16 January 2020

EBF_039779

# EBF response to the European Data Protection Board's consultation on the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

**Key points**:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's consultation on the draft guidelines on Article 25 Data Protection by Design and by Default (DPbDD).
- We welcome the clarifications provided by the EDPB in its guidance, however, we believe further ones are needed, particularly regarding implementing data protection principles in the processing of personal data using DPbDD. We would also encourage the EDPB to recognize the specific legislation and EBA Guidelines, Recommendations and Opinions (in the case of the financial sector) as this will shape the implementation of DPbDD for sectors.
- We welcome that the draft Guidelines recognize processors and technology providers as key enablers for DPbDD and ask for further clarifications in the guidelines to reflect their role and responsibilities.

## EBF position:

The European Banking Federation (EBF) welcomes the European Data Protection Board (hereafter 'E-DPB') draft guidelines on Article 25 Data Protection by Design and by Default (hereafter DPbDD) and the opportunity to respond to this consultation.

You will find below some general and some technical comments on the draft guidelines.

**European Banking Federation aisbl**

**Brussels /** Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
**Frankfurt /** Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
**EU Transparency Register /** ID number: 4722660838-23

**www.ebf.eu**

## 1. General Comments

The **risk-based approach should be applied to implementation of DPbDD**, which allows controllers to concentrate on the systems and applications which are used regularly or may contain risky elements to privacy. The responsibility of technology providers should also be addressed, and we welcome that the draft guidelines recognize the role of technology providers as key enablers of DPbDD.

It is also important to note that, when implementing DPbDD, financial services providers can face challenges in relation to old legacy IT systems, compared to newer IT systems. In addition, the examples provided in the guidelines relating specific industries (e.g. financial sector on page 21), should take into account the specific legislation and EBA Guidelines, Recommendations and Opinions pertaining to that sector, as this will also shape their implementation of DPbDD.

Finally, the draft guidance incorporates concepts which have either already been the subject of other Guidelines (e.g. transparency, consent, Article 6.1.(b), automated decision-making etc.) or of an "opinion" (anonymization, pseudonymization). To avoid the risk of creating contradictions, we suggest to clarify that these guidelines do not override them and refer to, where necessary, previously adopted guidelines and opinions, instead of re-drafting principles which were already the subject of guidance.

## 2. On the controller's obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing

In paragraph 10 (page 6), the draft guidance lists examples of safeguards to secure data subjects' rights including "*enabling data subjects to intervene in the processing".* However, intervention lacks a clear definition in this context, which could cause issues in certain business environments, for example, where data processing is also performed to meet a legal obligation (e.g. compliance with the Anti-Money laundering Directive, Payment Services Directive). We would therefore welcome a clarification in the guidance that "*enabling data subjects to intervene in the processing" is* not feasible in all business environments. We would also suggest to include an example as to the type of "automatic and repeated information" to be provided, such as privacy notices and policies.

## 3. On elements to be taken into account when implementing data protection by design

"Cost of implementation" is included as one of the elements to be taken into account and paragraph 24 (page 8) of the draft guidelines states that "*Incapacity to bear the costs is no excuse for non-compliance with the GDPR*." However, as Article 25 GDPR inherently defines a certain proportionality for the implementation of privacy by design and by default, it shall be considered that no disproportionately high demands shall be placed on controllers, especially for existing systems, where adaptions are often difficult to achieve in a proportional manner. We therefore suggest the following amendment:

**EBF Suggested amendment:**

24. *"…The controller must manage the costs to be able to effectively implement all of the principles. Incapacity,* ***as long as the proportionality (including costs) is given****,* ~~***to bear the costs***~~ *is no excuse for non-compliance with the GDPR..."*

EDPB Draft Guidelines on the DPbDD, page 8.

In relation to paragraph 30 (page 9), we query how controllers should use the Data Protection Impact Assessment (DPIA) guidelines in the context of Articles 24 and 25. Although these articles require controllers to consider the level of risk associated with the processing, this should not generally be the same as under a full DPIA, which is only required for *high risk* processing. We recommend that the guidance clarifies that, although the DPIA guidelines can be a useful *reference*, it is not necessary under Articles 24 and 25 to do a full assessment as per Article 35(7).

