26th May, 2026 r.

Position Paper of the Polish Bank Association to the European Data Protection Board regarding the template for Data Protection Impact Assessment (DPIA)

The Polish Bank Association welcomes the European Data Protection Board's efforts aimed at harmonising the approach to conducting Data Protection Impact Assessments across the European Union. A common DPIA template may contribute to greater regulatory predictability, reduction of discrepancies between the practices of national supervisory authorities, and improvement of the quality of documenting risk assessment processes concerning the rights and freedoms of data subjects.

At the same time, the banking sector identifies a number of significant practical, methodological and drafting-related concerns in the proposed template. In its current form, the project may lead to excessive formalisation of DPIAs and transform this instrument from a tool for assessing data protection impacts into a very broad GDPR compliance document, also encompassing elements of governance, system architecture, information security management, enterprise risk management and operational documentation.

From the perspective of the banking sector, preserving the functional nature of the DPIA is of particular importance. A Data Protection Impact Assessment should serve to identify and mitigate risks to the rights and freedoms of data subjects, rather than replace the record of processing activities, security documentation, ICT documentation, outsourcing documentation, operational risk management documentation or the organisation's overall GDPR compliance documentation.

Below, the Polish Bank Association presents its detailed comments regarding the template and the Explainer document.

1. The need to clearly embed the template in the principle of proportionality

The template should explicitly state that the scope, level of detail and depth of a DPIA should remain proportionate to the nature, scope, context and actual level of risk associated with the processing of personal data.

In practice, the current structure of the document suggests a uniform, maximally extensive DPIA model for all categories of high-risk processing operations, regardless of the scale of

processing, the organisational maturity of the controller, the type of technology used, the nature of the legal obligations related to the processing operation, or the actual impact on data subjects.

As a consequence, even standard sectoral processing operations requiring a DPIA may require the preparation of highly extensive quasi-audit documentation. Such an outcome is difficult to reconcile with the principle of proportionality under the GDPR and with the practical role of a DPIA as a risk management tool.

In the opinion of the Polish Bank Association, the template should expressly allow the use of simplified DPIA models, enable differentiation in the level of detail of the analysis, and limit documentation obligations to elements genuinely necessary for assessing risks to the rights and freedoms of data subjects.

2. Excessive extension of the DPIA function beyond the assessment of risks to the rights and freedoms of data subjects

The proposed template covers a very broad range of compliance elements, including detailed analyses of legal bases for processing, extensive lifecycle management descriptions, information regarding architecture and asset inventory, implementation status of security measures, process governance, documentation of DPO activities, versioning and change history. Such scope results both from the structure of the template itself and from the Explainer document, which indicates that the template is intended to document the minimum amount of information expected in a format acceptable to supervisory authorities.

In the banking sector's view, some of these elements go beyond the DPIA function envisaged in Article 35 GDPR and lead to duplication of documentation already existing within organisations as part of other compliance, cybersecurity and operational risk management processes.

There is a risk that, in practice, the DPIA will become a comprehensive GDPR compliance repository rather than a tool primarily intended to identify, analyse and mitigate risks to the rights and freedoms of data subjects.

In the opinion of the Polish Bank Association, it is necessary to establish a clearer distinction between elements genuinely necessary for the impact assessment itself and elements constituting additional organisational or compliance documentation.

3. The need for a clear distinction between mandatory and optional elements

The template currently does not distinguish between mandatory information, optional information and recommended good practices. In practice, this may lead both controllers and supervisory authorities to treat all template fields as mandatory.

In the opinion of the Polish Bank Association, the document should clearly specify which elements constitute the minimum required by Article 35 GDPR and which elements are supplementary or merely recommended.

The lack of such distinction may lead to excessive formalism and disproportionate documentation burdens, particularly in large organisations conducting multiple DPIAs simultaneously.

4. Lack of clarity regarding the relationship between sections 3.1 and 4.1.a concerning risks

The template introduces a distinction between risks resulting from the very nature and design of the processing operation and risks resulting from incidents, errors, breaches or operational irregularities. Section 3.1 concerns risks that exist even when the processing operates as intended, whereas section 4.1.a concerns non-default, accidental, unlawful or abnormal events.

While such distinction is theoretically justified, the current wording of the document does not provide sufficiently clear criteria for the practical application of this distinction.

In practice, this may lead to duplication of risk analyses, methodological difficulties in classifying threats and significant interpretative inconsistencies between organisations.

