EDPB Guidelines 4/2019 Data Protection by design and by default
Feedback by the members of the
Luxembourgish National GDPR Working Group for Research

Regina Becker, ELIXIR-Luxembourg, Luxembourg Centre for Systems Biomedicine (LCSB)
Anne Drochon, National Cancer Institute (INC)
Chloë Lellinger, Luxembourg Institute of Socio-economic Research (LISER)
Sandrine Munoz, University of Luxembourg
Marc Pauly, National Institute of Statistics and Economic Studies of the Grand Duchy of Luxembourg (STATEC)
Laurent Prevotat, Luxembourg Institute of Health (LIH)

Contact for the group: Regina.Becker@uni.lu

Summary of feedback

We appreciate the comprehensive overview on adherence to the data protection principles that is provided by the EDPB Guidelines 4/2019 on Data Protection by Design and Default (DPbDD). However, we found that the Guidelines seem unbalanced towards the aspects related to "effectiveness" and missing out on providing more guidance on the "by design and default" aspects for the planning of the processing. Similarly, the accountability principle is taking much room in the document. While these aspects are important elements of the GDPR, the principle of DPbDD, which is governed by Art. 25, should be more in the focus of the Guidelines. We would like to encourage the EDPB to include the in-depth discussion of these aspects on future Guidelines and provide a more focussed guidance on the consequences of "by design" and "by default" in the light of an advance planning and anticipation of inherent data protection in the processing. This should ideally include relevant sector specific discussions and examples as processing situations differ widely such as between scientific research and internet services for example. Such considerations would improve very much the practical guidance that was proposed in the Executive Summary.

In addition, we believe that the intention of the legislator of addressing efficiency rather than effectiveness only had not been captured in the current draft of the Guideline. A discussion of this aspect is an important element that also deserves room in the considerations on DPbDD.

In the same context of proportionality of efforts, we have some doubts on the way the documentation efforts were indicated in the Guidelines. To require a full documentation of all possible risk on all possible aspects of the data processing as it transpired in the document seems outside the intention of the GDPR. More guidance in the sense of proportionality with criteria for what makes documentation important and reasonable allowing a prioritisation would be a helpful guidance, that could be provided in a future guideline on accountability.

Recommendations by the Working Group

- **Re-adjust the focus on aspects of design and default on the aspects of**
  - **planning in advance appropriate technical and organisational measures and analysing the processing conditions and context to set up the processing in a way that the data protection principles are implemented.**
  - **and ensuring that processing conditions as well as the platforms engaged have a default setting to foresee privacy and fairness of processing for the data subject.**

In its current formulation, the guidelines rather give the impression to be a recapitulation of the entire GDPR, with a strong focus on the notion of effectiveness of a measure. In the recapitulation, an unnecessary room is given to the aspect of "effectiveness" – the idea appears actually no less than 9 times in the Executive Summary alone, thus indicating the major focus of the document.

From our point of view, the discussion of what accounts as appropriate measures and the necessity to demonstrate the processing in accordance with the GDPR is more appropriate if a guideline on the

obligations of the controller were compiled (Art. 24). Indeed, while Art. 25(1) repeats largely Art. 24(1), the aspect of demonstrating GDPR compliance is not included. Therefore, we do not follow the conclusion of section 2 of the Guidelines that specifies on DPbDD "*The core of the provision is to ensure effective data protection both by design and by default, which means that controllers must be able to demonstrate that they have in place the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective*." We believe that even though the guidance provided by the EDPB on the effectiveness of organisational and technical measures and its demonstration is very important, it is out of scope for a guideline on DPbDD.

For this reason, we would also like to question the definition given in (14) that the "heart of the concept of data protection by design" is effectiveness. Effectiveness should be at the heart of any technical or organisational measure for data protection. We would like to propose to the EDPB to consider that the heart of data protection by design is the ANTICIPATION of the practical consequences to ensure the implementation of the data protection principles into the processing and the IMPLEMENTATION of these principles consequently in the design of the processing. Such anticipation will lead to the design of organisational and technical measures whose effectiveness should demonstrated as part of Art. 24 (and thus discussed in the light of Art. 24 rather than Art. 25).

- **Further enrich the case illustrations by covering a broader space, considering more examples that address organisational measures, a more varied selection of use cases that represent different sectors, clarifying the measures towards their effect and emphasising elements that are specific for the aspect of the "by design and by default" principles**

Examples are always an important tool to elucidate the generic principles and create a better understanding for the practical implementation. We appreciate that the EDPB aimed to provide examples for all principles. We do believe though that the effect of the example provision could be enhanced if the aspect of "design and default" were more emphasised, if the application fields were more varied and if the relation between measure and effect would be more explained.

