09 June 2026

EBF_ 047004

# EBF response to the European Data Protection Board's consultation on its Template for Data Protection Impact Assessment ("DPIA")

**Key points**:

- While the draft EDPB DPIA template and accompanying "Explainer" have clear potential to support EU-wide harmonisation, in their current form they are overly complex, duplicative and insufficiently aligned with the operational realities of (medium-to-large) organisations, while in several respects exceeding the requirements under Article 35 GDPR.
- The EDPB DPIA template should remain a voluntary, non-binding tool intended to support, rather than rigidly standardise, DPIA practices. It should not be conceived as a one-fit-all solution; rather controllers should remain free to use alternative methodologies or templates, thus recognising established practices and sectoral/organisational needs.
- A stronger focus on methodology, proportionality and consistent risk language would significantly improve its practical value.
- In light of the interplay between the GDPR and the AI Act, the DPIA template should ensure, to the greatest extent possible, alignment between DPIA requirements and the Fundamental Rights Impact Assessments (FRIAs) under the AI Act.

## General Remarks

We welcome the intention of the EDPB to support EU-wide harmonization of the DPIA Template. While specific comments on specific sections are provided below, we would like to highlight the following points.

### ➢ Guiding principles: voluntariness, flexibility, and adaptability

As stressed in our previous contribution to the EDPB consultation on Compliance Templates[1], **an EDPB DPIA template should be guided by the principles of voluntariness, flexibility, and adaptability**.

While the EDPB clarifies that the DPIA template is intended as a voluntary and supportive tool for controllers, the indication that all DPAs will align their practice with the EDPB template as a standard or meta-template ("*Following the public consultation, all Data Protection Authorities will initiate the necessary steps to adopt this template either as their sole standard or as a 'meta-template' to which national-specific templates will align*"[2]) may

[1] EBF, EBF Response to the EDPB's consultation on Compliance Templates

[2] EDPB, Enhancing compliance and consistency: EDPB adopts DPIA template

**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

lead to it exercising significant practical influence, positioning it as a *de facto* standard for DPAs.

In order to preserve the flexibility inherent in the **risk-based approach of Article 35 GDPR**, **it should be further emphasized that the template** (and associated "explainer"):

**A) Expressly qualifies as non-binding**, pursuant to Article 70(1)(e) GDPR, and that failure in its adoption does not constitute non-conformity; and

**B) Serves as a reference framework and is not intended to limit the use of alternative DPIA methodologies/templates**. Data controllers should remain free to choose any format or methodology they deem appropriate when conducting a DPIA, in such a way that adequately addresses the specific nature, context and risks of a given processing operation, provided that the substantive requirements of Article 35 GDPR are met.

We also note that the template has elements of a tick-the-box approach. While systematically addressing GDPR requirements provides structure, risk assessment and compliance processes are not always linear in practice. **The DPIA template, while promoting a baseline level of harmonised interpretation among Member States, should be modular, scalable, and adaptable to a wide range of different contexts**. This would help ensure that the template supports accountability and consistency while remaining sufficiently adaptable to diverse processing scenarios and organizational contexts.

**It would also be beneficial if the DPIA template could clarify the minimum DPIA requirements while allowing organisations to maintain flexibility to provide additional elements when developing internal templates, in line with their specific governance and risk management context**. In this respect, we note that the explainer states that "*the EDPB template is one way to record the most important results, a minimum amount of information that should always be documented*". Should this be understood to mean that the EDPB template sets out the minimum information to be included in a DPIA?

We also highlight that banks have developed DPIA practices, and the EDPB DPIA template should not result in the reinvention of processes that are already well established. Rather than requiring all fields of the template to be completed for every DPIA, organisations should also be allowed to cross-reference existing internal documentation and IT tools (e.g., RoPAs, Risk assessments, TIAs, security documentation, FRIAs when applicable due to the AI Act), provided that traceability is ensured.

Relatedly, we also wish to recall that there is no obligation for data controllers to perform a DPIA as a single, consolidated document. A DPIA may consist of multiple elements or materials that are documented and maintained separately (e.g., certain aspects on security or on the exercise of rights can be documented outside the DPIA), as long as they collectively demonstrate accountability regarding the measurement of risks associated with a high-risk processing activity.