In the opinion of the Polish Bank Association, the addition of practical examples, risk scenarios and more precise explanations regarding the expected level of detail in both sections would be advisable.

5. Lack of clear methodological guidance regarding risk assessment

The template requires the identification of, inter alia, inherent risk, residual risk, modulating factors, risk acceptance levels and likelihood and severity metrics. At the same time, it does not specify minimum methodological standards or relationships with existing risk management frameworks. Although the Explainer states that controllers may use the DPIA methodology of their choice, the template still expects certain categories of risk assessment which may not directly correspond to models used in large regulated organisations.

In practice, this may lead to significant interpretative discrepancies between controllers and supervisory authorities, as well as to the necessity of building parallel risk assessment models exclusively for DPIA purposes.

In the banking sector's view, the template should explicitly allow the use of existing enterprise risk management methodologies, ISO 27005 standards, NIST standards and sector-specific operational and cybersecurity risk management models.

Without such clarification, the template may lead to unnecessary compliance costs and hinder coherent risk management in organisations subject to multiple parallel regulatory obligations.

6. Excessively extensive requirements regarding architecture and asset inventory

Section 1.3 requires a very broad description of infrastructure, technical resources, architecture, system components, models, APIs, technical environments and personnel. The Explainer specifies that an asset may include hardware, infrastructure, networks, software, APIs, models, personnel, locations, procedures and contracts with processors and sub-processors.

In the banking sector's opinion, this scope is excessive from the perspective of the purpose of a DPIA and may lead to duplication of ICT, cybersecurity and operational resilience documentation already maintained within organisations.

Moreover, excessively detailed documentation of system architecture within the DPIA itself may create security risks and difficulties in maintaining the documentation up to date.

The Polish Bank Association postulates limiting the required level of detail to elements genuinely necessary for assessing risks to the rights and freedoms of data subjects and explicitly allowing references to existing technical documentation instead of duplicating it within the DPIA.

7. The need to take into account the specific nature of regulated sectors, including the banking sector

The banking sector operates within a highly regulated environment in which regulatory obligations frequently determine the purposes, scope and methods of personal data processing. This applies in particular to obligations relating to anti-money laundering and counter-terrorist financing, credit risk management, fraud prevention, cybersecurity, outsourcing, operational resilience and reporting obligations towards public authorities.

In many cases, data processing carried out by banks is not a freely chosen business activity of the controller, but results directly or indirectly from statutory obligations, prudential requirements, supervisory expectations or the necessity to ensure the security of clients' assets and the stability of the financial system.

The template should take this specificity into account. In particular, the necessity and proportionality assessment should be adapted to processing operations resulting from legal or regulatory obligations. Controllers should not be required to repeatedly justify the necessity of a processing operation whose performance is mandated by sectoral legislation or supervisory standards.

8. The need to clarify the necessity and proportionality assessment

The proposed template requires an assessment of whether the envisaged processing is effective and constitutes the least intrusive solution for the rights and freedoms of data subjects, as well as an assessment of proportionality through balancing the impact on rights and freedoms against the benefits resulting from the processing.

In the opinion of the Polish Bank Association, this approach is understandable in relation to processing operations that significantly interfere with privacy. However, in its current wording, it may lead to an excessively abstract and difficult-to-apply assessment in the case of standard operational processes in the banking sector.

In particular, the template should clarify how the necessity and proportionality assessment should be applied to processing operations based on legal obligations, performance of contracts, transaction security, fraud prevention, cybersecurity measures and regulatory risk management.

The Polish Bank Association recommends that the template expressly indicate that the scope of the necessity and proportionality assessment may be limited where the processing operation results from a legal obligation or is necessary for the fulfilment of prudential obligations or the protection of the security of the financial system.

9. The need to allow references to existing documentation

The proposed template should expressly allow references to existing organisational, technical, legal and risk documentation instead of requiring duplication of such information within the DPIA.

In large financial institutions, essential information concerning processing operations is already documented in numerous tools and registers, including records of processing activities, application registers, outsourcing documentation, information security documentation, ICT risk analyses, architecture documentation, retention procedures and sectoral compliance documentation.

Requiring the full duplication of such information within the DPIA would lead to disproportionate organisational burdens and increase the risk of inconsistencies between documents.

The Polish Bank Association postulates that the template should explicitly state that references, links and annexes to existing documentation are permissible, provided that they allow verification of the key elements of the risk assessment.

