EBF response to the EDPB's consultation on Compliance Templates

We welcome the initiative of the EDPB to develop practical models to facilitate organisations' compliance with the GDPR, in line with the Helsinki Statement on enhanced clarity, support and engagement. We share the objective of providing concrete support and guidance tools that simplify and harmonise the fulfilment of data protection obligations.

We recommend that the template-drafting process be guided by the following principles:

- **Voluntariness and non-prescriptiveness**: these templates should expressly qualify as non-binding, pursuant to Article 70(1)(e) GDPR, and that failure in their adoption does not constitute non-conformity. This approach is consistent with Article 24 GDPR, which grants controller the methodological flexibility to select measures appropriate to the specific risk of processing.
- **Flexibility and adaptability**: the EDPB should promote models that are modular, scalable, and adaptable to a wide range of different contexts, while also promoting a baseline level of harmonised interpretation among Member States.
- **Accountability** and the **risk-based approach**.

We encourage the EDPB to develop practical templates/checklists in the following priority areas:

- **Legitimate Interest Assessment**: a non-mandatory LIA template could help organisations outline, in a single document, the criteria and guidelines set out by the GDPR and the EDPB regarding the assessment of legitimate interest. Practically, it should be designed as an operational sheet covering the 3-step process outlined by the EDPB: pursuit of a legitimate interest, analysis of necessity and methodology for the balance of rights.
- **DPIAs**: we welcome the EDPB's commitment to producing a DPIA template. This should have a modular structure and include practical examples of processing-related risks and technical/organisational mitigation measures. To the extent possible, the DPIA template should be linked to the FRIA under the AI Act (i.e., which specific AI-related questions a DPIA should include).
- **Data Breaches**: we recommend developing the following templates for reporting personal data breaches in compliance with Articles 33 and 34 GDPR: breach notification to supervisory authorities; breach notification to data subjects; internal breach reporting; internal breach register; risk assessment for data breaches. We also recommend developing a common methodology for assessing the risk of security incidents.
- **Joint controllership arrangements**: we recommend developing a template/checklist for joint controllerships agreements given the complexity and interpretative challenges surrounding such arrangements. The template should provide a clear structure for allocating responsibilities in line with Article 26 GDPR, include practical examples of clauses (i.e., liability allocation), and offer guidance on how to adapt the agreement to different operational contexts (e.g., intra-group vs partnerships with third parties).
- **Transfer Impact Assessment and country assessment**: clear operational guidance on how to assess international data transfers remains scarce. A template for third-country data transfer assessments would help reduce uncertainty around how controllers are able to demonstrate compliance with Chapter V of the GDPR and promote greater consistency in the field of data protection enforcement.
- **Records of Processing Activities**: the template should clearly reflect the purpose and practical use of such records and help organisations understand how these records serve as a compliance and accountability tool under the GDPR, rather than as a purely administrative obligation. It should also be clear at what level of granularity a record should be created, so that organisations can ensure that records are created at an appropriate and consistent level of detail. The template should also come with a list of practical examples.
- **Privacy Notices**: divergent interpretations among DPAs have emerged regarding privacy notices. A template would therefore support consistent interpretation and improve readability and comparability for recipients (e.g., customers, employees). We recommend that the template A) is tailored to the target recipient, and B) includes examples of plain-language formulations, effective icons and layering of privacy notices to enhance clarity and accessibility.

We also recommend that each template integrates a risk assessment dimension (e.g., a risk matrix in DPIA templates, a risk tier indicator in the ROPA, a severity score card for data breaches, etc.). This would enable better compatibility with governance, risk management, and compliance systems already in place within the financial sector, and ensure coherence with the requirements of regulators (EBA, ECB, etc.). We also recommend that the EDPB engages in consultation with financial regulators/competent authorities to ensure that the proposed voluntary templates are aligned with the existing regulatory framework.

Finally, while not strictly necessary, we provide the following list of templates for potential future consideration:

- Consent templates
- Data subject rights: Data subject rights request responses, data subject access request, data subject complaint responses
- Accountability Framework Template
- Data sharing agreement (controller to controller sharing)
- Data processing agreement (controller to processor contractual agreements)
- Checklist for engaging and monitoring data processor, including a Processor Due Diligence Template
- Third party supplier assessment (e.g., for SaaS/cloud solutions)
- Risk assessment template for record keeping
- Risk assessment template under Art. 32 GDPR
- Risk assessment in the instances where the risk for the data subject doesn't trigger a DPIA
- Staff data protection training
- Cookie banner and policy