- **Strengthen focus on DPIA methodology and usability in line with the operational realities of (medium-to-large) organisations**

There is strong value added in harmonizing DPIA expectations across Member States. However, this value would be better realized by placing **greater emphasis on methodology** (how to assess necessity, proportionality and risk), rather than prescribing exhaustive documentation structures. Criteria could also be proposed to determine when there is a high risk to the rights and freedoms of data subjects (e.g., providing guidance on what is considered "*large volumes of data*", which may vary according to the different volume of business of each company).

Currently, the template assumes a level of detail and repetition that is not scalable for organizations with mature governance frameworks. It insufficiently accommodates reuse of existing documentation (e.g., security standards, certifications, and retention schedules), thereby risking a shift from a risk-based assessment to form-driven compliance.

**We therefore recommend further improving the usability of the template, (particularly for more complex processing activities), by 1) increasing its "customability" to reflect industry-specific and organizations' needs, 2) facilitating clearer cross-referencing between sections, and 3) enabling users to build more easily on previously provided information**.

For example, allowing multiple legal bases (Section 2.1) to be directly linked to the corresponding purposes of processing (Sections 1.1(b) and 1.1(c)) would significantly improve clarity and consistency. Similarly, in the section on technical and organisational measures, it would be useful to allow controllers to distinguish explicitly between different categories of personal data (Section 1.1.a), especially where special categories of data are concerned. This would better reflect the risk-based approach underpinning the DPIA and reduce the risk of overly generic descriptions.

- **Avoid misalignment with GDPR requirements & duplication**

In its current form, **the DPIA template requests information that goes beyond what is required under Article 35 GDPR, potentially leading to an increase in complexity**. In addition, multiple sections ask for similar or overlapping information (e.g., scope, context, processing description, risks, and measures), increasing duplication and the risk of inconsistencies rather than improving risk insight. Excessive complexity may also negatively affect the quality and usability of the output, increase the effort and resources required for execution, and reduce acceptance and understanding among data subjects.

**A simpler and more streamlined template, with greater emphasis on methodology, would therefore be preferable**. In particular, **the assessment should be performed at an appropriate level of granularity** so as to ensure that it remains a meaningful risk management instrument, while **any requirement exceeding those set out in Article 35 GDPR should remain strictly optional**.

- **Provide greater clarity on scope and level of granularity**

Core concepts, such as the *name of the processing, scope of the DPIA, purpose* and *context* lack clear guidance on the level of granularity. This is particularly problematic for complex processing with multiple subprocesses and differing legal bases and does not align well

with how DPIAs and RoPAs are managed in practice. In this regard, **we would appreciate if the EDPB could provide a complete sample DPIA template; this would help clarify what should be included in each field and the expected level of granularity**.

- **Better operational guidance and practical examples**

We would welcome if the DPIA template could **include examples of mitigation and minimisation measures, security control, or risk-reduction strategies.** This would help streamline the work of organisations and DPOs.

It would also be helpful to provide non-exhaustive lists of typical categories of personal data (Section 1.1.a) and technical organizational measures (Section 2.3). These lists should remain optional, allowing organisations the flexibility to add their own categories or introduce new ones as appropriate to specific cases.

We would also like to reflect on the role of the explainer/guidelines. In our view, the DPIA template itself should remain separate from the instructions and guidance on how to complete it. The template should focus on listing the information necessary to perform an adequate DPIA, while methodological explanations and completion guidance should be provided separately. In this regard, the explainer could serve as a consolidated reference document, where the EDPB incorporates the substance of EDPB Guidelines published over time, and where appropriate, provides clarification on completion instructions, recommended methodologies, etc.

- **Need for consistent, practical risk language across EDPB Guidance**

Harmonising terminology on "*risk to the rights and freedoms of individuals*" is necessary. While the Explainer makes a brief start, it is too limited to be of practical use. A consistent language and taxonomy on risks to the rights and freedoms of individuals that unifies the risk language in DPIAs and personal data breaches into multiple clear levels of risk (e.g., low, medium, high) would be especially valuable.

