LA POSTE GROUPE

Position Paper of La Poste Groupe on the EDPB Template for Personal Data Breach Notification

English Version followed by French version.

Executive Summary

La Poste Groupe fully supports the EDPB's objective of further harmonising personal data breach notifications across the European Union.

A common notification template is a welcome initiative that can help promote greater consistency among supervisory authorities and enhance legal certainty for organisations operating across multiple Member States.

However, several aspects of the proposed template would benefit from further clarification or adjustment to ensure its alignment with Article 33 GDPR, its compatibility with the 72-hour notification deadline, and its practical applicability in the context of incident management.

In particular, the template appears, in certain instances, to require at the initial notification stage detailed information that is not expressly required under Article 33 GDPR and that may not be available during the early stages of an incident. This approach could increase the administrative burden on organisations, complicate the submission of timely notifications and, in practice, create de facto reporting expectations extending beyond the requirements expressly established by Article 33 GDPR.

La Poste Groupe therefore encourages the EDPB to:

- more clearly distinguish information required under Article 33 GDPR from information that may be provided on a supplementary basis;

- adopt a more modular approach, differentiating between information necessary for the initial notification and information that may be provided subsequently as investigations progress;
- clarify the purpose and status of certain highly detailed sections in order to preserve the distinction between the notification of a personal data breach and its subsequent assessment;
- provide further guidance on the circumstances in which a previously submitted notification may be withdrawn;
- maintain a degree of flexibility allowing supervisory authorities to take into account national administrative specificities where appropriate.

Such an approach would strengthen legal certainty, ensure the proportionality of reporting obligations and preserve the primary purpose of the notification mechanism established by the GDPR: enabling supervisory authorities to receive timely and relevant information on personal data breaches in order to assess their risks and potential consequences.

La Poste Groupe welcomes initiatives aimed at improving consistency and legal certainty in the application of the GDPR across the European Union. As a major provider of postal, logistics, banking, insurance and digital services, operating through multiple entities and serving millions of users, La Poste Groupe strongly supports efforts to facilitate a more harmonised approach by supervisory authorities, particularly in areas where organisations may interact with several authorities across different Member States.

From this perspective, a common breach notification template has the potential to simplify compliance efforts and improve predictability for organisations. However, we believe that several aspects of the proposed template could benefit from further clarification and adjustment to ensure that it remains aligned with the GDPR framework and operationally compatible within the notification deadlines established by Article 33 GDPR.

1. Alignment with Article 33 GDPR

The objective of harmonisation is welcome. However, several sections of the draft template appear to require information that goes significantly beyond the elements expressly listed in Article 33(3) GDPR.

For example, section 63 requests a detailed description of the systems, software, services and infrastructures involved in the breach and their location. Similarly, section 90 requires a further description of the risk assessment methodology used by the controller and the factors taken into account.

While such information may be useful to supervisory authorities in certain situations, it is not explicitly required by Article 33 GDPR for the purposes of a breach notification. While the objective of harmonisation is welcome, it would be helpful to clarify the status of these additional fields and whether they are intended to be optional, recommended or expected as part of a complete notification. Without such clarification, there is a risk that information requests contained in the template may be perceived in practice as creating de facto reporting expectations beyond those expressly established by the GDPR.

Such clarification is particularly important as the absence of information requested by the

template, but not expressly required under Article 33 GDPR, could be perceived as affecting the completeness of a notification. It is therefore essential to maintain a clear distinction between GDPR requirements and additional information that may be requested for harmonisation purposes.

To mitigate this risk and strengthen legal certainty, the template could more clearly distinguish between information required under Article 33 GDPR and information that may be provided on a voluntary basis or at a later stage where appropriate.

Additional clarification on the status of these fields would help ensure consistent implementation across the Union and avoid creating de facto expectations that go beyond the legal requirements established by the GDPR.

2. Compatibility with the 72-hour notification deadline

The GDPR establishes a notification deadline of 72 hours after becoming aware of a personal data breach. The effectiveness of this framework relies on a balance between timely reporting and the progressive availability of information as investigations develop.

