L'Afep

Paris, July 24th 2026

POSITION PAPER

EDPB template for personal data breach notification

L'Afep supports the EDPB's intention to propose to controllers a template for personal data breach notification.

French large companies note that, the preparation of this template is not foreseen in the current version of Article 33 of the General Data Protection Regulation (GDPR), and proposed by the European Commission in its draft Digital Omnibus currently under analysis, review and discussions by the colegislators. **L'Afep warmly welcomes and supports the idea to prepare a common template and a common methodology for conducting personal data breach notification**.

This will contribute to a **better harmonization of the GDPR implementation within the internal market as well as simplifying the requirements on companies**. The development of a regulatory framework that is as simple, clear and consistent as possible must be a strategic objective of the EU and its institutions in order to ensure optimal economic development for its citizens and businesses.

Therefore, L'Afep encourages the EDPB to adopt the most ambitious approach possible in terms of simplification, rationalization pragmatism, and coordination of the application of article 33.

Furthermore, **it is essential that national authorities**, in line with the commitment made by the EDPB and the national authorities in their Helsinki Declaration of 2 July 2025, **refrain from adopting additional measures at national level** that would complicate the European regulatory framework and undermine the harmonisation of the internal market that this model rightly seeks to achieve.

French large companies point out that a personal data breach notification often occurs in **a crisis situation** in which the data controller is fully engaged with other public bodies, notably the national cyber defence authority, to contain the spread of the crisis and minimise its adverse effects on citizens, businesses and society as a whole.

The primary aim of developing such a model must therefore not be to create new regulations, obligations, standards or cumbersome forms that are out of touch with reality, but rather **to simplify crisis management by data controllers, whilst ensuring full transparency and cooperation with the competent authorities**.

If it does not pursue that aim, **the proposed model risks missing the point of the exercise and remaining a purely theoretical exercise**.

On the template itself, French large companies note, as a preliminary point, that **this draft template goes much further and requires far more information** – which is neither required by Article 33 of the GDPR nor necessary – than is currently required by the CNIL and other national data protection authorities. They therefore identify a risk that the EDPB may distort the meaning of Article 33 of the GDPR by treating the notification of personal data breaches as a much broader tool than envisaged by the regulation, particularly with regard to the analysis of the breach, the assessment of its impact, the action plan and, consequently, its very purpose.

Above all, the EDPB appears to be disregarding Article 33(1) of the GDPR, which requires the data controller to make this declaration within 72 hours after becoming aware of the breach. However, **the template proposed by the EDPB is 27 pages long and contains 126 lines to be completed, of which only 10 (8%) are not mandatory…** It is unrealistic to expect data controllers to complete such a long and detailed form within such a short timeframe and in the midst of a cyber crisis. By way of comparison, a data breach notification form submitted to the CNIL, once completed, is on average 8 pages long. Under these circumstances, **the template proposed by the EDPB therefore appears to be out of touch with the reality of business life and the practical management of cyber crises**.

By adopting such an approach, **the EDPB appears to be moving – once again – towards a maximalist interpretation of the GDPR, contrary to the Helsinki Declaration, and is even acting as a legislator in place of the EU's co-legislators**. At a time when industry is struggling with regulatory complexity and administrative burdens, it is not reasonable for the EDPB to work towards increasing the length of time to report a breach, without clearly explaining how this would better protect individuals.

This proposed model therefore still needs to be simplified considerably to focus on the information required by Article 33 of the GDPR and necessary for the handling of the personal data breach. As a reminder, Article 33(3) of the GDPR only contains four notification requirements. **French large companies have identified at least 31 lines of information not required by Article 33 of the GDPR and which could therefore be removed from this notification template, as well as several lines that could be merged to simplify the notification procedure**.

French large companies are also considering the proposed future conditions for using this template, in particular whether a single notification portal would be set up at European level under the auspices of the EDPB, which would then forward the notifications to the relevant authorities.

In these circumstances, **French large companies are encouraging the EDPB to adopt a communication accompanying this template, setting out the conditions for its use across the EU**. The aim of this communication would, of course, be to streamline the notification of personal data breaches by data controllers, so as to enable them, in cooperation with all the relevant authorities, to focus on resolving the incident in question and mitigating the risks involved, rather than on administrative tasks.

