EBF_047046

31 July 2026

EBF Response to the EDPB Consultation on its Template for Personal Data Breach Notification

The European Banking Federation (EBF) welcomes the initiative of the EDPB to introduce a standardised personal data breach notification template; this can enhance harmonisation, legal certainty, and cooperation across the EEA, particularly in cross-border cases. It is important, however, that the template remains proportionate, supports rapid and efficient reporting, and ensures alignment with existing regulatory frameworks and the broader EU efforts to streamline reporting.

While specific comments on specific sections are provided below, we would like to highlight some key points.

- **Concerns Regarding Proportionality, Scope, and Level of Detail in the Proposed Template**

The template would benefit from a **more proportionate and flexible approach**, particularly at the initial notification stage. In its current form, it risks significantly increasing the complexity of the notification process, not least because of the level of detail required, which may create barriers to timely notification.

In particular, we have identified three main concerns with the proposed template:

1) Volume of information and detail requested, which is considerably higher than what currently required in the notification templates provided by national DPAs;
2) Information requirements exceeding Article 33 GDPR; and
3) Disclosure requirements extending to sensitive security-related information.

A) High volume of information and detail requested

Compared to the templates provided by national DPAs, **the total number of fields/questions has increased significantly**. Certain elements – such as extensive justification of assessments and highly granular classifications – may also create operational challenges, particularly when information is still evolving, which may in turn affect both reporting timelines and data quality. Given the high volume of information requested, it is highly likely that, if the template remains unchanged, controllers will, in the vast majority of cases, submit pre-notifications/notifications that are incomplete with respect to the 72-hour deadline.

B) Information requirements exceeding Article 33 GDPR

Several fields, and the associated level of detail requested (e.g., risk scoring, root cause analysis, system descriptions, documentation, etc.), **also appear to go beyond what is required under Article 33 GDPR**. Article 33 GDPR requires controllers to provide information on the nature of the data breach, its likely consequences, and the measures taken or proposed to be taken to address it; by contrast, the template requires

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

the submission and disclosure of extensive internal documentation, including confidential internal assessments, investigation reports, security-related information and internal policies. In practice, the template resembles more an internal investigation processes rather than an external notification. Requiring such documentation as a standard attachment in a data breach notification template appears disproportionate and may create additional risks and concerns for controllers (as discussed in the sections below).

In particular, we consider **the following requirements to be excessive and falling outside the scope of Article 33 GDPR, and as such, should be deleted:**

- **Field 25 – National identification number**: the identity and contact details of the reporting person are sufficient. An additional requirement for the national ID number lacks necessity and poses a risk to the confidentiality of such sensitive data;
- **Field 106 - Content of the information provided to the data subjects**: such communication may include data subjects' personal data (including identification, account and financial data). Such an additional requirement may pose a risk to the confidentiality of data subjects' personal data.

C) Disclosure of sensitive security-related information

We are of the view that the requirements to disclose internal control frameworks and security practices may create additional security risks and should only be requested where strictly necessary. In particular, **the following entries are particularly concerning and should be deleted:**

- **Field 63 - Description of the systems, software, services, and infrastructures involved in the personal data breach and where they are located**
- **Field 90 - Further description of the risk assessment carried out by the data controller**

Recommendations

With a view to supporting prompt and efficient reporting, we recommend that the EDPB:

1. **Clearly distinguishes between: (i) the information required for the notification itself under Article 33 and (ii) the supporting documentation** that controllers must retain under with the accountability principle and make available only upon specific request from the supervisory authority.
2. **Distinguishes between internal incident management processes and external notification**, ensuring that reporting stays proportionate and focused on relevant supervisory needs.
3. **Considers reducing and/or aggregating the number of questions** and avoid including unnecessary complexity (e.g., question 56, where question 55 should suffice).
4. **Deletes requirements to disclose information revealing sensitive, security-related information** that may lead to additional security risks for controllers.

- **Format of the Template**

We understand that the intention is to report personal data breaches via an online form[1]. In our view, this will generate a significant additional workload for controllers compared to the current notification situation, where controllers attach their report directly in the DPA's reporting platform. Unless some form of automation is foreseen, this could lead to manual copy-pasting and potentially poor quality of submitted data, and make it difficult to include a four-eye control.