- **Avoid duplication between DPIA and other GDPR compliance processes**

**We encourage avoiding duplication between the DPIA and other GDPR compliance processes**. The **DPIA should be able to rely on existing internal documentation** in order to cover specific operational and security specificities while supplementing this information with data protection-specific details.

These considerations apply, for example, to the Record of Processing Activities (RoPAs). While DPIAs and RoPAS are closely interconnected and should remain consistent with one another (e.g., updating the DPIA when a corresponding information in the RoPA is amended), the DPIA should not require organisations to reproduce extensive information that is already documented and maintained within the RoPA as currently required in Section 2 and points 1.1.a and 1.1.b of the DPIA template. Instead, cross-references to existing documentation should be permitted where appropriate, provided that this information can be linked and reused by the DPIA and if sufficient in relation to the identified risk.

More broadly, the DPIA should remain an assessment tool rather than evolve into a comprehensive repository of all processing documentation. Information already maintained in e.g., records of processing activities, retention schedules, security

documentation or governance systems should be capable of being referenced where appropriate, provided that traceability is ensured.

## Section 0: Overview of the processing

As a preliminary remark, we highlight that the assessment of whether a processing activity requires a mandatory DPIA is performed directly within the DPIA template itself. No prior, separate risk assessment, including cases requiring a mandatory DPIA ("inherent risk assessment") is required before conducting the DPIA.

0*.1 - Controller(s)*

We would like to receive clarification from the EDPB on whether the entry "*Management units responsible for the processing inside the organisation*" needs to be tied to the management structure or to the business unit responsible for data processing.

To facilitate and further develop the analysis of processing activities, we also recommend introducing a separate entry for data processing activities involving joint controllers *(0.1.a – Joint controller*). If this entry is not applicable, it should be sufficient to select "No". As noted on pages 2-3, organisations should be allowed to cross-reference existing internal documentation and IT tools; accordingly, details relating to joint controllership arrangements should, where appropriate, be provided by reference to supporting documentation.

*0.2 - Processor(s) and sub-processor(s)*

While a list of sub-processors certainly has added value in the DPIA, we would appreciate clarification on the level of detail of information to be provided per sub-processor.

*Interplay between Section 0.3 - Name of the processing & Section 0.5 - DPIA technical sheet*

It is unclear why the entry **"current version"** has been listed twice, both under Section 0.3 (Name of the processing) and Section 0.5 (DPIA technical sheet). Maintaining this entry under Section 0.3 also appears illogical and we therefore **recommend only having this entry under Section 0.5**.

*0.5 - DPIA technical sheet*

| *Current version and version log (explaining the history of changes made to the information contained in the DPIA template for this processing, if any)* |
|---|

A free-text summary of historical changes is difficult to maintain and the value of maintaining such format of a RoPA entry in the DPIA template is unclear. **A version history of the full template – recording changes overtime - would therefore be preferable**. In addition, where DPIAs are managed through governance or workflow tools, information such as version history, completion dates, approval dates and participants may already be maintained automatically in system metadata. The EDPB should clarify that such information does not necessarily need to be reproduced within the DPIA itself, provided that it remains auditable and can be produced upon request.

*Team involved in conducting this DPIA (providing details of their roles, tasks, responsibilities, etc.)*

Defining roles and responsibilities should not be defined at template level, as this could lead to extra effort each time DPIA is completed and in practice, these roles are defined internally; instead, it should be possible to have this section prefilled at the level of the data controller.

*Guidelines, standards, codes of conduct and other reference materials used to conduct this DPIA*

This entry appears to refer primarily to external guidance (e.g., EDPB Guidelines). This should be described at process level rather than at template level.