Several sections of the proposed template, including points 39, 55, 57, 60, 63, 72, 90, 94 and 125, may require information that is often not available during the initial stages of incident response.

Although each individual request may appear reasonable, their cumulative effect could significantly increase the administrative burden associated with the preparation of an initial notification. In some cases, organisations may be required to devote substantial resources to completing the reporting exercise while technical investigations and remediation activities are still ongoing.

While the draft aims to promote greater harmonisation and efficiency in breach notification procedures, the level of detail required may, in practice, increase the administrative burden on organisations and reduce some of the expected benefits of such harmonisation.

As a result, the proposed level of detail may reduce the practical usability of the template within the 72-hour period and could unintentionally undermine the objective of facilitating timely notifications.

We therefore encourage the EDPB to consider a more modular approach, distinguishing between:

- Information required for the initial notification;
- Optional information that may, for example, be provided through subsequent updates as investigations progress.

Such an approach would remain fully consistent with the phased notification logic already reflected in Article 33 GDPR.

3. Purpose and use of highly detailed information requests

Certain sections of the template appear closer to a detailed incident assessment report than to an initial personal data breach notification.

Greater clarity regarding the purpose and subsequent use of the information requested would also help strengthen confidence in the notification process and ensure that it

remains a mechanism for the prompt reporting of personal data breaches rather than evolving into an exercise comparable to a comprehensive compliance assessment.

While supervisory authorities legitimately require sufficient information to assess a personal data breach, the EDPB could consider treating certain highly detailed information as optional—provided that such information is not required under Article 33 GDPR—and, where appropriate, request it at a later stage of the investigative process. Maintaining a clear distinction between the notification phase and the subsequent assessment carried out by the supervisory authority would enhance legal certainty and encourage controllers to submit timely notifications.

Greater clarity regarding the intended use of such information would help organisations provide relevant and proportionate information during the early stages of incident management while avoiding unnecessary reporting burdens.

In this respect, the template should ensure that the notification process remains focused on its primary objective: enabling supervisory authorities to understand the nature of the breach, its potential impact on data subjects, and the measures taken or envisaged by the controller to mitigate its effects.

4. Withdrawal of previously submitted notifications (section 4 of the template)

The possibility, provided for in Section 4 of the template, to withdraw a previously submitted notification would benefit from further clarification. In particular, additional guidance would be welcome regarding the circumstances in which organisations are expected to submit an initial notification and subsequently withdraw it.

The existence of this mechanism raises questions regarding its interaction with the obligation to notify a personal data breach within 72 hours where the breach is likely to result in a risk to the rights and freedoms of natural persons. Clarification would be particularly welcome on situations where a notification may initially be submitted and subsequently withdrawn in light of information obtained during the course of the investigation.

Without such clarification, this mechanism may create uncertainty as to the appropriate threshold for notification and could encourage some organisations to adopt an overly cautious approach by notifying incidents even where the need for notification has not yet been established.

The template should seek to avoid creating such uncertainty, particularly where investigations are still ongoing and the factual circumstances of the incident continue to evolve. Additional guidance on the intended purpose of this mechanism would contribute to a more consistent application of the notification obligation.

5. Need for flexibility at national level

Finally, some elements included in section 2 (“Identification of the data controller and the person submitting the notification") may not fully reflect specific national administrative practices, particularly in the French context.

While harmonisation remains an important objective, a degree of flexibility should be preserved to allow supervisory authorities to adapt certain practical aspects of the template to their national context where necessary.

Conclusion

La Poste Groupe strongly supports the objective of greater consistency in personal data breach notifications across the European Union. However, achieving this objective requires a framework that remains closely aligned with Article 33 GDPR, proportionate to the 72-hour notification deadline and sufficiently flexible to accommodate the practical realities of incident response.