From an operational perspective, it would also be beneficial for the **template to better reflect the iterative nature of incident response and the possibility of phased notifications under the GDPR** to better support timely and accurate reporting. The template should continue to reflect the GDPR's risk-based approach in a practical and consistent manner, allowing for a high-level initial assessment and further refinement as more information becomes available. To this end, **the template should expressly recognise that information provided in an initial notification may be preliminary and may subsequently be updated or corrected as the investigation progresses. A tiered or staged model could support this.**

- **Greater Alignment with other Reporting Frameworks**

Greater alignment with other regulatory reporting frameworks (e.g., in cybersecurity and operational resilience) and enabling reuse of information would help reduce duplication and administrative burden, in line with the broader EU policy objectives. The current situation is characterised by significant complexity resulting from incident reporting requirements established in a variety of legal acts, addressed to a variety of authorities and set in different timelines, templates and taxonomies. This fragmentation and overlap between horizontal and sectorial acts, carries high compliance burdens, leading to an over-commitment of resources.

By way of example, banks and other financial institutions in scope of DORA are subject to parallel mandatory incident reporting obligations to financial supervisors (NBB, ECB/SSM) within tight and partially overlapping deadlines.

We would therefore appreciate if the EDPB, in coordination with financial sector authorities could:

- Ensure **alignment of reporting templates and greater consistency in risk terminology/taxonomy across legal acts** to enhance both clarity and practical usability;
- Provide **guidance on how GDPR data breach notifications relate to, or can be coordinated with DORA major incident reports**, to avoid duplicative or conflicting notifications on the same event; and
- Allow controllers to cross-reference information already submitted under other regulatory reporting frameworks, such as DORA or NIS2, and to attach or reference existing incident reports instead of being required to re-enter the same information manually.

[1] EDPB, Template for personal data breach notification: "*This template is primarily designed to be implemented by DPAs via an IT tool. It incorporates rules to collect certain information only when necessary. It includes predefined values and recommended tooltips to facilitate the answering for organisations*."

Section 2 – Identification of the data controllers and the reporting person

Field 12 – Name of organisation: we recommend replacing the entry "Name of the organisation" with "Name of the Controller".

Field 15 – Type of organisation: it remains unclear what threshold(s) controllers should rely on to know whether they qualify as a "microenterprise" or a "small enterprise" and relatedly, which threshold DPAs will use to assess such qualification. To ensure legal certainty and consistent application, we recommend referring directly to the definitions provided in Article 2 of the Annex to the Commission Recommendation 2003/361/EC.

Field 23 - Function of the reporting person: we note that the DPO is listed as the first option for the person reporting a data breach. Given **the independent and supervisory role of the DPO**, it would be more appropriate for the reporting person's function to be listed as follows:

Field	Value
Function of the reporting person	A) Controller (or delegate e.g. first line privacy office) B) Legal representative C) Other, ……

The same consideration applies to **Field 33 - More information about the incident can be obtained at**, where the DPO should be removed as first option.

As regards the DPO, we recommend including an additional field under Section 2.3.1 - About the data protection officer, asking whether the DPO has been informed of the data breach.

We also note the presence of double entries (i.e., Fields 21-24 & Fields 33-36); we propose merging them, as keeping them separate would create additional administrative effort as appointing multiple contact points/individuals to manage a single incident could result in inconsistent communication, additional coordination efforts, and confusion during times of crisis.

Field 25 – National Identification Number: we question the rationale for, and necessity of, requiring the National identification number of the reporting person. The reporting person's identity and contact details should be sufficient to enable the competent authority to identify and communicate with the reporting person. Requiring the inclusion of the national identification number does not appear necessary or proportionate for this purpose and is probably not in line with the data minimisation principle in Article 5(1)(c). The sharing of such information also poses a risk to the confidentiality of such sensitive data. We therefore **strongly recommend removing such requirement**.

Field 26 – Accuracy & Responsibility: Field 26 requires controllers to provide "*information on the liability for the accuracy of the information provided (can be combined with Art. 13 information)*". The purpose and scope of this requirement are unclear. In particular, it is not evident what kind of liability this entail/is envisaged and how this relates to the information obligations under Article 13 GDPR, or on what legal basis it is imposed. We would therefore **welcome clarification from the EDPB regarding the nature and intended purpose of this requirement, the expected input, the foreseen insights from this for the EDPB, as well as an explanation of why this field is considered mandatory**.

Field 34 – Name of the contact person: it may be worth reconsidering the wording of this field to also allow for the use of common mailboxes. This would be more practical for larger organisations.

Field 38 – Are other parties such as data processors or joint controllers involved?: with reference to the non-exhaustive list of organisations potentially involved in a data breach, we recommend including a reference to "*other independent controllers*", as these entities (e.g., mail delivery companies) may sometimes be relevant parties in data breaches.