*Reasons to conduct the DPIA*
*(…)*
*4. New processing activity, DPIA necessary or beneficial:*
*(…)*
□ *Required by a code of conduct, standard, best practice, etc.*

**We recommend keeping the list of reasons to conduct the DPIA simpler and targeted to instances where a DPIA is required for 1) new processing activities that can pose a high risk to data subjects; and 2) existing high-risk processing activities for which there has been a change of risk**. All other entries should be removed. This would ensure greater alignment with the risk-based approach, whereby processing activities should be assessed through a risk-based lens to determine whether a DPIA is necessary and what safeguards are appropriate.

We also note that the reference to codes of conduct, while clear to data protection professionals, may cause confusion for business stakeholders with internal codes of conduct, which are ethics/principle-based documents**. We therefore recommend deleting this entry, unless further clarified. Similarly, we recommend deleting the related Section 1.4 - Compliance with approved codes of conduct**; the meaning of the first option "*Compliance is likely to be required (legal obligation). Why?*" is not clear. The second option "*Compliance is necessary or beneficial. Why?*" is unnecessary given that the concept of "necessity" is already captured in the first option.

*Scope of this DPIA (what has been considered and what has been left out of the assessment and why)*

We recommend removing the wording "*and what has been left out of the assessment and why*", as its added value is unclear and may create confusion regarding the scope of the assessment.

*Formal validation date (approval of the DPIA as complete and finished by a responsible official)*

The specification to have a "responsible official" for a DPIA should not be construed as an obligation, but rather remain non-binding and subject to each controller's internal governance structures and procedures (which, in the case of banks, have been in place for several years).

| | |
|---|---|
| *Is the DPIA (or parts of it) intended to be published or to be shared externally?* | ☐ *No*<br>☐ *Yes it is going to be published: How?*<br>☐ *Yes, it is going to be shared externally: How?* |

With regards to the possible publication/sharing of the DPIA, the explainer states that "*While it may be a good practice from a transparency point of view, sensitive information should not be published (concerning security, for example).*" **It should be better clarified that the publication/sharing of DPIA is not mandatory**. There is a risk that the publication of information related to security measures could compromise the security of systems or compromise/give away trade secrets or commercially sensitive information (e.g. bank secrecy, anti-fraud framework).

## Section 1: Systematic description of the processing

*1.1.a - Processed personal data*

We would like to share the following observations relating to Section 1.1.a:

- The headline "processed personal data (item or element)" and the accompanying explainer suggest a requirement to list personal data at the level of individual data element/item. Considering that a data element or data item is the smallest unit of data, listing of all data items involved in a processing activity would amount to hundreds, if not thousands, of entries. If this requirement reflects the EDPB's expectation, such requirement would be highly disproportionate in practice. **We would therefore welcome clarification from the EDPB on this point to ensure that expectations remain proportionate and documentation requirements are not unduly burdensome**.
- We also note that, while Section 0.5, entry 3 refers to both GDPR Article 9 and Article 10 personal data, Section 1.1.a only refers to special categories of personal data (Article 9 GDPR), without mentioning personal data relating to criminal convictions and offences (Article 10 GDPR). Such omission/inconsistency could generate uncertainties in sectors (e.g., FTA, anti-fraud) in which processing of personal data pursuant to Article 10 GDPR is recurrent and relevant (e.g. for the purposes of risk assessment). **We therefore recommend including an explicit reference to Article 10 GDPR** as reported in the table below.

| | Processed personal data (item or element) | Explanation (data type, data subject category, additional details) | Special category of personal data or personal data relating to criminal convictions and offences |
|---|---|---|---|
| 1 | | | □ No<br>Yes:<br>□ Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.<br>□ Genetic data.<br>□ Biometric data for the purpose of uniquely identifying a natural person.<br>□ Data concerning health.<br>□ Data concerning a natural person's sex life or sexual orientation.<br>* Data relating to criminal convictions and offences. |

*1.1.b - Purposes of the processing*

We are concerned that, if the assessment of purpose of the processing is expected at data-element level, the workload will be vast and likely disproportionate. We therefore suggest clarifying this point with a view to simplifying it.

*1.1.c - Secondary and compatible uses*

The requirement under this section suggests that an *ex-ante* compatibility assessment is required to determine conditions for hypothetical future secondary processing. We are of the view that such requirement would not be practical and should be deleted.

