31 July 2026

Position Paper of the Polish Bank Association to the European Data Protection Board regarding the 'Template [2026] for personal data breach notification'

The Polish Bank Association (PBA) welcomes the efforts of the European Data Protection Board (EDPB) to harmonise the manner in which personal data breaches are notified to supervisory authorities. A common European template may reduce differences between the forms used in individual countries, increase the predictability of supervisory authorities' expectations and facilitate the handling of cross-border personal data breaches.

The 'Template [2026] for personal data breach notification', adopted by the EDPB on 8 June 2026 in a version intended for public consultation, is not merely a simple notification form. The document contains an extensive structure of fields, indicates whether they are mandatory, provides tooltips for controllers and sets out detailed Business Logic for the future electronic tool. The template covers the successive stages of a notification, from identification of the data controller and the reporting person, through the description of the personal data breach and the risk assessment, to remedial measures, communication to data subjects, notification to other authorities and the submission of attachments. From the banking sector's perspective, a common template may provide significant assistance, provided that it remains proportionate, capable of being used in the circumstances of an actual incident and interoperable with other reporting obligations applicable to the financial sector. In its current wording, the draft may transform a notification submitted within 72 hours into an extensive reporting and evidentiary process that partly overlaps with the controller's internal documentation of the personal data breach, ICT incident reporting and the technical investigation.

The Polish Bank Association sets out its detailed comments on the draft below.

1. The need to clearly limit the function of the template to the notification referred to in Article 33 GDPR

The draft covers information that may be useful for a comprehensive investigation of a personal data breach but is not always necessary for notifying the supervisory authority. Article 33(3) GDPR defines the minimum content of a notification, comprising a description of the nature of the personal data breach, the contact details of the Data Protection Officer or other contact point, a description of the likely consequences and a description of the measures taken or proposed to address the personal data breach. At the same time, Article 33(5) GDPR imposes a separate obligation on the controller to document personal data breaches, including their circumstances, effects and the remedial action taken. In the PBA's view, the draft partly blurs the distinction between the notification submitted to the supervisory authority and the controller's complete internal documentation of the personal data breach. This concerns, in particular, the extensive description of systems and infrastructure, the detailed risk assessment methodology, information on measures intended to prevent similar incidents, technical reports

and documentation of internal procedures. The template should clearly state that it does not extend the substantive scope of the obligation arising from Article 33 GDPR. Information going beyond what is necessary to submit the notification should be optional or provided at a later stage where the supervisory authority needs it to assess the particular personal data breach.

2. The need to effectively distinguish between an initial notification and Follow-Up Notifications

The draft provides for 'Complete' and 'Incomplete' notifications, as well as the possibility of submitting a Follow-Up Notification or withdrawing a previous notification. This approach should be welcomed. However, it has not been consistently reflected in the designation of individual fields as mandatory. A considerable amount of detailed information has been marked as mandatory even where the controller submits an Incomplete notification. In practice, within the first 72 hours a bank may be unable to determine the definitive root cause of the incident, the final number of data subjects concerned, the complete list of systems, the scope of any data exfiltration, the effectiveness of the safeguards applied or the long-term remediation plan. Article 33(4) GDPR expressly allows the controller to provide information in phases where it is not possible to provide it at the same time. The PBA therefore recommends clearly distinguishing the initial notification from one or more Follow-Up Notifications, with the possibility of marking the last notification as Complete.

3. The need to clearly distinguish between mandatory, conditionally mandatory and optional fields

The draft designates individual fields as mandatory, conditionally mandatory or optional, but this structure is not fully consistent. In many instances, a field formally marked as mandatory concerns information that may not be available, may not apply or may go beyond what is required in the particular notification. The template should introduce at least four clear categories: information mandatory in an initial notification, information mandatory once it has been established, information required only in a particular scenario, and voluntary information. It should also be possible to select 'not applicable', 'not known at this stage' and 'cannot be determined'. These answers have different meanings and should not be treated as equivalent.

4. The need to take account of the operational conditions in which a major incident is handled

During the initial phase of a major incident, a bank carries out technical, operational, legal and communication activities in parallel. The priorities are to contain the incident, preserve evidence, mitigate the effects on customers, restore the availability of services and establish the basic facts. An extensive form requiring detailed descriptions, classifications, calculations and attachments at the same time may divert resources from the actual incident response. This risk is particularly significant in the case of ransomware attacks, incidents affecting payment systems, large-scale operational errors and incidents involving ICT third-party service providers. The template should be designed to assist the controller in rapidly providing the most important information rather than competing with the activities necessary to contain the incident.