Field 39 – Qualification of the other involved party: to ensure greater clarity, we recommend replacing the term "qualification" with "role(s)".

Field 41 – Contact details: the relevance and mandatory nature of the requirement to provide the contact details of other involved parties in a data breach is unclear. In particular, **the requirement to include the contact details of processors should be removed from the template**. As per the GDPR, it is the controller who is responsible for communicating with the supervisory authority; processors do not bear responsibility in the reporting process.

Section 3 – Initial information on the personal breach

Field 46 – Beginning date and time of personal data breach: Considering that a data breach may have a cross-border dimension, we recommend including an option to specify/select the relevant time zone(s) (e.g., CET). Moreover, we note that the exact date and time of a data breach might not always be known with precision, even at a later date. Requiring this information could lead to inaccurate or speculative reporting. We therefore recommend removing this field, or at a minimum making it optional where the exact timestamp cannot be determined.

Fields 48 - Date and time of awareness of the data controller of the personal data breach & 49: We would welcome further **guidance on the interpretation of the concept of "awareness"** as the starting point of the 72-hour notification period under Article 33(1) GDPR. In particular, it would be useful to clarify whether this threshold is reached upon e.g., initial detection of a potential breach, confirmation that a personal data breach has occurred, internal escalation, or formal incident registration. To promote regulatory consistency, we recommend that the EDPB **aligns its interpretation of "awareness" with the approach set out under DORA[2].**

In addition, the current wording of the field may create ambiguity. We therefore recommend rephrasing it as follows: **Date and time the data controller has initially detected a potential personal data breach and started the internal investigation**.

Field 49 - Reasons for late notification of the personal data breach: as mentioned in the introduction, owing to the extensive number of fields required by the template, controllers will have no other option than to submit pre-notifications or incomplete notifications in order to comply with the notification deadline.

Field 50 - How was the personal data breach discovered?: we would like to make the following observations regarding Field 50:

[2] Recital 31 of Delegated Regulation (EU) 2024/2690

- With a view to better aligning the terminology with Articles 33 and 34 GDPR, we recommend replacing the term "*communication*" with "*notification*";
- We would welcome clarification as to what is meant by the term "*external party*" in this context.

Field 52 - Date of notification by other party: We believe that referring to the "*date of information*" would be more appropriate in this context, considering that the "*date of notification*" refers to the notification to DPAs. At the same time, however, we note that this field substantially duplicates Field 48. In practice, information received from another party would trigger internal initial knowledge and assessment. **We therefore recommend removing Field 52 to avoid duplication and confusion.**

Field 53 - Further comments on timeline and additional information: we would like to make the following observations regarding Field 53:

- We question the relevance and appropriateness of including a "further comments" field in a template already composed of 100+ questions;
- In complex IT environments, precise timestamps may not be immediately available. The template should therefore expressly **allow approximate dates and times** and should not require detailed justification of such estimates at the initial notification stage;
- Clarification is also needed on the mandatory nature of the requirement; Field 53 states that the requirement applies where Field 41a applies. However, no Field 41a appears to exist in the template.

Field 55 – Nature of the personal data breach: We invite the EDPB to consider formatting this field as a multiple-choice question. A single data breach may fall within more than one category (e.g., both a) and c).

Field 56 – Type of confidentiality breach & Field 57 - Was the data unintelligible to anyone who was not authorised to access it or were individuals not identifiable?: Fields 56 and 57 do not appear to take into account cases where personal data was disclosed through physical documents. We consider it prudent to have them included, but as optional.

Field 57 - Was the data unintelligible to anyone who was not authorised to access it or were individuals not identifiable?: we would like to share the following reflections on Field 57:

- We note that the template refers interchangeably to "individuals" and "data subjects". We recommend aligning the terminology throughout the template to ensure greater consistency.
- We also recommend clarifying that this requirement only refers to "***affected*** *data subjects*".

Field 58 – Type of integrity breach: The multiple-choice options do not include the possibility of indicating that the information is "not possible to assess" or "to be determined". We recommend adding these response options to accommodate situations where the type of the integrity breach cannot (yet) be determined at the time of notification.

Field 59 – Type of availability breach: to align the response options with Field 58, we suggest adding the following entries: "Not possible to assess" and "To be determined".