*1.1.d - Nature, scope and context of the processing*

| | |
|---|---|
| Context of the processing: circumstances and environment (use cases, supported business processes, status of the controller and relationship with the data subjects, data subjects categories and potential vulnerable groups, cross-border processing, international transfers, etc.). | Is this a cross-border processing?<br>□ No<br>□ Yes (justification and details):<br><br>Is personal data going to be transferred to a recipient in a third country or international organisation?<br>□ No<br>□ Yes (justification and details): |

We would welcome clarification of the "status of the controller", e.g., whether or not it refers to private / public entity.

*1.2 - Functional description*

| | Processing phase or stage | Type of operations | Explanation |
|---|---|---|---|
| 1 | | □ Collection<br>□ Use<br>□ Storage<br>□ Sharing and Transfer<br>□ Deletion and Destruction<br>□ Other | |

Under the entry "Type of operations", we suggest adding a new point "other" (e.g. adapting, combining) to those already listed above.

*1.3 - Means of processing, supporting assets and underlying architecture*

Despite the additional guidance provided in the explainer, it remains unclear what should be referenced and in what manner. We would appreciate it if the EDPB could provide an illustrative example to better guide controllers in how to carry out the assessment.

*1.4 - Compliance with approved codes of conduct*

It is unclear what is expected to be reported under this section in light of the explainer. Clarification is therefore welcome.

**Section 2: Analysis of the processing**

*2.1.a Legal basis*

The template appears to presume the identification of a single legal basis for each purpose. In practice, however, several legal bases for the same processing may coexist, depending on the different phases or components of the same. A restrictive approach could lead to simplified representations that do not fully adhere to the reality of complex treatments. It should **therefore be made clear that, for the purposes of filling in the template, it is possible to indicate several legal bases** in a structured and transparent way.

We also highlight that the justification for the identified legal basis should primarily be documented in the Lawful Basis Assessment rather than in the DPIA. Cross-referencing should therefore be allowed.

*2.1.b - Reasons to lift the processing prohibition*

It should be noted that the Digital Omnibus proposal envisages introducing additional exceptions to the prohibition on processing special categories of personal data. In this context, the list included in the template may require updating in the near future.

*2.2.a – Data minimization and retention period*

Similar to our comment under Section 1.1.a, if the justification of processing, sharing and retention periods is to be documented and provided at the level of individual data elements, this section is likely to become excessively detailed and could extend to hundreds of lines. It is also unclear whether this approach is intended to represent a standard for demonstrating compliance with the data minimization principle and whether the expectation is that effective minimization must be assessed and evidenced at the level of each individual data item or element. In view of these considerations, **we recommend**

**ensuring that the level of granularity required is proportionate**, taking into account realistic workload estimates relative to the actual value from a privacy risk perspective. **We also recommend clarifying that controllers may rely on existing records retention schedules and records management frameworks where these are already maintained and governed centrally**. Controllers should not be required to reproduce detailed retention information within each DPIA where appropriate cross-references can be provided.

We also recommend strengthening the link between Section 1.1.b (purposes of processing) and Section 2.2 (data minimisation and retention period). In accordance with the principle of storage limitation (Article 5(1)(e) GDPR), the retention period must be strictly determined based on each identified purpose (not the data). **We therefore suggest that, in Section 2.2.a, each retention period be explicitly justified in relation to the corresponding purpose, with a clear reference to Section 1.1.b**.

*2.2.b - Data quality*

We raise concerns at the requirement to provide a detailed description of the data quality parameters (i.e., quality metrics, thresholds, requirements), which appear to be excessive. **We therefore recommend deleting this section. If not feasible, consideration should be given to simplifying this requirement and supplementing this section with practical examples** or a non-exhaustive list of the information expected, to ensure a consistent and proportionate application and manage workload.

More specific to the requirement to describe "quality metrics, requirements or thresholds", the explainer does not provide clear enough instructions as to what is expected in practice and this should be clarified.