In order to further the objective of harmonising and simplifying the implementation of the GDPR within the internal market, once adopted by the EDPB, this single template should allow for a single notification to be made, ideally at European level, or to a single national authority for both domestic and cross-border incidents, so as to reduce the administrative burden on businesses operating in a federal state or across different Member States (one stop shop). Furthermore, groups must be able to appoint a single entity to make these notifications on behalf of all group companies across the EU. Similarly, all national data protection authorities must allow notifications to be made via their websites in English in order to genuinely make life easier for data controllers.

Lastly, French large companies would like to stress that one of the best way so simplify data breach reporting is to clarify when such reporting is genuinely needed to avoid that companies report all of their security incidents to the data protection authorities "just in case". Having a clear and harmonised interpretation of the situations where "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" would enable companies to perform a preliminary triage and focus on notifying the most impactful breaches for individuals only.

1 - Section 1 – Information on the personal data breach notification

In cases where previous notifications need to be amended or supplemented (**line 6**), French large companies note that only the identification number of the previous notification is required. **L'Afep encourages the data protection authorities to plan for and implement a secure system to access the file relating to the previous notification**. Indeed, the information provided to data protection authorities is sensitive and must be subject to appropriate safeguards to ensure that it cannot be accessed solely on the basis of an identification number.

Furthermore, they point out that the internal reference number for the incident (**line 7**) is not information required under Article 33 of the GDPR, and is not necessary for the data protection authorities. **They therefore call on the EDPB to remove this line**.

2 - Section 2 – Identification of the data controller and the reporting person

With regard to **lines 10 to 19**, French large companies are encouraging data protection authorities to introduce a mechanism for automatically populating this information – this mechanism is already widely used by French public institutions – based on the data controller's identification number, VAT number, etc.

Lines 14, 15, 16 and 17 are not required by Article 33 of the GDPR and are not necessary for

the management of the incident. **They therefore call on the EDPB to remove them from the proposed template**.

With regard to information about the person reporting the incident, L'Afep notes that the notification obligation set out in Article 33 of the GDPR rests with the data controller, not with their DPO; therefore, it is the data controller's representative, not their DPO, who should be the first option offered by the template (**line 23**).

French large companies see no added value in the information requested in **lines 24, 25 and 26**, which are not provided for in Article 33 of the GDPR either, and which complicate the proposed form, and may even pose a risk of information being disclosed by the authorities that are supposed to protect it (in particular information on individual identity cards). Once again, **they urge the EDPB to remove these lines**.

With specific regard to the DPO (**line 29**), L'Afep invites the EDPB to clarify which DPO should be specified here for international groups, which may have a single global DPO for the group, DPOs for certain countries, or data protection officers for other countries.

3 - Section 3 – Initial information on the personal data breach

Regarding the date on which the data breach occurred, French large companies welcome the option to state that the date cannot yet be determined, or to provide a timeframe or an estimated date (**lines 44 to 47**). This flexibility is important for data controllers in the context of crisis management, which is often the situation when personal data breaches occur. L'Afep also notes that **lines 46 and 47 could be merged for the purpose of simplification**.

Line 53 requires the disclosure of the date on which the data processor became aware of the data breach. This requirement goes beyond article 33(2) of the GDPR which only requires data processors to notify data controllers without undue delay. It does not require data processors to disclose the precise date when they became aware of the data breach. L'Afep recommends therefore to remove this requirement.

Lines 55 to 59 list various categories of personal data breaches; however, in principle, **the definition of personal data breach set out in Article 4 of the GDPR makes it clear that such breaches must result from a security breach**. By omitting this clarification, this section of the model risks broadening the scope of notifications to include, for example, mere service outages which do not, however, result from a security breach. This point would therefore benefit from further clarification in order **to avoid a broad interpretation of the obligations of data controllers by data protection authorities**.

Line 63 requires the mandatory provision of extensive details about their internal security procedures and vulnerabilities such as access controls, encryption protocols, and auditing histories. The disclosure of such technical data can be very burdensome depending on the specific case. Moreover, some of this information may contain cyber-sensitive elements or trade secrets. Compelling companies to document their internal defensive measures (or failures) in a standard template creates additional confidentiality risks in case of leakage, unauthorized access, or if it is publicly disclosed.

Above all, French large companies note that the whole of sub-section 3.5 is not provided for in Article 33 of the GDPR (**lines 74 to 76**). In these circumstances, they do not see why this information should be provided to data protection authorities as part of a data breach notification, even on an optional basis. **They point out that the purpose of a data breach notification is not to conduct an audit of the security measures in place prior to the incident, and therefore urge the EDPB to simply remove these provisions**.