Field 60 – Nature of the incident: we would like to make the following observations on Field 60:

- **Option e) Security vulnerability (likely) exploited (known CVE or zero day)**: We recommend clarifying the abbreviation "CVE";
- **Option j) E-waste (personal data still present on obsolete device)**: Does EDPB mean "*discarded devices*", as opposed to "*obsolete devices*"?;
- **Option n) Incorrect access permissions (e.g., cloud storage, shared folder)**: For greater clarity, we recommend inserting the word "***to***", so that the Option reads "*Incorrect access permissions (e.g., **to** cloud storage, shared folder)*". This more clearly indicates that the reference is to access to those resources.
- **Option p) Personal data deleted/destroyed**: we suggest clarifying that the personal data has been **"*wrongfully*"** deleted or destroyed;
- **Option q) Personal data displayed to wrong recipient**: we recommend replacing the term "displayed" with "disclosed";
- **Option r) Personal data sent by mistake (post/email)**: We recommend clarifying that this refers to the sending of personal data "*to the wrong recipient(s)*".
- We also **recommend including "human error" among the circumstances triggering a data breach**. This would cover, for example, situations where an employee inadvertently confuses clients with similar names and dates of birth.

Field 62 - Further description of the nature of the incident: this field should only be made mandatory where Option "y) Other" has been selected under Field 60. **We therefore recommend amending the requirement to read "*Yes, if 60y applies*"**.

We would also welcome **clarification regarding the related tooltip**, which states: also says the following: "*Please describe the nature of the breach (detection, awareness, cause, measures in place) shortly and provide on what facts **your decision** is grounded. If possible indicate the root cause of the incident*." **It is unclear which decision is being referred**.

Field 63 - Description of the systems, software, services, and infrastructures involved in the personal data breach and where they are located: requiring controllers to disclose details of all the systems, software, services, infrastructure involved in a breach is overly broad and may create additional security risks, administrative work and cause delays in reporting. For financial institutions operating complex, multi-layered IT environments, this field risks creating open-ended disclosure obligations that go beyond what is necessary for supervisory purposes and may expose sensitive security architecture. We also note that such information may constitute commercially sensitive information or trade secrets, and it is unclear how this level of technical detail would assist supervisory authorities at the initial notification stage (noting that this information may not even be readily available at the time of notification). We therefore **recommend that the scope of this field be limited to information that is strictly necessary and directly relevant to understanding the breach**. Where information on the affected

systems is considered necessary, controllers should be permitted to provide it at an appropriate level of abstraction, without disclosing detailed system architecture or security-sensitive technical information.

Field 65 – Categories of concerned data subjects: Option "d) Minors" falls under the broader category of Option "i) Vulnerable individuals". We therefore recommend that minors be explicitly included as an example under "Vulnerable individuals," rather than being listed as a separate category. More generally, the categories listed are not mutually exclusive, creating uncertainty as to which category should be selected where multiple categories may apply.

Field 66 - Further description of categories of concerned data subjects and additional data subjects: This field should not be mandatory unless the answer to Field 65 is "j) Additional concerned data subjects".

Field 67 - Data subjects concerned by the personal data breach & Field 68 - Number of data subjects concerned by the personal data breach: With a view to ensuring efficiency and avoiding multiplying related fields/queries, **we recommend combining Fields 67 and 68**. The combined field should include an option such as "cannot yet be determined" or "to be confirmed", and should clarify that the information may be updated as the investigation progresses. The same efficiency approach should be adopted throughout the document (for example, Fields 72 and 73).

Field 71 - Further description of breached data and additional data categories: it should be clarified that this refers to "*personal data*".

Field 72 - Personal data records concerned by the personal data breach: the information requested depends heavily on the type of data breach (e.g. documents or a structured dataset), making it difficult to provide a meaningful response within the current question and answer format. In addition, this field appears to overlap with Field 73.

Field 73 - Number of personal data records concerned by the personal data breach: it is unclear what is intended by this requirement, as the interpretation of the question may vary depending on the respondent at hand. For example, for the financial sector, it is unclear whether the expectation is for a financial entity to calculate the number of individual transactions affected in the event that a file containing transaction data is breached. In such contexts, it is difficult to provide meaningful estimates where financial transaction data is involved. The accompanying explanation does not provide sufficient guidance and **could give rise to a degree of interpretative uncertainty**. This could lead to divergent approaches by different controllers, with the consequent risk of inconsistencies in the notifications submitted to supervisory authorities and difficulties in ensuring a homogeneous application of the regulatory framework. Such an approach would also impose a considerable administrative burden on controllers. To promote a coherent and uniform application of the notification criteria, we recommend either of the following clarifications:

- **define the scope of the concept of "personal data records concerned by the personal data breach"; or, alternatively,**
- **assess whether the information relating to the categories of personal data and the number of affected data subjects is sufficient** to achieve the objectives pursued by the notification, thereby avoiding potential interpretative discrepancies between entities and competent authorities.