5. The need to clarify the distinction between detection and awareness of a personal data breach

The draft separately addresses the time at which the personal data breach occurred, the date of its detection and the date and time of awareness of the data controller of the personal data breach. This distinction is necessary but requires a more precise explanation. In practice, detection of a technical anomaly or security incident does not necessarily mean that the controller already has a sufficient degree of certainty to conclude that a personal data breach has occurred. A period of time may be required between detection of the initial signal and confirmation that the incident affects personal data in order to perform a basic verification. The form should distinguish between the time at which an anomaly was detected, the time at which information was provided by a data processor or other party, the time at which an impact on personal data was confirmed, and the time at which the controller became aware of the personal data breach.

The field concerning the reasons for late notification also requires clarification. According to the Business Logic described in the draft, field 49 is to be visible where 'date of awareness of breach + 72h > current time'. This condition means that the 72-hour period has not yet expired. The field should be activated where the current time is later than the time of awareness plus 72 hours.

6. Excessive scope of data relating to the reporting person

The draft provides for the possible inclusion of a field concerning the National identification number of the reporting person. In the PBA's view, such information should not form part of the common European set of notification data. Where it is required under national law or for user authentication purposes, it should be collected outside the substantive content of the personal data breach notification. In banks, a notification is usually the result of cooperation between the Data Protection Officer, the information security function, the incident response team, the legal department, compliance and the relevant business unit. The template should permit a functional contact point to be provided, including a dedicated team or organisational email address, without requiring the disclosure of an excessive amount of personal data relating to a particular employee.

7. The need to amend the 'Accuracy & Responsibility' field

The 'Accuracy & Responsibility' field is described as a confirmation concerning liability for the accuracy of the information provided. Its meaning is, however, unclear. In its current wording, the field may suggest personal liability on the part of the employee submitting the notification. This would be inappropriate, particularly in the case of an Incomplete notification, where some information is by definition preliminary, estimated or subject to further verification. If the field is retained or implemented by a national supervisory authority, it should clearly refer to the reporting person acting on behalf of the controller and to the controller's current state of knowledge, rather than to the employee's personal liability. It should also be made clear that the information may subsequently be corrected and supplemented without creating a presumption that the information originally provided was inaccurate or unreliable.

8. The need to adapt the form to incidents involving groups and supply chains

The draft is essentially based on a model involving one controller and additional parties classified as data processors, joint controllers or other parties. This model may be insufficient for incidents involving banking groups, shared service centres, sector-wide information systems, cloud service providers or processors acting simultaneously for multiple controllers. A single technical incident may affect multiple banks and result in several related personal data breaches differing in the scope of data, the number of data subjects concerned and the level of risk. The template should allow notifications to be marked as related to a common technical incident, identify a shared provider and use a common incident identifier, without affecting the separate responsibility of each controller.

9. The need to ensure interoperability with reporting under DORA

For the banking sector, a personal data breach may simultaneously constitute an ICT incident subject to reporting under DORA. That Regulation establishes uniform digital operational resilience rules for financial entities, including banks, and includes a reporting regime for major ICT-related incidents. The EDPB draft is limited to asking whether the incident has been notified to other authorities and to providing the authority and the case ID. This does not address the problem of repeatedly providing the same information through different forms.

The PBA recommends that the template be interoperable with sectoral reporting. It should allow the use of a common incident identifier, the import of data, references to information previously provided to another competent authority and the reuse of common elements of reports. Harmonisation in the area of data protection should not result in the creation of another separate documentation system operating alongside DORA and other sectoral obligations.

10. Excessive scope of information concerning systems and infrastructure

Field 63 requires a description of the systems, software, services and infrastructures involved in the personal data breach and where they are located. Examples include production customer databases, test infrastructure, accounting software and payment system software. In the case of a bank, this information may reveal the architecture of critical systems, the segmentation of environments, the location of assets, technical dependencies and the structure of databases. Excessively detailed disclosure may increase security risks, hinder remedial action or adversely affect interests connected with an ongoing investigation.

The mandatory field in the form should require a description at a level sufficient to assess the personal data breach. More detailed technical information should be provided, where necessary, upon a reasoned request from the supervisory authority and through an appropriately secured channel.