10. The need to add a "not applicable" option

In many sections, the template requires selecting the implementation status of measures as "planned", "partially implemented" or "implemented". However, no "not applicable" option has been provided. This issue is particularly visible in sections concerning data subjects' rights,

consent, relationships with processors, international transfers and certain compliance-supporting measures. Comments from the banking sector explicitly indicate that the absence of such an option may lead to artificial completion of fields that are irrelevant to the given processing operation.

In the opinion of the Polish Bank Association, the absence of a “not applicable” option may lead to incorrect interpretation of the template and to forcing descriptions of measures that are not relevant in a given context.

The template should allow controllers to indicate that a given right, obligation, safeguard or mechanism does not apply to the specific processing operation, together with a brief justification.

11. The need to clarify the concept of “responsible official”

The Explainer indicates that the DPIA should be formally approved by a “responsible official”, for example a Managing Director or CEO.

In the opinion of the Polish Bank Association, this concept requires clarification. In large organisations, including banks, formal responsibility for approving DPIAs may be assigned to different functions, committees or organisational units depending on the nature of the process, the level of risk, the governance model and the internal allocation of competences.

The template should not suggest that every DPIA requires approval by the CEO or the highest management level. Such an expectation would be disproportionate and operationally difficult in institutions conducting numerous DPIAs.

The Polish Bank Association postulates that the template should clarify that “responsible official” means a person, function or internal body authorised under the controller’s governance model to approve the DPIA or decide on continuation of the processing operation.

12. Lack of clarity regarding the “current version” and “version log” fields

Comments from the sector indicate that the “current version” and “version log” fields are unclear. It is not evident whether they refer to the version of the processing operation itself, the version of the DPIA document, the version of the template, the version of the IT system, or the history of changes concerning risks and mitigating measures.

In the opinion of the Polish Bank Association, these fields should be separated and clarified. In particular, the template should distinguish between the version of the DPIA document, the date of the latest update, the reason for the change, the scope of the change and, where relevant, the version of the process or system.

The current wording may lead to inconsistent completion of the document and difficulties in its subsequent assessment.

13. The need to supplement data categories with data referred to in Article 10 GDPR

Section 1.1.a of the template provides for the identification of special categories of personal data but does not properly address data relating to criminal convictions and offences within the meaning of Article 10 GDPR. This issue was also raised by a representative of the banking sector.

In the opinion of the Polish Bank Association, this constitutes a significant gap. Data referred to in Article 10 GDPR are not special categories of data within the meaning of Article 9 GDPR, but are subject to a separate and enhanced protection regime. Therefore, they should be explicitly included in the template as a separate category of data requiring identification and justification.

This is particularly important in the banking sector, where certain processing operations may involve information relating to suspected fraud, sanctions, proceedings, anti-financial crime measures or other circumstances requiring enhanced caution.

14. The need to clarify the section concerning processors and sub-processors

Section 0.2 covers the identification of processors and sub-processors as well as the definition of their obligations and tasks. In the banking sector's opinion, this table should be supplemented with categories of entrusted personal data. This comment was also raised by a representative of a bank.

Information concerning categories of entrusted data is important for risk assessment purposes, as the scope of data entrusted to a processor or sub-processor directly affects the assessment of potential impacts on data subjects.

At the same time, the template should allow references to existing data processing agreements, vendor registers or outsourcing documentation without requiring duplication of the full content of such documents within the DPIA.

15. The need to separate questions concerning cross-border processing and international transfers

Section 1.1.d includes questions concerning cross-border processing and transfers of data to third countries or international organisations. From a practical perspective, these are two distinct issues which should be clearly separated. This comment was also raised by a representative of the banking sector.

Cross-border processing within the meaning of the GDPR concerns processing carried out within the EU and may be relevant for the one-stop-shop mechanism and the competence of supervisory authorities. International transfers concern transfers of personal data to a third country or international organisation and are subject to separate obligations under Chapter V GDPR.

Combining these issues within one structure may lead to imprecise responses and confusion between two different legal regimes.

16. The need to clarify sections concerning the data lifecycle

Sections 1.2 and 1.3 should more practically indicate what type of information the EDPB expects at each stage of the data lifecycle. Comments from the sector indicate that it would be helpful to explicitly refer to stages such as data collection, data use, data storage, data sharing or transfer, archiving, retention, deletion and anonymisation.

Although the Explainer already contains some discussion of these stages, the template itself could be more transparent and operational.