Also, in paragraph 31 (page 9), the draft guidance states that "*controllers…****must always carry out an assessment of data protection risks for the processing*** *activity at hand ….*" , which seems to imply that a DPIA should be extended to all cases. We therefore suggest clarifying that the expectation is for the firm to assess the risk under Article 35(1), not to do a full DPIA. In addition, the EDPB previously released Opinions on DPA's draft lists of the kind of processing operations which are subject to the requirement for a Data Protection Impact Assessment under Article 35(4).

## 4. On the implementation of DPbDD at the time of determination of the means for processing

In paragraph 35 (page 10), in relation to the assessments required under paragraph 34, the draft guidelines state that "*controllers must demonstrate that such assessments have been made for* ***all of the means*** *that are part of the processing*." Given the "means for processing" is a vague and abstract term under the draft guidance, it is not practical to say that "all of the means" must be considered. In addition, the word 'means' lacks a clear definition in this context. Needing to demonstrate that 'all of them' have been considered would therefore not be possible. Instead, the guidance should recommend a *comprehensive assessment* of the means.

Regarding the reference to "regular reviews" in paragraph 37 (page 10), we suggest for the draft guidance to clarify that controllers can determine their own review periods, as appropriate in the context of the processing.

In paragraph 38 (page 10), the draft guidance writes that: "***Processors' operations should be regularly reviewed and assessed*** *to ensure that they enable continual compliance with the DPbDD principles and support the data controller's obligations in this respect*." We would like to flag that the intention to use a processor is sometimes driven by the lack of IT-knowhow within the organization of the controller. Therefore, we recommend the guidelines acknowledge the possibility to perform the necessary reviews, through considering guarantees, as provided for under (Article 28 (3h)), requiring

external/internal audits, as possible alternatives to "regular reviews" of processor operations

## 5. On data protection by default

In paragraph 41 (pages 10-11), the draft guidance mentions the use of 'third party software': " ***If the controller uses third party software*** *or off-the-shelf software, it is vital that functions that do not have coverage in the legal grounds or are not compatible with the intended purposes* ***are switched off****."* However, controllers may face significant difficulties and a complex process to switch off the functions, as it is third party software. We suggest amending the draft guidelines to acknowledge this. In addition, the processor may themselves not be able to switch off a certain function, especially if the software is a standard one. In this case, it is hard for the controller to negotiate with the processor and the controller may have a 'take it or leave it' choice.

Paragraph 46 (page 11) of the draft guidelines references the 2019 guidelines of the European Data Protection Supervisor (EDPS) *on assessing the necessity and proportionality of measures that limit the right to data protection*. We recommend to delete this reference. The EDPS, governed by Regulation 45/2001[1], does not have the power to enact guidelines on the application of the GDPR. According to Regulation 45/2001, the EDPS is responsible for ensuring that the fundamental freedoms and rights of individuals, including their privacy, are respected by Community institutions and bodies. While the EDPS participates in the work of the EDPB with the right to vote, with exceptions, it cannot replace it in terms of interpretation of the GDPR. The publication of GDPR guidelines remains an exclusive competence of the EDPB (Article 70(1) of the GDPR). Therefore, the reference to the EDPS guidelines exceeds the provisions of the GDPR and Regulation 45/2001.

## 6. Implementing data protection principles in the processing of personal data using data protection by design and by default

In this section, we would like to suggest specific amendments to the following key DPbDD elements (covered in pages 14-23 of the draft guidelines): transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy and storage limitation.

### Transparency

Whilst we support a 'clear and open' approach in relation to notice on how individuals' data will be collected, used and shared we would like to emphasize that the financial services sector is required by law to process certain personal data for anti-fraud prevention, anti-terrorism and anti-money laundering (AML), market abuse and other purposes.

[1] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

We would therefore welcome an addition to the guidance recognising that **meeting the principle of transparency needs to be balanced against these other regulatory and legal obligations**; privacy notices cannot be too granular in their description of processing and algorithms to prevent fraud, money laundering and terrorism, as too much information would risk undermining the purposes of the processing. If there is too much information on how the AI / algorithms work, this would increase the risk of these systems being abused or deceived by fraudsters, terrorists and money launderers.

We also note that "multi-channel provision of information", listed in paragraph 61 (page 14) can be helpful in some contexts, for example, when dealing with consumers. However, in other contexts this will not be appropriate, for example when data subjects are highly sophisticated and being dealt with in a business context, or when the processing is very simple. The draft guidance should be amended to make clear that multi-channel information should be considered when appropriate to the context and specific processing. In the same paragraph, the draft guidance states that privacy information should be "machine readable". It is not clear why this should be the case, given the goal of privacy notices is to inform data subjects, or what exactly it would mean in this context.