For instance, section (11) refers to pseudonymisation as safeguard to implement a number of principles, such as the integrity and confidentiality and data minimisation. It is not clear how pseudonymisation relates to the integrity principle. Furthermore, the phrasing of "implement principles" rather than "contributes to" suggests that the requirements of these principles may be entirely fulfilled by pseudonymisation alone, which is not necessarily the case.

We would further appreciate if the chapters 2.1.4 (Time aspects) and 2.2 (Data protection by default) were enriched with examples. In other examples, in particular in Part 3, the information provision and in many cases the corresponding examples are of a very generic nature. More explicit reference of what makes the "by design" or "by default" element in such examples would be appreciated as the Guidelines on DPbDD will be an important reference for the controllers in the conception of their processing in the future.

We would also welcome if more examples included organisational measures. We appreciate the explicit reference in section (21) to state of the art organisational measures considered in DPbDD as often organisational measures are overlooked in DPbDD. This principle is often interpreted as a purely technical measure, despite the explicit reference to organisational measures in Art. 25. We would appreciate if more examples for effective organisational measures would also considered in the examples of Part 3 in the document as otherwise the examples might further support the conception of the mostly technical nature of DPbDD. An organisational measure to support fairness as well as many other principles in data protection (e.g. necessity to process the data, data minimisation, storage limitation) is the ethical review in health research. While this measure is specific for this particular domain, it could be well worth considering to extend such approaches to research with personal data in general or to the application of new technologies such as Artificial Intelligence.

In this context, we would also like to point out that we have observed the most examples to target the world of service provision. We believe the discussion of specific sectors with their corresponding

challenges as e.g. done by the EDPB in the Guidelines on Consent would improve the value of the recommendations. Here, we would also like to refer to the recent Preliminary Opinion of the European Data Protection Supervisor (EDPS) on Data Protection and Scientific Research that stated the necessity that the specific aspects the interpretation of the GDPR for scientific research needs much more elucidation. In the need for more sector-specific guidance, we also agree with the EDPS that an encouragement by the EDPB for codes of conduct around research topics would be very helpful. Therefore, the consideration of the discussion of the guidelines in the research context (where relevant) would be very much appreciated. We would be happy to provide input to such discussions and to examples from the experience made in Luxembourg.

- **Discuss appropriate safeguards and the cost of implementation as part of a balancing exercise for efficiency rather than effectiveness only**

Section (24) refers to the fact that the cost for appropriate data protection measures needs to be planned and factored in advance. While we agree with this approach, we believe that the motivation of the legislator to include the reference to cost in Art. 25 is not (solely) the aspect of anticipating such cost. We would like to point out that the same consideration is used in the phrasing of Art. 32 while it is notably omitted in Art. 24. We believe the motivation of the legislator to be an indication that decision making criteria for the selection of measures can be based on efficiency rather than on effectiveness only. Efficiency means that the effectiveness of a measure can be balanced against the cost. Compromises between effectiveness and cost should be done based on the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. A measure may be perfect but if it is too expensive, and here indeed not just the monetary costs but also other consequences need to be considered, alternatives could be an option. Other measures that may not be quite as effective but cheaper could be deemed as sufficient, in particular where the risks to the rights and the freedoms of the data subject in the processing are limited or already largely reduced due to the implementation of other measures. However, we fully agree with the EDPB that the avoidance of high cost alone is no reason to exclude relevant technical or organisational measures. Therefore, we would like to suggest to the EDPB that the aspect of cost should not be discussed entirely uncoupled of the aspects of the processing and the risk as currently done through section (24) on cost on the one hand and on effectiveness in sections (25,26) on the other hand. We would appreciate a discussion on the possibility to perform a balancing exercise to assess the efficiency of measures based on effectiveness and cost in the light of the nature, scope, context and purposes of processing.

- **Compile a guideline on "accountability" as a new principle under the GDPR as the scope of documentation requirements is still unclear**

We have observed that in the current Guidelines, documentation efforts are suggested that could lead to a tedious over-documentation, such as in section (35) of the DPbDD Guidelines. If consequently pursued for all possible means (from architecture aspects to individual protocols as suggested in section (33)), and combining this with risk assessments including metrics as e.g. postulated in section (16), this would amount to enormous efforts and does not seem to comply with the intention of the GDPR to reduce red tape. In particular, the consequent implementation of the suggested efforts appears to go beyond the requirements of Art. 35 that require a full and extensive risk analysis and corresponding assessment of impact only for processing with a high risk. Therefore, criteria for the documentation needs for different aspects to comply with the accountability principle under the GDPR and the discussion of the principle in the light of proportionality are both subjects where recommendations by the EDPB would be very welcome by data controllers throughout Europe.