For large organisations, including banks, clearly mapping the data lifecycle is crucial for the effective preparation of DPIAs. The absence of a precise structure may lead to inconsistent process descriptions and omission of important stages of processing.

17. The need to clarify the section concerning codes of conduct

Section 1.4 concerning compliance with approved codes of conduct requires clarification. It is unclear whether it refers exclusively to approved codes of conduct within the meaning of Article 40 GDPR or also to other sectoral codes, organisational standards or good practices. This issue was also raised by a representative of the banking sector.

In the opinion of the Polish Bank Association, the template should clearly specify whether this section concerns only codes approved pursuant to Article 40 GDPR and monitored pursuant to Article 41 GDPR, or whether it also covers broader categories of sectoral standards.

If the intention is to refer exclusively to Article 40 GDPR codes, the template should use precise terminology and explicitly refer to that provision. If, however, the EDPB intends to include broader self-regulatory standards, this should also be clearly indicated in order to avoid confusion between approved codes of conduct and other sectoral documents.

18. Lack of clarity regarding the "discussion of appropriateness and effectiveness" column

Many sections of the template contain a column concerning the discussion of appropriateness and effectiveness of measures. From a practical perspective, it is unclear what level of detail

is expected and whether the requirement concerns justification of the final assessment, description of the internal discussion process, or assessment of the effectiveness of controls. This issue was also raised by a representative of the banking sector.

In the opinion of the Polish Bank Association, the DPIA should document the outcome of the assessment and the justification for the adopted measures, rather than the internal deliberation process itself. The term “discussion” may suggest the need to describe internal deliberations, which is not necessary for demonstrating compliance.

The Polish Bank Association therefore postulates replacing this wording with a more precise phrase such as “assessment and justification of appropriateness and effectiveness”.

19. The need to add examples of measures under Article 25 GDPR

Section 2.3.d concerning data protection by design and by default should be supplemented with examples of measures that may be considered within this part of the DPIA. This issue was also raised by a representative of the banking sector.

In practice, the concept of data protection by design and by default may be interpreted differently by organisations. It would therefore be helpful to include examples such as minimisation of default data scope, access restrictions, pseudonymisation, data segmentation, retention limitations, privacy-friendly default settings, access control mechanisms and safeguards limiting secondary use of data.

Adding such examples would improve comparability between DPIAs and reduce the risk of merely formal completion of this section.

20. The need to add examples of measures under Article 32 GDPR

Section 2.3.e concerning security of processing should be supplemented with examples of technical and organisational measures relating to Article 32 GDPR. This issue was also raised by a representative of the banking sector.

The Explainer provides general examples such as pseudonymisation, encryption, ensuring confidentiality, integrity, availability and resilience of systems, as well as the ability to restore availability of personal data following an incident.

In the opinion of the Polish Bank Association, these examples should be further developed either within the template itself or in an annex, so that controllers can document security measures in a coherent and comparable manner without being required to disclose excessively detailed technical information.

21. The need to supplement the template with examples of threats and risk scenarios

Sections 3.1 and 4.1.a may be difficult to complete in practice because they require distinguishing between threats resulting from the very design of the processing operation and threats resulting from deviations, incidents or errors. This issue was also raised by a representative of the banking sector.

The Polish Bank Association recommends adding examples of threats and risk scenarios. For example, a risk resulting from the very design of a process may consist in excessive interference with privacy through systematic monitoring of customer behaviour. By contrast, a risk resulting from an incident may involve unauthorised access, incorrect configuration of permissions, sending data to the wrong recipient or unauthorised modification of data.

Such examples would improve the practical usability of the template and reduce the risk of duplicating the same risks across different sections.

22. The need for a cautious approach to documenting the DPO's position

The template requires presentation of the DPO's opinion, findings and recommendations, as well as an explanation of how the controller implemented the DPO's recommendations.

In the opinion of the Polish Bank Association, this approach is generally consistent with the role of the Data Protection Officer but requires clarification. The DPO performs an advisory and monitoring function, whereas the decision regarding processing and risk acceptance remains the responsibility of the controller.

The template should avoid wording suggesting that DPO recommendations must always be implemented or that the DPO co-decides on risk acceptance. It should be sufficient to document that the DPO's opinion was obtained, considered and that the controller justified its approach to that opinion.

23. The need to clarify the involvement of data subjects or their representatives

The template requires indicating, where appropriate, the views of data subjects or their representatives, as well as explaining their involvement in the DPIA process or the reasons for the absence of such involvement.

