<br><br>It is proposed to apply to the "effectiveness" requirement under Art. 25 GDPR, the approach corresponding to the one used when assessing the effectiveness of measures implemented under Art. 32 GDPR (not every personal data breach means a violation of security requirements. The controller that implemented safeguards in accordance with the premises indicated in Article 32 GDPR, is not liable even if in a specific case such measures occurred to be ineffective to prevent a breach of data protection):</td></tr>
<tr><td>6.</td><td>page 5th</td><td>pt 2nd</td><td>The requirement is for controllers to have data protection designed into and as a default setting in the processing of personal data. The core of the provision is to ensure effective data protection both by design and by default […]</td></tr>
<tr><td>7.</td><td>page 6th</td><td>pt 10th</td><td>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.</td></tr>
<tr><td>8.</td><td>page 8th</td><td>pt 24th</td><td>[…] 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. 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.</td></tr>
<tr><td colspan="3">Proposed new wording:</td><td colspan="2">It is proposed to delete parts of the guidelines quoted in point 8th above, and to introduce the following position:<br><br>“The controller is not obliged to ensure the implementation of effective measures "at all costs". In a specific case, the inability to bear costs of implementing technical and organizational measures or unavailability of the relevant technology, may constitute grounds for exempting the controller from the obligation to implement data-protection principles in an fully effective manner. In such cases, the controller should implement measures which ensure the highest level of effectiveness from the available technology to controller and within controller’s reach, taking into account the costs of implementation.<br><br>In very exceptional cases, the controller should be obliged to ensure the implementation of the principles in an effective manner, even if he is not able to bear costs of such implementation (the alternative is to terminate the data processing operation). It should be noticed that according to Article 36 of the GDPR, even in the case where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, and controller failed to take measures to minimize it (also because he is not able to do so e.g. due to costs), the controller is not obliged to stop the processing operation, but to consult the supervisory authority at first.”</td></tr>
</table>

<table>
<tr><td colspan="5">Reservations area: too broad interpretation of the 'protect the rights of data subjects' obligation (to the detriment of controllers / technology providers)</td></tr>
<tr><td>9.</td><td>page 6th</td><td>pt 12th</td><td>The data protection principles are in Article 5 GDPR (hereinafter “the principles”), the data subjects’ rights are found in Articles 12 to 22, the data subjects’ freedoms are found in Recitals 4 and in the EU Charter of Fundamental Rights (hereinafter “the rights”). It is essential for the controller to have an understanding of the meaning of the principles and the rights.</td><td>Article 25 GDPR uses the term “rights”, which may be referred to the rights of data subjects granted under the GDPR (chapter III, Articles 12-22). However, the provision explicitly indicates that the obligation is "to integrate the necessary safeguards into the processing in order to protect the rights of data subjects.", referring directly to the area of ‘data security’ (as in Article 32 GDPR).<br><br>The term of "rights" used in Art. 25 GDPR should therefore only apply to data security guarantees, referring to the protection of rights and freedoms regulated in the EU Charter of Fundamental Rights.<br><br>If the legislator's assumption were to apply the rules of Art. 25 GDPR to the rights regulated in Art. 12-22 GDPR - the provision would provide for the "exercise of rights", as in Article 12 GDPR.</td></tr>
<tr><td colspan="3">Proposed new wording:</td><td colspan="2">It is proposed to amend part of the guidelines quoted in point 9th above, as follows:<br><br>“The data protection principles are in Article 5 GDPR (hereinafter “the principles”), the data subjects’ rights are found in Recitals 4 and in the EU Charter of Fundamental Rights (referred to as the “right and freedoms”). It is essential for the controller to have an understanding of the meaning of the principles and the rights.”</td></tr>
<tr><td colspan="5">Reservations area: accountability obligation in the scope of compliance with art. 25 GDPR</td></tr>
<tr><td>10.</td><td>page 4th</td><td>section 1st</td><td>Controllers must be able to demonstrate the effectiveness of the implemented measures.</td><td rowspan="3">The accountability obligation under the GDPR is always explicitly included in a specific provision (e.g. Article 5 (2), Article 7 (1) or Article 24 (1) GDPR). There is no such obligation in Art. 25 GDPR regarding implementation of “privacy by design / by default” rules.<br><br>This does not exclude the obligation of accountability for specific solutions covered by Article 25 of the GDPR, fulfilled during verification in individual cases (e.g. deletion of personal data as a implementation of the data-protection principle). Such verification provides an explicit legal basis – Art. 5 (2) GDPR.<br><br>Therefore, EDPB should not extend the obligation of accountability directly to Art. 25 GDPR. There is no legal basis for this approach, it may also results in practical difficulties:<br>- the SME sector, primarily implementing 'off the shelf' technical measures, will often not be able to demonstrate effective DPbDD implementation of a specific solution without a link to individual case;<br>- specific solution provided by the technology provider can be assessed as DPbDD-compliant (or not) only along with all other technical and organizational measures implemented by the controller;</td></tr>
