Brussels, 30 July 2026
FINAL

EACB Position Paper on the EDPB Template for Personal Data Breach Notification

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 29 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,400 locally operating banks and 35,150 outlets cooperative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 228 million customers, mainly consumers, retailers and communities. The cooperative banks in Europe represent 91 million members and 747,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the opportunity to provide the European Data Protection Board (EDPB) with its comments on the Template for Personal Data Breach Notification.

The EACB welcome the EDPB's objective of promoting harmonisation, consistency and legal certainty across the European Economic Area in relation to personal data breach notifications under Articles 33 and 34 GDPR. A standardised template has clear potential to facilitate cooperation between controllers and supervisory authorities, particularly in cross-border contexts.

For organisations operating in complex and highly digital environments, further harmonisation is of significant value. At the same time, it is important that any common approach remains workable in practice and sufficiently aligned with existing regulatory frameworks. Ongoing EU initiatives aimed at streamlining reporting and enabling the reuse of information illustrate the broader importance of reducing fragmentation, which is equally relevant in this context.

The proposed template represents a constructive step in this direction. The observations below are intended to contribute to its further development, with a view to ensuring that it remains proportionate, practical and closely aligned with the GDPR framework.

Nonetheless, we would like to underline that in **its current form, the template does not achieve this key objective of simplification in its entirety**, as in some areas, the administrative burden tends to be strengthened more than diminished.

Consideration could be given to **structuring the template into two distinct sections**:

(i) information strictly required under Articles 33(3) and 34 GDPR, and
(ii) supplementary information to be provided upon request by supervisory authorities.

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

Proportionality

The current template appears to introduce a relatively detailed structure at the initial notification stage, including elements such as system descriptions, predefined classifications, structured risk scoring, root cause analysis, and supporting documentation. Given the varying nature and complexity of personal data breaches, it may be helpful to consider whether a **more flexible and proportionate approach could be maintained** at this stage.

In particular, it may be useful to ensure that the template continues to reflect the balance embedded in **Articles 33 and 34 GDPR**, whereby notification focuses on conveying the key relevant facts. Some elements of the template could be perceived as more closely aligned with internal investigation processes, whereas the purpose of notification is more limited.

The template may also risk transforming the notification process into a **justification exercise**, requiring controllers to explain in detail internal decision-making and assessment processes, even where the notification itself already reflects the conclusion that the applicable legal threshold has been met.

Moreover, the mandate created by Articles 33(3) or 34 should be respected on information required on controllers. That balance also materialises in the **72 hours notification obligation** set out in Art. 33(1), which is already strict enough, and **should not lead for the template to expand the need for data collection** such as in system description, assessment methodology and attachments, thus increasing the risk that controller will make initial notifications with incomplete information. This may in turn require additional follow-up notifications, even in relatively straightforward cases.

Relatedly, certain aspects of the template may place emphasis on the underlying reasoning and assessment. While such information can be valuable in specific cases, it may not always be necessary at the point of initial notification. A requirement to provide this level of detail in all cases could have practical implications, including for the timeliness of reporting.

The level of granularity proposed also merits consideration. While detailed classifications may support analytical objectives, they may be more difficult to apply consistently where information is still developing, which could in turn affect overall data quality.

A more high-level and flexible approach at the initial stage could therefore **support both clarity and timely reporting**, while allowing for further detail to be provided as needed.

Additionally, it may be helpful to further reflect on the necessity and proportionality of the identifying information requested from the reporting individual. In particular, more clarity would be welcomed on why a national

identification number would be required in cases where the notification is submitted in a professional capacity, thus ensuring alignment with data minimisation principles.

Article 33(3) GDPR

This article exhaustively defines the information that must, at a minimum, be included in a notification, e.g. the nature of the personal data breach, the name and contact details of the data protection officer or other contact point where more information can be obtained, the likely consequences of personal data breach, and the measures taken or proposed to be taken by the controller to address the personal data breach.

That being said, the proposed **template contains numerous fields that are not based on these provisions**, thus deleting any justification for these additional fields in any way. The mention of 'mandatory' in the template does not bring any legal clarity, as it is unsure whether this obligation comes from the authority's perspective or whether their mandatory nature is intended to stem from binding GDPR requirements.

Sections related to system descriptions, e.g. 'description of the systems, software, services, and infrastructures involved in the personal data breach and where they are located', constitute significant new requirements that exceed the description of the nature of the breach required under Art. 33(3)(a). Producing a system inventory in the context of an acute personal data breach is operationally extensively burdensome.

This approach serves the authority's cybersecurity investigation needs, rather than the notification obligation under Art. 33(3). Moreover, requiring such information may lead to the unnecessary disclosure of organisations' trade secrets to supervisory authorities.

Similarly, **field (90)** 'Further description of the risk assessment carried out by the data controller' goes beyond Art. 33(3)(c) requirement of a description of the likely consequences, by demanding the controller to describe the risk assessment methodology and explain the factors considered in the assessment.

