Public consultation on EDPB - Template [2026] for personal data breach notification, Version 1.0, Adopted on 08 June 2026

Bruno RASLE's contribution – Former DPO for a branch of the French Social security, Former Chief Executive Officer of the French DPO Association (AFCDP), DPO trainer since 2006

France, 28th june 2026

The initiative is to be commended and is welcomed.

Whilst it has several positive aspects (compared with current practice in France) and pursues relevant objectives (ensuring that the notification contains all the information required under Article 33 of the GDPR in order to facilitate the supervisory authority's assessment of each situation; standardise practices across Europe), I would like to make a few suggestions to broaden the scope of this unified data breach notification template, with a view to strengthening the role of DPOs and supporting their efforts within the organisations that have appointed them (my proposals specifically aimed at this objective are in bold).

Compared with the procedure currently proposed by the CNIL, I note the following improvements:

- Among the types of notification (point 4), the addition of the withdrawal of a previously submitted notification (and the reasons for this withdrawal in point 5);
- The option to provide an estimate of the number of individuals affected by the breach (whereas the CNIL's online service requires an exact figure to be entered) in point 68;
- In point 63, the addition of a description of the resources and infrastructure involved in the data breach (point 63);
- In point 109, the addition of information regarding the possible lodging of a complaint (in France, a recent provision stipulates that an organisation which has taken out insurance against cyber-attacks is not covered if it has not lodged a complaint within 72 hours, which reinforces the synergy with the provisions of Article 33 of the GDPR).
- Point 7 provides the option to specify the internal reference number of the notified data breach. However, under Article 33(5) of the GDPR, records must be kept. The CNIL has specified that this documentation must be structured (it uses the term 'register'), which effectively implies a reference system. **In that case, why not make the provision of this information mandatory to help DPOs ensure that data breaches are (at last) documented internally?**

However, in my view, the following improvements are lacking:

- Given the low number of PIA assessments carried out and the generally poor quality of those that have been conducted, in paragraph 89 (Outcome of the risk assessment carried out by the controller), in the case of response (a) ("The personal data breach is likely to result in a high risk to the rights and freedoms of natural persons"), **it should be mandatory to provide the PIA that must (or should have) been formalised** (and not optional, as stated in point 125 ("b) Dated copy of the risk assessment")). **Furthermore, the term 'Impact Assessment' should replace the term 'Risk Assessment'**. This would be consistent with point 76 ('Further description of relevant measures in place when the personal data breach occurred'), which requires a detailed response;

- It would be useful to ask whether a similar data breach (of the same scope, involving the same processing, under the same circumstances) has already occurred in the last 24 months but did not require notification (as the level of risk did not warrant it at the time);
- In section 6.1 ('Whether other authorities or bodies have been notified'), it would be useful to ask whether this breach has resulted (or will result) in another notification to a different authority under a framework other than the GDPR? And if so, which framework and which authority?
- **It would be useful to ask whether this breach has led (or is likely to lead) to a formal lessons-learnt exercise,** particularly to align with practice within the NIS2 scope, as DPOs are finding it difficult to ensure that a thorough review is carried out following incidents to prevent the breach from recurring.