While the objective of harmonisation is strongly supported, the template should avoid unintentionally increasing reporting obligations beyond those necessary to fulfil the objectives of Article 33 GDPR. A proportionate and risk-based approach remains essential to ensure that breach notifications can be submitted rapidly, consistently and effectively throughout the Union.

We therefore invite the EDPB to simplify certain information requirements, clarify the status of supplementary sections, and reinforce the distinction between information required for the initial notification and information that is optional and may, where appropriate, be provided subsequently as investigations progress.

Position du Groupe La Poste sur le modèle de notification de violation de données à caractère personnel du CEPD

Version française

EN RÉSUMÉ

Le Groupe La Poste soutient pleinement l'objectif du CEPD visant à renforcer l'harmonisation des notifications de violations de données personnelles au sein de l'Union européenne. Un modèle commun de notification constitue une initiative bienvenue pour favoriser la cohérence des pratiques des autorités de contrôle et renforcer la sécurité juridique des organisations opérant dans plusieurs États membres.

Toutefois, plusieurs aspects du projet de modèle mériteraient d'être clarifiés ou ajustés afin de garantir son alignement avec l'article 33 du RGPD, sa compatibilité avec le délai légal de notification de 72 heures et sa prise en compte des réalités opérationnelles de la gestion des incidents.

En particulier, le modèle semble, dans certains cas, exiger dès la notification initiale des informations détaillées qui ne sont pas expressément prévues par l'article 33 du RGPD et qui peuvent ne pas être disponibles dans les premières phases d'un incident. Cette approche pourrait accroître la charge administrative des organisations, compliquer la réalisation de notifications rapides et créer, dans la pratique, des attentes déclaratives allant au-delà des exigences prévues par le RGPD.

Le Groupe La Poste encourage dès lors le CEPD à :

- Distinguer plus clairement les informations requises au titre de l'article 33 du RGPD de celles pouvant être fournies à titre complémentaire ;

- Adopter une approche plus modulaire distinguant les informations nécessaires à la notification initiale des informations susceptibles d'être communiquées ultérieurement à mesure que les investigations progressent ;
- Clarifier la finalité et le statut de certaines rubriques particulièrement détaillées afin de préserver la distinction entre la notification d'une violation et son évaluation ultérieure par l'autorité de contrôle ;
- Préciser les conditions d'utilisation du mécanisme de retrait d'une notification ;
- Maintenir une certaine flexibilité permettant la prise en compte de spécificités administratives nationales lorsque cela est nécessaire.

Une telle approche contribuerait à renforcer la sécurité juridique, à garantir la proportionnalité des obligations déclaratives et à préserver l'objectif premier du mécanisme de notification prévu par le RGPD : permettre aux autorités de contrôle de recevoir rapidement des informations pertinentes sur une violation de données personnelles afin d'en apprécier les risques et les conséquences potentielles.

Le Groupe La Poste salue les initiatives visant à renforcer la cohérence et la sécurité juridique dans l'application du RGPD au sein de l'Union européenne. En tant qu'acteur majeur des services postaux, logistiques, bancaires, assurantiels et numériques, opérant à travers plusieurs entités et servant des millions d'utilisateurs, le Groupe La Poste est particulièrement favorable aux démarches permettant une approche plus harmonisée des autorités de contrôle, notamment pour les organisations susceptibles d'interagir avec plusieurs autorités dans différents États membres.

Dans cette perspective, un modèle commun de notification des violations de données personnelles pourrait contribuer à simplifier les démarches de conformité et à améliorer la prévisibilité pour les organisations. Toutefois, plusieurs aspects du modèle proposé mériteraient, selon nous, d'être clarifiés ou ajustés afin de garantir sa conformité avec le cadre du RGPD et sa compatibilité avec les contraintes opérationnelles liées au délai de notification prévu à l'article 33 du RGPD.

1. Alignement avec l'article 33 du RGPD

L'objectif d'harmonisation est bienvenu. Toutefois, plusieurs sections du projet de modèle semblent exiger des informations qui vont significativement au-delà des éléments expressément prévus à l'article 33, paragraphe 3, du RGPD.