11. The need to refine the taxonomy of incident types and causes

The draft contains an extensive list of incident types. This may facilitate statistical analysis of notifications, but some categories overlap or combine different phenomena.

For example, the category ‘Encrypted device / ransomware’ covers both a potential protective measure and a type of malicious attack. The categories ‘Hacking / malware activity detected’, ‘Unauthorised access to personal data in IT systems’, ‘Data exfiltration / unauthorised extraction of personal data’ and ‘Security vulnerability (likely) exploited’ may simultaneously

describe different elements of the same incident. The form should clearly allow multiple selections and distinguish between the nature of the personal data breach, the attack vector, the direct technical cause, the organisational cause and the consequences of the incident. In the case of data exfiltration, it should be possible to indicate the level of certainty and the basis for the assessment. The absence of evidence of exfiltration does not always mean that the controller has sufficient evidence confirming that personal data were not exfiltrated.

12. The need to separate the assessment of the effectiveness of safeguards from the identifiability of individuals

Field 57 combines, in a single question, the assessment of whether the data were unintelligible to anyone who was not authorised to access them with the assessment of whether individuals were identifiable. These are two distinct circumstances that may independently affect the risk assessment. Encryption or another protective measure may make the data unintelligible to an unauthorised person even though the data relate to identifiable individuals. Conversely, the absence of direct identifiers does not automatically mean that identification is impossible when other available information is taken into account.

The PBA recommends separating these issues into two distinct fields: one concerning the effectiveness of measures that render personal data unintelligible and another concerning the possibility of directly or indirectly identifying the individuals affected by the personal data breach.

13. The categories of data subjects concerned are not adapted to the banking sector

The category 'Customers (current and prospects)' is too narrow and requires a linguistic correction. In particular, it omits former customers whose personal data continue to be processed by a bank after the contractual relationship has ended. A personal data breach may concern the personal data of former customers retained in connection with retention obligations, the handling of complaints, the establishment, exercise or defence of legal claims, AML obligations, fraud prevention, the archiving of documentation and ensuring the security of the bank and its customers. At a minimum, the category should read 'Customers: former, current and prospective'.

Personal data breaches in banks may also concern authorised representatives, representatives of corporate customers, beneficial owners, members of the governing bodies of legal persons, guarantors, co-borrowers, providers of collateral, heirs, cardholders, online banking users, originators and beneficiaries of transfers, employees of counterparties and individuals subject to fraud or AML monitoring. The template should permit more flexible and multiple classification of categories of data subjects without requiring most relationships typical of the financial sector to be placed in the general category 'Additional concerned data subjects'.

14. The need for a cautious approach to the category 'Vulnerable individuals'

The form includes the category 'Vulnerable individuals', with examples such as elderly persons, refugees, persons with disabilities and victims. The controller does not always possess information allowing it to definitively determine the particular vulnerability of the data subjects affected by the personal data breach. In many cases, this circumstance may only be identified during further analysis. The template should allow the controller to indicate that vulnerable

individuals may be among the data subjects concerned without requiring a final classification at the stage of the initial notification. It should also recognise that vulnerability may result not only from personal characteristics but also from the nature of the service, a person's financial situation, dependence on access to an account or the potential consequences of exclusion from financial services.

15. Overly broad categories of financial data

The draft includes, among others, the categories 'Economic and financial data', 'Payment methods', 'Profile data', 'Identification data' and 'Official documents'. These categories are too broad to properly reflect the different levels of risk arising in the banking sector. Disclosure of a bank account number has a different risk profile from disclosure of transaction history, account balance, authentication data, authorisation codes, payment card data, credit documentation, indebtedness information, scoring results or complete KYC documentation.

The template should allow at least the following to be distinguished: account data, payment instrument data, transaction data, authentication and authorisation data, financial situation data, indebtedness data, creditworthiness data, scoring data, KYC and AML data, and copies of identity documents. Such a distinction would enable a more accurate assessment of the likely consequences of the personal data breach, particularly the risks of fraud, identity theft, account takeover or the use of disclosed information for social engineering.

16. Unclear meaning of the number of personal data records

The draft attempts to explain the difference between the number of data subjects, the number of data categories and the number of personal data records. The explanation provided is, however, complex and does not ensure a uniform understanding of the term 'record'. In banking systems, a record may mean a database entry, account, transaction, document, message, file or set of related fields. The same personal data may also appear in multiple systems and technical copies. The template should allow the controller to indicate the unit of measurement used, the method of estimation and the limitations of the calculation. It should not require all elements to be artificially converted into single database entries where the number of accounts, documents, transactions, messages or files provides a more meaningful measure.