*2.3.a - Measures supporting compliance with principles in Article 5(1)(a-f) GDPR*

We would like to share the following observations on Section 2.3.a:

- While the general intentions of this section are understood, responses risk becoming overly generic. We therefore suggest including practical examples for each principle to support more meaningful and consistent responses.
- **There also appears to be several overlaps between these principles and other sections of the template**. Overlaps may be observed between Section 2.3.a and Section 2.3.b, in particular regarding the transparency principle and the information to be provided to data subjects, which may lead to reporting duplication of the same risks. Other overlaps arise between Section 4.1 (Risk assessment and management) and Section 4.2 (Action plan)[3]. Streamlining of these sections would improve overall coherence and template usability.
- Regarding the implementation status of each safeguard, clarification would be welcome as to whether 1) for planned or partially implemented measures, a timeline for completion should be attached to the status; and 2) any item that is not fully implemented requires the registration of a residual risk.

[3] See, for example, Section 4.1.c (Modulating factors), 4.2.a (Discussion of appropriateness and effectiveness [of mitigated risks]), and 4.2.b (Additional mitigating measures that apply)).

*2.3.c - Measures supporting compliance with other GDPR requirements*

Further clarification would be welcome regarding what is expected under entry "Relationship with processors (Article 28 GDPR)". In particular, it is unclear whether this refers to ensuring that the organisation has in place the necessary data processing agreements or contractual arrangements with all processors, and that a supplier assessment has been performed prior to initiating the processing activity, or whether additional/different elements are envisaged.

Similarly, with regards to the entry "Safeguards relating to international transfer(s) (Chapter V GDPR)", it would be helpful to understand whether the expectation is limited to the appropriate safeguards listed under Article 46 GDPR, or whether further information is required. More generally, where organisations rely on established information security frameworks, internal control libraries, certifications or security governance programs, the DPIA should be permitted to reference those frameworks rather than requiring a detailed restatement of baseline security measures within each individual DPIA.

**Section 3: Considerations on necessity and proportionality**

*3.1 - Impacts of processing on the rights and freedoms of data subjects*

We would welcome clarification from the EDPB regarding the structuring of the risk assessment, particularly with regards to the distinction between "inherent/design risks" (Section 3.1) and "incident or abnormal event risks" (Section 4.1.a). Is the explicit separation intended to be a mandatory conceptual distinction, or may these risks be documented within a single integrated risk model, provided that clarity is maintained? With a view to improving coherence and avoiding unnecessary fragmentation, while still ensuring that risks are properly identified and assessed, **we recommend merging Sections 3.1 and Section 4.1.a**.

More generally, we note that Section 3.1 of the template appears to fall more naturally within the risk assessment addressed in Section 4. Aligning this question with the risk assessment section could improve the logical structure and clarity of the template.

*3.2 - Assess the necessity of the processing*

We recommend clarifying whether the assessment of necessity should be conducted across all legal bases (e.g. performance of a contract, legal obligation, legitimate interest, consent); as currently drafted, and in light of the reference in Footnote 5, the requirement appears to focus solely on the legitimate interest ground. If the intention is indeed to include all legal bases, we note that, for processing necessary to comply with a legal obligation, necessity (and the assessment thereof) is effectively determined "upstream" by the legislator. Requiring controllers to re-assess that necessity and to interrupt processing because of an alleged "incomplete need" for processing has emerged, could create legal inconsistencies and a violation of the law.

In addition, we raised concerns about the **requirement to provide evidence that measures taken have already achieved their intended effects** (see, for example, Sections 3.2 and 3.3), as this appears far-reaching and difficult to reconcile with the *ex-ante* nature of the assessment (i.e., obligation to conduct the impact assessment before processing begins). We therefore **recommend removing this requirement**.

*3.3 - Assess the proportionality of the processing*

Similar to the reflections made under the previous section, we note that the description of the proportionality assessment appears to reflect elements typical of a Legitimate Interest Assessment (LIA), suggesting a focus on the legal basis of legitimate interest rather than a broader application across all legal bases. We therefore recommend clarifying this point to avoid confusion.