In the opinion of the Polish Bank Association, this requirement should be clarified in a manner reflecting the realities of large organisations and sectoral processes. In many situations, obtaining the views of data subjects may be impossible, disproportionate, methodologically questionable or contrary to the purpose of the process itself, for example in fraud prevention, AML, cybersecurity or investigative processes.

The template should expressly indicate that consulting data subjects is not an automatic requirement for every DPIA and should be assessed taking into account the purpose of

processing, the risk of revealing control mechanisms, trade secrets, security considerations and proportionality.

24. The need to clarify rules regarding publication or external disclosure of DPIAs

The template provides for indicating whether the DPIA or parts thereof are intended to be published or externally disclosed. The Explainer correctly states that publication may constitute a good practice from a transparency perspective, while sensitive information, particularly concerning security, should not be published.

In the opinion of the Polish Bank Association, it should be emphasised more strongly that, in regulated sectors such as banking, a DPIA may contain information concerning system architecture, security controls, fraud detection mechanisms, vendors, AML processes, cybersecurity and risk management. Publication of such information could increase operational and security risks.

The template should therefore expressly confirm that controllers may limit the scope of publication or refuse publication where justified by security concerns, protection of trade secrets, banking secrecy, effectiveness of fraud prevention mechanisms or protection of the interests of data subjects.

25. The need to clarify the relationship between DPIAs and records of processing activities

The proposed template repeatedly refers to information typically documented within records of processing activities, such as process names, purposes, categories of data, recipients, retention periods, transfers and legal bases.

In the opinion of the Polish Bank Association, the template should clearly clarify the relationship between DPIAs and records of processing activities. A DPIA should not duplicate the ROPA but may refer to information already contained therein as the source of basic information about the processing operation.

Without such clarification, there is a risk of duplication of documentation and inconsistencies between the record of processing activities and the DPIA.

26. The need to clarify the relationship with legitimate interest assessments

The template indicates that where processing is based on Article 6(1)(f) GDPR, a legitimate interest assessment and balancing test should be carried out.

In the opinion of the Polish Bank Association, the template should expressly allow references to separately prepared legitimate interest assessments without requiring duplication of their full content within the DPIA.

A DPIA and a legitimate interest assessment serve different functions. A legitimate interest assessment concerns the permissibility of relying on legitimate interests as a legal basis for processing, whereas a DPIA concerns the assessment of impacts on data protection and risk management. The two documents may complement each other but should not be treated as identical.

27. The need to clarify the concept of "data quality metrics"

Section 2.2.b requires the identification of data quality metrics, requirements or thresholds.

In the opinion of the Polish Bank Association, this field requires clarification. In many processing operations involving personal data, data quality is assessed qualitatively, procedurally or through operational controls rather than through formal metrics or quantitative thresholds.

This applies particularly to legal, compliance, customer service, debt collection, complaints handling, AML, fraud prevention and security-related processes. Requiring formal metrics in such cases may be artificial and disproportionate to the nature of the processing operation.

The Polish Bank Association therefore postulates that the template should allow descriptive explanations concerning data quality and indicate mechanisms ensuring adequacy, accuracy and up-to-dateness of data without requiring quantitative metrics in every case.

28. The need to clarify implementation status categories

The template uses the implementation status categories "planned", "partially implemented" and "implemented". The Explainer further clarifies that "implemented" means a measure existing, deployed and effectively operating in the production environment, supported by evidence confirming its operation.

In the opinion of the Polish Bank Association, such a standard may be appropriate for certain measures but requires flexibility. Not all measures documented in a DPIA are technical measures operating within production environments. Some measures are organisational, legal, procedural, contractual or project-related in nature.

The template should therefore allow different methods of evidencing implementation depending on the nature of the measure. Otherwise, organisations may be forced to create additional evidence documentation for every measure, even where such an approach would be disproportionate.

29. The need to explicitly limit the risk of disclosing sensitive security-related information

Due to the scope of information expected within the template, particularly concerning architecture, assets, security measures, risks and vulnerabilities, the DPIA may become a document containing highly sensitive information from the perspective of organisational security.

In the banking sector, such information may concern system protection mechanisms, transaction monitoring, fraud detection, access management, incident response and vendor controls.

The Polish Bank Association postulates that the template should contain an explicit principle according to which security-related information should be documented only to the extent necessary for assessing risks to the rights and freedoms of data subjects, without requiring disclosure of technical details that could increase the risk of attacks or circumvention of safeguards.