Field 74 - 3.5 Measures in place when the personal data breach occurred: This requirement is excessive and concerning, as it would force companies to document and submit their internal defensive measures (and potential failures) in a template, which may create additional risks if that notification data were to be hacked, leaked, or otherwise publicly disclosed. **We strongly urge the DPB to delete this section. Such information should only be disclosed to the supervisory authority in case of an investigation.**

If the section is retained, it should be expressly clarified that the list is non-exhaustive, does not establish a mandatory security baseline and does not imply that the absence of a listed measure constitutes a compliance deficiency. The relevance of individual measures must be assessed on a case-by-case basis, taking into account the nature and risks of the processing concerned.

Field 75 - Relevant measures in place when the personal data breach occurred:

- We consider the term "Relevant measures" to be overly broad and open to different interpretations; it is unclear whether the question is intended to capture an organisation's security measures at large or the particular protections applied to the personal data involved in the specific data breach.
- Consideration could be given to including common technical security measures, such as "network security (e.g., firewalls) and data loss prevention tools.

Field 76 - Further description of relevant measures in place when the personal data breach occurred: It is unclear why this field is mandatory and what specific information is expected to be provided.

Section 4 – Further information on the personal data breach

Field 79 - Likely consequences in case of breach of confidentiality: it is unclear why the consequences have to be separated according to the type of data breach. **We therefore recommending grouping the likely consequences in case of a data breach under one single field**.

Field 89 - Outcome of the risk assessment carried out by the controller: **Option c)** *The personal data breach is **unlikely to result in a risk** to the rights and freedoms of natural persons* **should be deleted**. Under Article 33 of the GDPR, personal data breaches that are unlikely to result in a risk to the rights and freedoms of natural persons do not need to be reported to the supervisory authority.

Field 90 - Further description of the risk assessment carried out by the data controller: we would like to share the following observations:

- This **requirement appears overly extensive and would entail a significant additional workload for each notification**. It is also potentially **duplicative**, as the impacts have already been addressed throughout the questionnaire.
- With regards to the requirement to "*describe the methodology used and the relevant factors you put into account*", it is unclear why a description of the methodology used is relevant or necessary for notification purposes. At the initial notification stage, a high-level and provisional assessment should be sufficient. We also note there is no harmonised methodology provided by the EDPB. While providing relevant factors may be appropriate, requiring a full explanation of the methodology appears unnecessary.

Overall, this requirement appears more akin to a supervisory audit than to a breach notification requirement. **We therefore suggest considering its deletion.**

Field 93 - 4.4 Measures taken (or proposed to be taken) to prevent similar personal data breach: This requirement is premature, as within the 72-hour notification window, it is not possible to meaningfully determine the measures to prevent reoccurrence of similar data breaches. By comparison, the CNIL template focuses only on measures already taken following the breach. In addition, as already mentioned in previous sections, this requirement is overly excessive as it obliges companies to document their updated internal defensive measures and post-incident actions in a standardised notification template; this could create additional security risks if that notification data were to be hacked, leaked, or otherwise publicly disclosed.

Section 5 – Communication to the data subjects

The template should more clearly distinguish between the notification to the supervisory authority under Article 33 GDPR and the separate assessment of whether communication to data subjects is required under Article 34 GDPR. **Controllers should not be required to reach or substantiate a final Article 34 assessment at the initial notification stage where the relevant facts are still being investigated**.

Further clarification would be particularly necessary in those cases where any of the exceptions set out in Article 34(3) GDPR apply. In particular, it would be appropriate to clarify whether, where exceptions (a)[3] and (b)[4] apply, the obligation to notify the supervisory authority would still be required and, consequently, the obligation to communicate the breach to the affected data subjects. In such cases, we would welcome greater precision as to whether the existence of those circumstances could exclude both the obligation to notify the supervisory authority (as per the proposed new wording of Article 33 GDPR proposed in the Digital Omnibus) and the obligation to communicate the breach to data subjects under the current Article 34 GDPR.

Field 97 - Has the personal data breach been communicated to data subjects?: We recommend including an option to select "*No, exemption in local GDPR implementation act applies*".