<tr><td>11.</td><td>page 7th</td><td>pt 14th</td><td>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.</td></tr>
<tr><td>12.</td><td>page 27th</td><td>indent 11th</td><td>Controllers should […] demonstrate effective DPbDD implementation, in the same manner as controllers demonstrate compliance with the GDPR under the principle of accountability.</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | | | | |
| Proposed new wording: | | | It is proposed to delete parts of the guidelines quoted in points 10th – 12th. | |
| *Reservations area: too broad interpretation of the 'privacy by default' obligation (to the detriment of controllers / technology providers).* | | | | |
| **13.** | page 10h | pt 40th | […] data protection by default 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 program 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. | Reservation: extension of the 'privacy by default' obligation to areas other than indicated in art. 25 (2) GDPR.<br><br>This causes a risk of violating the principle of legal certainty by introducing an open catalog of obligations (the controller cannot assess the scope of the obligation under "privacy by default" rule) and enabling authorities to impose fines against controller for not fulfilling unspecified obligations. |
| Proposed new wording: | | | It is proposed to amend part of the guidelines quoted in point 13th above, by deleting the following fragment:<br>"[…] in particular but not limited to [...]" | |
| *Reservations area: certification system for technology providers (in scope of 'data protection by design and by default')* | | | | |
| **14.** | page 26th | indent 2th | A processing operation may be certified for DPbDD. **Such a certification may provide an added value to a controller when choosing between different processing systems from technology providers**. A certification seal may also guide data subjects in their choice between different goods and services, such as applications, software, systems, Internet of Things, including wearables and implants. Having a DPbDD-seal **can therefore serve as a competitive advantage for both technology providers and controllers**, and may even enhance data subjects' trust in the processing of their personal data. Where there is no certification, controllers should seek to have other guarantees **that technology and service providers comply with the requirements of DPbDD**. | Due to the admission of technology providers to the certification system pursuant to Art. 42 GDPR (in scope of meeting the requirements of "privacy by design / by default" rules), this mechanism should be precisely described in chapter 4 "Certification" (page 24th of the guidelines).<br><br>Purpose: removal of possible doubts caused by admission to the certification mechanism a group of entities that generally does not act as either a controller or a processor (enabling certification contrary to the literal wording of Article 42 GDPR: "[...] certification mechanisms [...] for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors."). |
| *Reservations area: others* | | | | |
| **15.** | page 7th | pt 15th | It should be noted that the measures and safeguards should be designed to be robust and **be able to be scaled up in accordance with any increase in risk of non-compliance with the principles**. | EDPB does not explicitly underline the acceptability for limitation of expenses on data protection in the event of changes to the processing circumstances indicated in Article 25 GDPR (i.a. due to the increasing costs of maintaining appropriate technical measures and the worsening financial situation of the controller). |

| | | |
|---|---|---|
| Proposed new wording: | It is proposed to introduce the following position:<br><br>"*It is allowed to limit expenses on data protection in the event of changes to the processing circumstances indicated in Article 25 GDPR (i.a. due to the increasing costs of maintaining appropriate technical measures and the worsening financial situation of the controller).*<br><br>*In some situations, nominally the same data protection costs over time may place a greater burden on the controller than at the implementation stage. Such cases imply a change in the "costs of implementation" which, according to Art. 25, shapes the scope and manner of implementing obligations resulting from the "privacy by design" principle*." | According to the guidelines - "cost of implementation" should be understood as costs occurred not only at the stage of implementation of the technical / organizational measure, but also throughout its lifetime. What is more, as EDPB points out, costs are not only meant in terms of money or economic advantage. Cost, in this context, refers to resources in general, including time and human resources.<br><br>In the event of income reduction / reduction of employment, nominally the same data protection costs may place a greater burden on the controller than initially, compared to his financial situation. Such cases imply a change in the "costs of implementation" which, according to Art. 25 GDPR, shapes the scope and manner of implementing obligations resulting from the "privacy by design" principle.<br><br>EROD should explicitly allow limiting expenses on data protection in these situations. The issue should be considered as important not only for the security of controllers who are in temporary financial problems (e.g. due to the financial crisis / recession) but also for the development of the digital single market in the EU as such. The alternative to allowing limitation of expenses is the obligation to stop certain processing operations (including those valuable from the point of view of the interests of data subjects and sometimes also technological progress – i.a. data processed by research and development centers). There is a need to clearly support the possibility of reducing costs in above situations. |