30. The need to ensure consistency of the template with national DPIA lists and supervisory practices

The proposed template refers to national lists of processing operations requiring DPIAs as well as guidance issued by national supervisory authorities. The annex to the Explainer also references materials published by national authorities, including the Polish supervisory authority.

In the opinion of the Polish Bank Association, it is important that the template does not create an additional autonomous catalogue of situations requiring DPIAs beyond Article 35 GDPR and the national lists adopted by supervisory authorities. The template should serve as a documentation tool for DPIAs rather than extending the scope of the obligation to conduct them.

Otherwise, uncertainty may arise as to whether a given processing operation requires a DPIA because this follows from the GDPR or national supervisory authority lists, or solely because the template identifies it as potentially relevant.

31. The need to clarify the meaning of “minimum amount of information”

The Explainer states that the template is intended to provide a way of documenting the key outcomes and the “minimum amount of information” in a format readily acceptable to supervisory authorities.

In the opinion of the Polish Bank Association, this wording requires caution. If the entire template were to be regarded as the minimum expected scope of a DPIA, the resulting documentation burden would be very substantial. In practice, the proposed template covers

an extremely broad range of information that goes beyond what is necessary in many processing operations.

The Polish Bank Association therefore postulates that the EDPB should expressly clarify that “minimum” means the minimum appropriate for the given processing operation and level of risk, rather than an obligation to complete every field with the same degree of detail in every DPIA.

32. The need to adapt the template to large organisations conducting multiple DPIAs

In large financial institutions, a DPIA is not a one-off document prepared for a single project, but rather an element of a broader system of change management, risk management, technology governance and compliance.

For this reason, the template should be capable of functioning effectively within large-scale environments, including organisations conducting numerous processing operations, using multiple systems, relying on many vendors and operating within complex group structures.

The current level of detail may hinder large-scale, repeatable and efficient use of DPIAs. As a result, organisations may focus on formal completion of the template rather than on genuine risk analysis.

33. The need to clarify the treatment of changes in existing processing operations

The template provides for conducting a DPIA in relation to an existing high-risk processing operation where there has been a change in risks, including changes to the processing itself or changes in the organisational or societal context.

In the opinion of the Polish Bank Association, it would be advisable to clarify what level of change should trigger the obligation to update a DPIA and how to distinguish material changes from ordinary operational changes.

In the banking sector, processes, systems and security measures are updated regularly. Not every technical, organisational or procedural change should require a full DPIA update. The template should expressly allow a risk-based approach under which a DPIA update is required only where the change may materially affect risks to the rights and freedoms of data subjects.

34. The need to clarify final decision-making and the conditions for consultation with supervisory authorities

Section 6 of the template provides for a final decision, including rejection of the processing operation, consultation with the supervisory authority, approval of the processing operation or conditional approval of the processing operation.

In the opinion of the Polish Bank Association, it should be clarified that consultation with the supervisory authority is required under Article 36 GDPR where the controller cannot sufficiently mitigate high risk through appropriate measures and the residual risk remains high. The template should not lead to an expansive interpretation of the obligation to consult.

Furthermore, it should be clarified that conditional approval of a processing operation should be permissible where clearly defined measures remain to be implemented before the start of processing or before transition to a subsequent stage of the process.

***

Conclusion of the Polish Bank Association's position

The Polish Bank Association supports the objective of harmonising the approach to DPIAs across the European Union. A common template may prove beneficial both for controllers and supervisory authorities, provided that it remains a practical, proportionate and operationally feasible tool for use within large and complex organisations.

In the opinion of the Polish Bank Association, however, the proposed template requires substantial refinement. The most important changes should consist in clearly embedding the template within the principle of proportionality, distinguishing between mandatory and optional elements, allowing references to existing documentation, limiting unnecessary duplication of compliance documentation and clarifying the methodology for risk assessment.

Particular importance should also be attached to recognising the specific nature of regulated sectors such as the banking sector, where many processing operations result from statutory obligations, supervisory requirements and the necessity to ensure the security of clients and the stability of the financial system.

The Polish Bank Association therefore recommends that the final version of the template should function as a flexible documentation framework rather than as a uniform, maximum mandatory form applicable to all DPIAs. Only such an approach will allow the harmonisation objective to be achieved without excessively formalising the process of assessing impacts on the protection of personal data.