Lastly, we recommend that the notion of obliging the controller to inform the data subject in the "*right context, at the appropriate time*", mentioned in the example on page 14, is clarified. It would be helpful for the guidance to acknowledge that what is appropriate will vary depending on the context and the sector. The draft guidance currently suggests that this principle requires provision of more notifications when processing occurs. For example, in financial services, certain personal data must be processed every time a transaction is processed, but it would clearly not be in data subjects' interests to receive a privacy notification each time they make a or receive a payment. It is also important to mention that there may be different financial, risk and credit controllers who all respectively have their own obligations.

## Lawfulness

One of the elements proposed under paragraph 63 (page 15) is consent withdrawal. We recommend to amend this bullet to clarify that the right to withdraw consent only applies if consent is the basis for processing. In financial services, firms must frequently rely on the other bases such as the performance of a contract, a legal obligation or the legitimate interest of the controller or a third party.

**EBF Suggested amendment:**

63. (bullet point 3) "*Consent withdrawal – The processing shall facilitate withdrawal of consent, **where consent is the legal basis for processing**. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid.*"

EDPB Draft Guidelines on the DPbDD, page 15.

It is also not clear why the draft guidance in the paragraph 63 (page 15) suggests maximising the level of data subject autonomy in the context of 'lawfulness'. If this is

intended to suggest that controllers should seek to rely on 'consent' as much as possible, this is not in line with Article 6. We suggest to clarify this bullet. Also, there is no specific requirement in the GDPR for controllers to disclose their "balancing of interests" assessments,

Lastly, we would recommend to delete the example provided in this section (page 15). The example contradicts with credit risk management requirements and there are concerns about the interpretation, that by using the example, one could get the impression that (parts of) the processing cannot be based on another legal ground e.g. for performance of a contract. The bank may need to verify the documents provided by the customer and there might be also specific national legislation in place, which sets up strict requirements to verify income.

## Fairness

In paragraph 64 (page 16), the guidance states that in order to achieve fairness, "*personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject*". However, intervening in fraudulent transactions, preventing terrorism, identifying market abuse, rejecting credit applications from customers that will not be able to make repayments, etc, are actions by financial institutions that could be interpreted as 'detrimental' to the data subject. **These are legitimate processing activities that are in the public interest which in these circumstances would outweigh the rights of the particular data subject**. We therefore recommend amending this paragraph of the guidance to make clear that processing is only unfair if it leads to unjust adverse effects.

The guidance on 'power balance' in paragraph 65 (page 16) should be amended. The GDPR text only refers to 'power imbalance' in the context of processing based on 'consent', not other processing. It would be advisable for the guidance to recognize this.

We would also recommend to amend the guidance on human intervention in paragraph 65 (page 17), which currently states that "*The controller must incorporate **qualified human intervention** that is capable of recovering biases that machines may create in relation to the right to not be subject to automated individual decision making in Article 22.*"

First of all, this section should be amended to make clear that the right to obtain human intervention only applies when Article 22(3) applies, not to all uses of automated decision-making. We would also welcome a clarification as to whether this is an obligation falling under Article 25, or if it is a derivative of the requirements under Article 22. Secondly, there is no clarity on *how* the required qualified human intervention can be achieved. We recommend the guidelines refer to the adopted WP29 Guidelines on Automated individual decision-making and profiling, which specify that the person must have the authority and competence to change the decision.

Lastly, we would recommend better recognising, after paragraph 65, that data subjects have a range of interests that firms should take into account when determining fairness, in addition to privacy and data protection. We would therefore suggest adding the following into the draft guidance: "*In considering fairness, controllers should take into account the*

*interests of data subjects. This includes not just privacy rights, but also their interest in receiving quality services and relevant information, including advertising. Firms should consider any trade-offs between these interests carefully, along with the data subjects' expectations*."

**Purpose limitation**

It is common that there are several legal grounds and legitimate purpose for processing at the same time. For example, customer data is collected in order to set up the customer relationship, to offer specific investment product and to comply AML requirements. Additional requirements could also appear afterwards, meaning they cannot be taken to account when designing the processing. Further processing of data should be allowed, for example to comply with legal requirements. Article 6 provides data controllers the possibility to reuse the data when new/other purpose complies with the requirements as stated in Article 6(4).