Field 100 - Further information about conditions referred to in article 34(3) of the GDPR that are met & Field 101 - Further description why the conditions referred to in article 34(3) of the GDPR that are met and the measures taken: the purpose of these fields is unclear, as they appear redundant in light of other sections of the template, in particular those relating to mitigation measures. It would also be advisable not to include references to the GDPR without providing sufficient context.

Field 102 - Number of data subjects informed: we suggest rephrasing this field, as data subjects may be informed of a data breach for different reasons. On the one hand, notification may be required to comply with regulatory obligations; on the other hand, organisations may choose to inform data subjects voluntarily, for example of the basis of transparency considerations, even when no regulatory obligation requires such disclosure.

---

[3] Article 34(3)(a): *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption*;
[4] Article 34(3)(b): *the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*

Field 106 - Content of the information provided to the data subjects: we question the rationale of this requirement.

Section 6 – Possible other issues

Field 109 - Has the incident been reported to the police/judicial authorities as a criminal offence?: Unless there is a specific reason to here use the term "*incident*", we suggest to instead use "*personal data breach*" in order to ensure consistency with the terminology used in the template.

Field 111 - Further information about notification to other authorities or bodies: clarification on the rationale for this field is welcome, particularly in light of our understanding that the template is intended to be sufficiently broad to enable reporting and centralisation of feedback across multiple regulatory frameworks.

Section 6.2 - Whether the personal data breach involves a cross-border processing: The cross-border notification section (fields 113-118) requires (approximate) per-country data subject counts for controllers with EEA-wide client bases. These figures are often unavailable within the initial 72-hour notification window, and the requirement risks incentivising speculation rather than accuracy. **We therefore recommend making approximate ranges acceptable and align the timing requirement with what is realistically achievable in an initial notification**.

Field 115 - List of EEA countries where the controller has an establishment: in our view, this entry is not relevant in case of a data breach. **We recommend deleting this Field and instead stick to Field 116**, which is more relevant and appropriate.

Section 7 – Attachments

We would like to raise **significant concerns regarding Section 7 – Attachments**. Supporting internal documentation, including risk assessment and policies, are retained by controllers as part of their accountability obligations. Such documents may be requested at a later stage by a supervisory authority where necessary if it requires additional information or decides to investigate the incident. Proactively submitting this information does not appear necessary and could result in unnecessary disclosure of internal assessment and governance material beyond the scope of the notification requirements under Article 33 GDPR. **Attachments should therefore be voluntary unless specifically requested by the competent supervisory authority**, without prejudice to applicable legal privilege and confidentiality restrictions.

In particular, the requirement to submit a copy of the research report into the data breach (cyberincidents) is alarming, as it may contain confidential security information, details of vulnerabilities, banking security architecture, information subject to legal privilege, information affecting forensic investigation, etc. Disclosure of such information might lead to exposure of sensitive security-related details, increase operational and cybersecurity risks, prejudice ongoing investigations, and potentially undermine the effectiveness of remedial measures.

The level of detail requested should be limited to information necessary to understand the incidents and its impact and do not pose additional risks and concerns for the controller, in line with Article 5 and 25 GDPR. We therefore **recommend limiting the submission to the information expressly required by Article 33 GDPR. Any additional documentation should only be provided where**

there is a specific request from the supervisory, where justified in the context of a specific investigation, which should preferably be conducted at the controller's premises.

Additional EBF Recommendations

- We **recommend introducing a dedicated field allowing controllers to indicate that specific information cannot be provided due to a legal prohibition under national or EU law**, with a reference to the applicable legal basis. For financial institutions, this is particularly relevant where disclosure of breach details, such as the nature of the incident, the systems involved, or the remediation measures taken, would constitute a tipping-off offence under Article 39 of the Anti-Money Laundering Directive or its national transpositions.
- We would also welcome if the EDPB could supplement the template with a risk assessment methodology to help controllers determine, in an objective and consistent manner, when a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects. This would provide greater legal certainty to the risk assessment process and promote a more uniform interpretation of the regulatory framework. While we note that the Digital Omnibus proposal envisages whitelists for personal data breaches, such lists alone may not capture the full range of scenarios encountered in practice[5]. A complementary risk assessment methodology would therefore allow controllers to assess, in a consistent manner, the risk factors present in each personal data breach.

ENDS

[5] Personal data breaches may give rise to a wide variety of factual situations that do not always fit neatly within predefined scenarios. As a result, different controllers could still reach different conclusions when assessing similar incidents.

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