17. The need to supplement the risk assessment model

The draft requires the severity of potential impacts to be classified as 'Minor', 'Moderate' or 'Severe', followed by the outcome of the risk assessment. It does not, however, provide a separate structured field concerning the likelihood that adverse effects will materialise. Risk to the rights and freedoms of natural persons should not be assessed solely by reference to the severity of potential harm. Relevant factors also include the likelihood of the data being used, the nature of the recipient, the possibility of identifying the individual, the duration of exposure, the effectiveness of safeguards, the possibility of linking the data with other information and the reversibility of the effects. The template should separately address likelihood, severity and the final level of risk. At the same time, it should allow the controller to use its own documented methodology, provided that the methodology makes the basis for the adopted classification understandable.

The form should also clarify how to proceed where the controller submits a notification as a precaution while its current assessment indicates that the personal data breach is unlikely to result in a risk. The form should distinguish this situation from the subsequent withdrawal of a notification after new information has been obtained.

18. The need to correctly address communication to data subjects

The draft includes the response 'No, the investigation is still ongoing' as one of the reasons for not communicating the personal data breach to data subjects. The mere fact that an investigation is ongoing does not constitute an independent ground for postponing communication where the controller has already determined that the personal data breach is likely to result in a high risk. Article 34(1) GDPR requires the controller to communicate the personal data breach to the data subject without undue delay in such a case. The option should be replaced with wording indicating that the assessment of high risk has not yet been completed. The mere continuation of the investigation does not justify postponing communication where a high risk has already been established.

The situation in which individual communication would involve disproportionate effort has also been placed incorrectly. A public communication or similar measure under Article 34(3)(c) GDPR is an alternative means of informing data subjects, rather than a situation in which they are not informed at all. It should be included in the section concerning the means of communication.

19. The need to enable phased and multi-channel communication

In the case of extensive personal data breaches, a bank may inform different groups of data subjects at different times and through different channels. This may result from the scope of the data, the nature of the relationship, whether the contact details are up to date and the different measures that the data subjects should take. The template should allow phased communication to be described, including several dates, different channels and different versions of the communication. It should also allow an explanation that some data subjects could not yet be informed for objective reasons. In justified cases, it should also be possible to indicate that the timing or scope of the communication was agreed with law enforcement authorities where immediate disclosure of details could hinder action to identify the perpetrator or secure the systems.

20. The need for a more precise distinction between the types of measures taken after the personal data breach

The draft distinguishes measures taken to address the personal data breach and mitigate its consequences from measures taken to prevent similar personal data breaches. The distinction is justified, but the current structure may lead to duplication of the same information. The template should separately address measures intended to immediately contain the incident, restore system availability, protect data subjects from adverse effects, preserve evidence, remediate the immediate vulnerability and implement long-term changes resulting from root cause analysis. A complete plan of long-term preventive measures should not be expected in the initial notification. In many cases, those measures can only be properly determined after the technical and organisational analysis has been completed.

21. Risk of excessive reporting to multiple data protection supervisory authorities

The section concerning cross-border processing requires the lead supervisory authority, the countries in which the controller has establishments, the countries in which affected data subjects are located and the supervisory authorities to which the personal data breach has been or will be notified to be identified. The form should clearly reflect the one-stop-shop mechanism and should not suggest that the controller is required to notify the same personal data breach to all supervisory authorities in countries where affected data subjects are located. It should distinguish between notification to the lead supervisory authority, notifications submitted as a precaution due to uncertainty as to competence, situations in which the one-stop-shop mechanism does not apply, and notifications submitted to other authorities under separate legislation.

In the section concerning controllers not established in the EEA, the expression 'EAA supervisory authority' should also be replaced with 'EEA supervisory authority'.

22. The need to clarify the meaning of questions concerning notifications to other authorities or bodies

Questions concerning notification to the police, judicial authorities, national cyber security centres and other supervisory authorities may be useful for understanding the broader context of the incident. The template should, however, clearly state that the mere inclusion of these questions does not create an additional notification obligation. Such an obligation may arise only under the relevant sectoral or national legislation.

The controller should be able to refer to the case ID of a report submitted under DORA or other legislation and indicate that certain information has already been provided to the competent authority. The template should allow the controller to indicate that certain aspects of the incident are the subject of proceedings conducted by law enforcement authorities and allow a secure method for providing detailed information to be agreed, without prejudice to the controller's obligations towards the supervisory authority.