4 - Section 4 – Further information on the personal data breach

With regard to the likely consequences of a personal data breach, French large companies note that **lines 79 to 84 could be merged** in order to facilitate notification by the data controller. Above all, in most cases, the answers to these various lines will be identical. They therefore point out that, given the purpose and context in which these notifications will be made, they must be as simple and quick as possible for data controllers to complete.

Line 87 requires organizations to classify the severity of the potential impacts: minor, moderate, severe, or to be determined. There is however, no common EDPB standard for assessing the severity of the impact on individuals. Such assessment tends to be largely subjective and will produce huge variations in how organizations categorize the impact of the breach. To solve this issue, L'Afep recommends the EDPB to explicitly refer to the ENISA recommendations for a methodology of the assessment of severity of personal data breaches.

French large companies are surprised to see the inclusion in this draft template for **lines 88, 89 and 90**, which are **not provided for in Article 33 of the GDPR but in Article 34**, which does not apply to notifications of personal data breaches. This information is therefore not required by the regulation, is not necessary for dealing with the reported breach, and unnecessarily complicates the crisis management process for data controllers. **They therefore call on the EDPB to remove them from its proposed notification template**.

Similarly, **lines 93, 94 and 95 are not provided for in Article 33 of the GDPR**. They are undeniably useful and necessary, but are not required by the regulation, are not necessary for the handling of the reported breach, and unnecessarily complicate the crisis management process for data controllers, who have only 72 hours to submit their notification. Thus **L'Afep encourages the EDPB to remove them from its proposed notification template**.

5 - Section 5 – Communication to the data subjects

Firstly, French large organisations wish to point out that the notification of a personal data breach to the data subject is not provided for in Article 33 of the GDPR, which concerns

notification to the supervisory authority, but in Article 34 of the GDPR, which specifically concerns notification to the data subject. Furthermore, such an obligation to inform exists only where there is a high risk to the rights and freedoms of individuals, and is therefore not automatic.

They therefore draw the EDPB's attention to the fact that **all the information requested by the EDPB in lines 96, 97, 98, 99, 100, 101, 102, 103, 104, 105 and 106** (i.e. 11 lines in total) **is not required by the GDPR in the context of notification to the supervisory authority**.

Once again, in the context of cyber crisis management, it is unlikely that the data controller would have been able, within the strict 72-hour time limit laid down in Article 33 of the GDPR, to carry out the exercise provided for in Article 34 of the GDPR. Whilst a preliminary analysis may, in certain circumstances, be carried out, **it is unreasonable to require a data controller to provide all of this information** – which is not mandatory – within 72 hours of a breach. **L'Afep therefore requests the removal of lines 96 to 106**. At the very least, the provision of this information should not be compulsory.

6 - Section 7 – Attachements

French large companies are surprised by the volume of documents the EDPB requires them to provide alongside their notification of a personal data breach.

Firstly, some of these documents are not mentioned in Article 33 of the GDPR, such as a dated copy of the internal notification procedure or a dated copy of the risk assessment, etc. Furthermore, certain documents, such as the notification to data subjects, will not yet be available within the 72-hour timeframe set out in the GDPR for the notification to the supervisory authority alone. Finally, others are simply not applicable to all cases of personal data breaches. Consequently, **L'Afep suggests deleting lines 124, 125 and 126 from this template**, as they are not required by the GDPR and may not necessarily be applicable or available at the time of notification. If it proves necessary to provide certain additional information, this may be done at a later date, following notification of the breach to the supervisory authority.

Apart from the validity of these requests for information, the websites of the relevant authorities will also need to be able to accommodate documents in a variety of digital formats, which is often not the case at present.

About L'Afep

Founded in 1982, L'Afep brings together 117 of the largest French companies, which represent 15% of France's commercial GDP, employ 13% of the private sector workforce, and account for 20% of the mandatory corporate contributions in France. L'Afep member companies employ 8.5 million people and are key players in the French, European, and global economies across all sectors of activity. Among the 60 largest European companies, a third is a member of L'AFEP.

Its mission is to contribute to the creation of an environment conducive to the development of economic activity and to make the voice of large French companies heard by policymakers in Paris and Brussels. They are fully committed to the green and digital transition, innovation, and the pursuit of better governance.

L'Afep is involved in drafting cross-sectoral legislation, at French and European level, in the following areas: economy, taxation, company law and corporate governance, corporate finance and financial markets, competition, intellectual property, digital and consumer affairs, labour law and social protection, environment and energy, corporate social responsibility and trade.

Transparency Register ide: 953933297-85