**Data minimisation**

In paragraph 70 (page 19), the guidelines state "…. *if the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the controller shall anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights."*

The principle of minimization, which guarantees adequate and pertinent processing, cannot take place through anonymization, given that anonymization is an irreversible process that entails, in other words, the erasure of data. However, to the extent there is a processing purposes to be fulfilled (e.g. for the performance of a contract or for compliance with a legal obligation) the personal data cannot be anonymized, and they shall be kept identifiable. This concept should be clarified in the paragraph.

Please also note, that in Article 25, reference is made to pseudonymization. This is only one of the possible security and technical measures to ensure the fulfilment of GDPR principles. The data controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing shall decide which are the most appropriate technical and organizational measures to be adopted.

In general, it would be helpful for the EDPB to recognise in this part of the guidance that there is **a tension between the principles of 'data minimisation' and 'accuracy' in the context of machine learning (ML)**. ML apps require large amounts of data to work effectively and give accurate outputs. The guidance should recognise that firms will need to consider the tension between these principles and strike the appropriate balance in the context of machine learning. An example recognising the need to manage this balance could be helpful.

## Accuracy

Example 1 (page 21) uses the case of a bank using AI to profile customers applying for bank loans. The example states that the bank tests for reliability and non-discrimination, then ultimately determines that it will "***never rely solely on the AI to decide whether to grant loans*.**" **However, it does not explain why the bank makes this decision**, which is ultimately unrelated to the explanation provided on the accuracy of the results.

Though not explicit, this seems to *imply* that banks cannot use AI to grant loans, which goes against the provisions of Article 22 and the accountability principle, which requires the controller to implement appropriate technical and organisational measures. The use of AI and machine learning tools in fully automated processing is nowadays more widespread and pervasive and is becoming more widespread in the financial industry. AI and ML provide significant opportunities to enhance financial institutions risk analysis capabilities, both helping more people to access financing, while also improving the sustainability of the financial system. **As a result, the implication of this example risks significantly limiting the use of automated processing by banks.**

The guidance should be amended to **make clear that automated decisions are permitted under GDPR if the Controller meets the requirements of Article 22 GDPR**. The example should therefore be amended to:

**EBF Suggested amendment:**

Example 1. *Finally, the bank tests whether the AI is reliable and provides non-discriminatory results. When the AI is fully trained and operative, the bank uses the results as a part of the loan assessments****. ~~and will never rely solely on the AI to decide whether to grant loan ns.~~***

EDPB Draft Guidelines on the DPbDD, page 21.

In the example, we would also recommend to replace the highlighted in the phrase "*to ensure that the data used for AI training is as accurate as possible,* ***the controller only collects data from data sources with correct and up-to data information"*** with ", information known to be incorrect or not up to date shall not be used to train the AI*."*

## Storage limitation

Given the growing role of machine learning, it would be helpful for this section to acknowledge that retention of data for the purposes of data discovery and algorithm training can be legitimate, provided appropriate safeguards and limitations are in place.

## 7. Role of technology providers

Given the increasing prominence and reliance on technology providers, **we welcome that ,in paragraph 85 (page 25), processors and technology providers are recognized as key enablers for DPbDD** and that *"they are in a position to identify the potential risks that the use of a system or service may entail, and are more likely to be up to date on technological developments".*

We would also like to highlight that:

- A technology provider may also be an independent or joint Data Controller.
- Technology providers often provide pre-designed off the shelf solutions.
- Equally, technology providers often insist on signing their own off the shelf standard terms and conditions.
- A technology provider is more likely to have expertise and "state of the art" technology solutions and this may be one of the main reasons for seeking an external provider.

**We therefore advise to amend the recommendations included in the guidance (pages 25-26) to reflect the role and negotiating power of many technology providers. Specifically:**

- Paragraph 85: We are of the view that it is important to state that technology providers may be a Data Controller in their own right, making Article 25 directly applicable. We therefore suggest the following amendment to the text:

**EBF Suggested amendment:**

85. "*When processing on behalf of controllers, or providing solutions to controllers, technology providers should use their expertise* ***in designing and providing solutions*** ~~***and seize the opportunity to build trust and guide their customers in designing solutions***~~ *that embed data protection into the processing. Processors and technology providers should also* ~~***be aware that controllers***~~ ***ensure that their end users, like themselves,*** *are required to only process personal data with systems and technologies that have built-in data protection*".