23. Attachments should be clearly voluntary

The draft provides for the possibility of attaching, among other things, a report into the cyberincident, a ransomware note, a phishing message, the internal procedure to notify a data breach, the internal policy to delete or destroy outdated personal data and the communication sent to the wrong recipient. Although attachments are marked as optional, their detailed enumeration may create an expectation that they should routinely accompany a notification. These documents may contain information covered by trade secrets, banking secrecy, confidentiality of proceedings, confidentiality of legal communications, personal data of third parties and detailed information on vulnerabilities and safeguards. The template should clearly confirm that attachments are voluntary, that they may be partially anonymised or redacted, and that they may be submitted at a later stage. It should also provide for a secure transmission channel and the possibility of marking materials as confidential.

24. The need to protect banking secrecy, trade secrets and information concerning safeguards

The scope of information expected by the draft may include information concerning customers, transactions, banking systems, providers, fraud detection methods and security controls. The PBA recommends introducing a general principle under which information should be provided at a level of detail sufficient to assess the personal data breach and the risk to data subjects, without unjustified disclosure of information covered by banking secrecy or trade secrets, or information the disclosure of which could weaken the organisation's security. This principle should not exclude the supervisory authority's power to obtain information, but should allow for a proportionate approach, secure communication channels and the separation of detailed technical documentation from the basic form.

25. The need to enable automation and reuse of data

As the draft is intended to form the basis of an electronic form, it should from the outset allow automatic integration with internal incident management systems. Large banks use tools that record the timeline of an incident, the systems involved, remediation measures, data categories and decisions concerning reporting. Manually re-entering this information into a separate form increases the risk of errors and inconsistencies. The common template should allow data to be submitted in a structured format, the use of technical interfaces, the export and import of information and the use of a common incident identifier in successive notifications.

26. The need to correct errors in the Business Logic and drafting errors

The draft contains numerous inconsistencies that must be corrected before the tool is implemented. In addition to the reversed logic in field 49, field 53 refers to the unidentified condition 'Yes, if 41a'. Field 83 concerning likely consequences in case of a breach of availability is to be visible where an integrity breach has been selected. In field 89, two answers are designated by the letter 'c'. Field 95 refers to answer 'm)' as 'Other measures', whereas that option is designated as 'o)' in the list. Section 6.3 uses the abbreviation 'EAA' instead of 'EEA'. Moreover, field 115 is described as the list of EEA countries where the controller has an establishment, while the tooltip refers to countries concerned by the breach. Field 118 refers to 'other EU Supervisory Authorities', although the list also includes supervisory authorities of EEA countries. In field 97, two answers are designated by the letter 'b'. The Business Logic for field 100 treats the situation under Article 34(3)(c) GDPR as one in which data subjects will not be informed, even though that provision requires a public communication or similar measure whereby data subjects are informed in an equally effective manner. The document also contains numerous linguistic and typographical errors, including 'your are', 'metodology', 'sufficent', 'attachements', 'datasubject', 'mentionning', 'sumed up' and 'to what extend'. In an electronic form, these errors are not merely drafting issues. Defective Business Logic may result in incorrect fields being displayed, their mandatory status being incorrectly designated or difficulties in submitting a notification.

***

Conclusion of the Polish Bank Association's position paper

The Polish Bank Association supports the harmonisation of personal data breach notification at European Union level. A common template may increase regulatory predictability, reduce differences between the practices of national supervisory authorities and facilitate the handling

of cross-border incidents. In its current form, however, the draft requires substantial refinement. The most important changes should consist in clearly limiting the function of the template to the notification under Article 33 GDPR, effectively distinguishing the initial notification from one or more Follow-Up Notifications, with the possibility of marking the last notification as Complete, limiting the obligation to disclose detailed technical information, and ensuring interoperability with sectoral reporting, in particular reporting under DORA.

It is also important to adapt the categories of data subjects and data to the realities of the financial sector. The template should take account of former customers and other persons connected with banking relationships, and should distinguish between financial, transaction, payment, credit, authentication and AML data. The final template should assist the controller in rapidly providing the supervisory authority with the most important information rather than transform the initial phase of incident response into an extensive reporting and evidentiary process. Only a modular, proportionate and interoperable template can genuinely facilitate controllers' compliance with their obligations and contribute to the harmonisation of supervisory practice.