The same applies to **field 106** 'Content of the information provided to the data subjects', also oversteps Art. 34(2) definition of the content of such obligations, as it does not require that the content is to be submitted as a copy to the supervisory authority in connection with a notification under Art. 33.

Field 109 and Section 7 also suffer from outstripping interpretations of Articles 33 and 34. The former includes a question on whether the incident has been reported to the police/judicial authorities as a criminal offence. This field is not based on any provision of the GDPR. The filing of a criminal complaint falls within

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

national criminal procedural law and is unrelated to the personal data breach notification under Art. 33 GDPR. Section 7 requires the submission of several attachments, including a dated copy of the communication provided to data subjects, the risk assessment, a breach investigation report, the ransomware note, the phishing message, internal procedures, and the message sent to the wrong recipients. The submission of such attachments is not required under Articles 33 or 34 GDPR.

Allowing such templates to go beyond GDPR requirements, in addition of lacking justification, also create unnecessary burden, in opposition with simplification attempts launched by the Commission these past two years.

Operational feasibility

The GDPR allows phased notification, recognising that full information may not be available within 72 hours. Incident response processes are inherently iterative, and establishing scope, affected systems, and root causes often requires time, particularly in complex or third-party environments. Reflecting this **more explicitly in the template**, for example through **a tiered approach**, could enhance both accuracy and usability.

Further **clarification** would be welcome on the **concept of 'awareness'** as the starting point of the 72-hour notification period under Art. 33(1) GDPR, including whether this refers to initial detection, confirmation of a personal data breach, internal escalation, or formal registration of the incident. Such clarification would promote greater consistency and legal certainty in the application of the notification deadline.

Operational considerations also arise in light of overlapping reporting obligations. Organisations may be required to report the same incident under multiple frameworks, which can create duplication during time-critical response periods. In this regard, further alignment and facilitation of information reuse – consistent with broader EU policy discussions – could help ease the overall operational burden.

Consistency with the GDPR risk-based approach

The risk-based approach is a central element of the GDPR. Applying this approach in a coherent and practical manner in breach notification would be advised. Requiring detailed descriptions of underlying risk methodologies may, however, present challenges, as organisations typically rely on internal frameworks tailored to their specific context. Additional standardisation may therefore introduce complexity without clear added value.

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail: secretariat@eacb.coop

Greater consistency in risk terminology across GDPR instruments would be beneficial, as current variations may create uncertainty. While the template provides a useful structure, it could further evolve towards a more practical and harmonised approach. Existing national guidance illustrates that risk concepts can be effectively translated into clear and operational categories. A flexible taxonomy, allowing for high-level initial assessments with scope for refinement, may support this objective.

Alignment with other regulatory frameworks

The interaction with other reporting obligations, particularly in the areas of cybersecurity and operational resilience, deserves careful consideration.

Organisations are often required to report the same incident to multiple authorities with differing requirements, timelines, and classifications, which can increase complexity during critical response periods.

Enhancing interoperability and supporting the reuse of information across frameworks could help to reduce duplication and contribute to greater overall coherence. This would be consistent with broader EU efforts to simplify reporting and improve efficiency.

Separation between internal reporting and external notification

Maintaining a clear distinction between internal incident management processes and external notification may be helpful. Internal processes are typically more detailed and support investigation and remediation, whereas external notification serves a specific regulatory purpose.

It may be useful to position the template as a standardised external reporting layer that can be mapped onto existing internal incident management processes, rather than as a replacement for established internal frameworks.

Ensuring that the level of detail required for notification remains proportionate could also help preserve this distinction, while still allowing supervisory authorities to request additional information where appropriate.

Supporting documentation and data quality considerations

Requiring supporting documentation at the time of initial notification may, in some cases, present practical constraints, as investigations are often ongoing. Allowing

such documentation to be provided at a later stage, where relevant, could offer a more proportionate approach.

Similarly, a focus on clear and high-level classifications may support both usability and data quality, particularly where information is still evolving.

Conclusion

The EDPB's initiative is welcomed as an important step towards strengthening consistency and cooperation across the EEA. In considering the further development of the template, it may be helpful to:

- ensure strict adherence to GDPR requirements without extending beyond the scope of Articles 33 and 34
- maintain proportionality and avoid unnecessary prescriptiveness
- reflect the evolving and phased nature of breach investigations
- align, where possible, with broader EU efforts to streamline reporting
- support a practical and consistent risk-based approach
- promote interoperability with other regulatory frameworks
- preserve an appropriate distinction between internal processes and external notification

A balanced and pragmatic approach in this regard could support both effective supervision and efficient incident response in practice.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Marieke van Berkel, Head of Department Retail Banking, Financial Markets, Payments, Digitalisation (marieke.vanberkel@eacb.coop)
- Chiara Dell'Oro, Director for Digitalisation (chiara.delloro@eacb.coop)