EDPB Draft Guidelines on the DPbDD, page 25.

The guidelines should also clarify in paragraph 85 that technology providers should play an active role in detecting and notifying new risks/threats and should therefore be required to regularly assess the effectiveness of the measures taken.

- Paragraph 86 (bullet 2): The draft guidelines guidance state that: "*where there is no certification, controllers should seek to have other guarantees that technology and service providers comply with the requirements of DPbDD*." We suggest to amend the text to:

**EBF Suggested amendment:**

*"Where there is no certification,* ***technology providers should provide*** ~~***controllers should seek to have***~~ *other guarantees that technology and service providers comply with the requirements of DPbDD,* ***where appropriate controllers should request technology providers to provide these guarantees"*****.**

EDPB Draft Guidelines on the DPbDD, page 26.

- Paragraph 86 (bullet 3): We welcome that, as a minimum, the draft guidance recommends that *"technology providers should seek to support controllers in complying with DPbDD".* **Since a technology provider often supplies pre-designed off the shelf solutions, their role in compliance is pivotal**. However, the point goes on to read that *"Controllers, on the other hand, should not choose providers who do not propose systems enabling the controller to comply with Article 25, because controllers will be held accountable for the lack of implementation thereof".* This is very problematic, as it ignores the point that a technology provider will often be a controller in its own right and if so, will therefore also be accountable for providing solutions which do not embed or allow for compliance with GDPR requirements.

- Paragraph 86 (bullet 4): We welcome the EDPB's guidance that technology providers should play an active *role in ensuring that the criteria for the "state of the art" are met (paragraph 86, bullet 4)..etc., a*nd would propose the following amendment to reinforce this:

**EBF Suggested amendment:**

*"Technology providers should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures they have in place. Controllers* ***and technology providers*** *should include this requirement as a contractual clause to make sure they are kept up to date".*

EDPB Draft Guidelines on the DPbDD, page 26.

- Paragraph 86 (bullet 5): We have some reservations on the cost element covered in bullet 5. As alike businesses, banks reserve the right to decide on their operations, means, and timing for cost effectiveness. In addition, Article 25 of the GDPR calls for proportionality to the extent it states *"the cost of implementation"* is to be taken into account as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

- Paragraph 86, (bullet 6): the draft guidelines state that "*controllers should demand that their technology providers are transparent and demonstrate the costs of*

*developing the solution."* Yet, technology providers should themselves be transparent and demonstrate the costs of developing the solution. We would therefore propose the following amendment:

**EBF Suggested amendment:**

*"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.* ***Technology providers should be transparent and demonstrate the costs of developing the solution. Controllers, where appropriate, should request the same.*** ~~***demand that their technology providers are transparent and demonstrate the costs of developing the solution***~~*."*

EDPB Draft Guidelines on the DPbDD, page 26.

- Paragraph 86 (bullet 9): As technology providers often provide pre-designed, off the shelf solutions we would suggest the following amendment:

**EBF Suggested amendment:**

*"The EDPB recommends controllers* ~~***to require***~~ ***to request*** *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****. In cases where technology providers supply off the shelf terms and conditions, technology providers should demonstrate accountability on how they have complied with DPbDD."***

EDPB Draft Guidelines on the DPbDD, page 26.

- Paragraph 86 (bullet 11): As the draft guidelines state that the data controller should demonstrate compliance, the guidance should make it clear that the recommendations presented are indeed recommendations, and not obligations. GDPR requires proactive diligence by establishing principles.

Overall, it is submitted that Article 25 requires *"technical and organisational measures"* through appropriate measures and necessary safeguards. We would like to emphasize that these guidelines should consistently and proportionately reflect this requirement whilst also recognising the increasing prominence and reliance on technology providers be it in their capacity of a Data Processor or Controller.

Finally, while Article 25 does not mention data processors specifically, Article 28 specifies the considerations the controller must take whenever selecting a processor. For example, controllers must only use processors that provide *"sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing*

*will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."* This also covers DPbDD in Article 25

Given that technology providers may act as processors and often supply predesigned off the shelf solutions and, are in a position to identify the potential risks that the use of a system or service may entail, and are more likely to be up to date on technological developments, we recommend that the guidance clarifies the necessity to integrate the respect of the DPbDD principles into the Data Processing Agreement (Article 28(3)).

**ENDS**

**For more information:**
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

**About the EBF**

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

**www.ebf.eu @EBFeu**