**Section 4: Risk assessment and management**

*4.1 - Risk assessment and management*

*Interplay between Section 4.1.c – Inherent risk assessment & Section 4.2.b – Residual risk assessment*

The template makes a clear distinction between the assessment of "inherent" risk (Section 4.1.c) and "residual" risk (Section 4.2.b). We note, however, that in practice, processing activities are defined and implemented following the principle of privacy by design and not without any controls from the beginning. In this context, the distinction between inherent and residual risks appears artificial. We would therefore welcome clarification as to whether this explicit separation constitutes a mandatory conceptual distinction, or whether controllers may document these risks within a single integrated risk model, provided that clarity is preserved.

In view of the upcoming FRIA to be carried out under the AI Act, we also recommend streamlining any overlap between the DPIA and FRIA assessments, as some elements assessed in this section, most notably the inherent and residual risk assessment, may be addressed in greater detail in FRIA, where applicable. We also ask EDPB to consider if there is a need to provide guidance on how to conduct DPIA in AI cases.

More broadly, as the DPIA and FRIA will co-exist, their coordination/alignment in terms of content and methodology is necessary. In light of the upcoming EDPB-AI Office guidance on the FRIA, we therefore recommend:

- Clarifying that the GDPR is the primary framework governing the processing of personal data in the context of AI systems;
- Ensuring, to the greatest extent possible, a substantive and structural integration of the DPIA and FRIA, aligning methodologies while preserving their distinct legal bases and objectives;
- Clarifying that, ultimately, controllers/AI deployers should have the freedom to choose which methodology to adopt when performing a FRIA and DPIA assessment for AI systems processing personal data based on their internal structure and processes already in place.

**Section 5: Involvement of interested parties**

*5.1 – DPO Advice*

The current template does not sufficiently distinguish between the DPO advice and the controller's final decision, which could in practice be perceived to undermine the DPO's independence. In addition, the template appears to focus only on describing "*how*" the DPO advice is implemented, without providing room for substantiated deviations from that advice. **We therefore recommend including explicit guidance clarifying that the**

**DPO advice, conclusions, and recommendations should be documented in full, irrespective of whether the controller ultimately follows them. Where the controller decides to deviate from the DPO's recommendations, the specific reasons for doing so should also be documented**. We also recommend clarifying that evidence of DPO involvement may be demonstrated through governance workflows, approval records or audit trails, rather than requiring extensive narrative documentation within the DPIA itself.

We also note that the requirement to "*Explain how the DPO's advice has been implemented*" appears to assume that the DPO's opinion is provided through a separate process and at an earlier stage. We recommend clarifying that controllers are allowed to determine their own operating procedures for obtaining and documenting the opinion of the DPO.

*5.2 – Views if data subjects or their representatives*

As it stands, it is unclear in which concrete scenarios controllers are expected to actively seek data subject's or their representatives' views as part of a DPIA. More broadly, we also highlight that this requirement appears difficult to implement in practice, particularly for organisations with a very large customer base, such as banks. In this regard, **we recommend the following clarification:**

- Clarify what is meant by "*where appropriate*" under Article 35(9) GDPR, including under which circumstances controllers are expected to involve data subjects or their representatives in the DPIA process, and the modalities for doing so. In its current form, the requirement is overly complex and insufficiently aligned with the operational realities of (medium-to-large) organisations. For the banking sector, such clarification should also take into account the risks associated with disclosing sensitive processes and information (e.g., in the context of AML, fraud, DLP). More generally, it should be clarified that, in line with Article 35(9), **not every DPIA must involve the consultation of data subjects or their representatives**;
- **Expand Section 5.2 on data subjects' participation in the DPIA process by providing more operational guidance. This could include practical examples and recognised best practices** on how data subjects or their representatives can be involved in the DPIA process, depending on the nature and risks of the processing and considering confidentiality, banking secrecy or any type of trade secret rules.

**Section 6: Conclusion and decision**

As already mentioned under Section 0.5 (DPIA technical sheet), the specification to have a "responsible official" validating a DPIA should remain flexible and not construed as an obligation.

**ENDS**

**For more information:**
Rachele Ceraulo
Policy Adviser – Data & Innovation
r.ceraulo@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 significantmajority 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**

**www.ebf.eu**