Par exemple, le point 63 demande une description détaillée des systèmes, logiciels, services et infrastructures impliqués dans la violation ainsi que de leur localisation. De même, le point 90 demande une description complémentaire de la méthodologie d'évaluation des risques utilisée par le responsable du traitement et des facteurs pris en compte.

Si ces informations peuvent présenter un intérêt pour les autorités de contrôle dans certaines situations, elles ne sont pas explicitement exigées par l'article 33 du RGPD dans le cadre d'une notification de violation de données personnelles.

Si l'objectif d'harmonisation est bienvenu, il serait utile de clarifier le statut de ces champs supplémentaires et de préciser s'ils sont facultatifs, recommandés ou attendus dans le cadre d'une notification complète. À défaut, il existe un risque que certaines demandes figurant dans le modèle soient perçues, dans la pratique, comme créant des attentes

déclaratives de facto allant au-delà des exigences expressément prévues par le RGPD.

Une telle clarification est d'autant plus importante que l'absence d'informations demandées par le modèle, mais non expressément prévues par l'article 33 du RGPD, pourrait être perçue comme affectant le caractère complet d'une notification. Il est donc essentiel de préserver une distinction claire entre les exigences prévues par le RGPD et les informations complémentaires susceptibles d'être demandées dans un objectif d'harmonisation.

Afin de limiter ce risque et de renforcer la sécurité juridique, le modèle pourrait distinguer plus clairement les informations requises au titre de l'article 33 du RGPD de celles pouvant être fournies à titre complémentaire ou à un stade ultérieur lorsque cela est pertinent.

Une clarification du statut de ces rubriques contribuerait à une mise en œuvre plus cohérente au sein de l'Union et permettrait d'éviter la création d'attentes de facto dépassant les exigences prévues par le RGPD.

2. Compatibilité avec le délai de notification de 72 heures

Le RGPD prévoit un délai de notification de 72 heures à compter de la prise de connaissance d'une violation de données personnelles. L'efficacité de ce mécanisme repose sur un équilibre entre la nécessité d'une notification rapide et la disponibilité progressive des informations à mesure que les investigations avancent.

Plusieurs sections du modèle proposé, notamment les points 39, 55, 57, 60, 63, 72, 90, 94 et 125, semblent requérir des informations qui ne sont pas toujours disponibles dans les premières phases de gestion d'un incident.

Si chacune de ces demandes peut paraître justifiée prise isolément, leur accumulation risque d'accroître substantiellement la charge administrative liée à la préparation de la notification initiale. Dans certains cas, les organisations pourraient être amenées à consacrer des ressources importantes au renseignement du formulaire alors même que les investigations techniques et les actions de remédiation sont encore en cours.

Alors que le projet vise à favoriser l'harmonisation et l'efficacité des notifications, le niveau de détail demandé pourrait, dans la pratique, accroître la charge administrative pesant sur les organisations et réduire les bénéfices attendus de cette harmonisation.

Le niveau de détail requis pourrait ainsi réduire la facilité d'utilisation du modèle dans le délai de 72 heures et, de manière paradoxale, compromettre l'objectif poursuivi de faciliter des notifications rapides et efficaces.

Nous encourageons donc le CEPD à envisager une approche plus modulaire distinguant :

- Les informations obligatoires et nécessaires à la notification initiale ;
- Les informations facultatives qui pourraient, par exemple, être transmises dans le cadre de mises à jour ultérieures, à mesure que l'enquête progresse.

Une telle approche serait pleinement conforme à la logique progressive de notification déjà prévue par l'article 33 du RGPD.

3. Finalité et utilisation des demandes d'informations très détaillées

Certaines sections du modèle apparaissent davantage comme un rapport détaillé d'analyse d'incident que comme une notification initiale de violation de données.

Une plus grande clarté quant à la finalité et à l'utilisation ultérieure des informations demandées contribuerait également à renforcer la confiance dans le mécanisme de notification et à garantir que celui-ci demeure un outil de signalement rapide des violations plutôt qu'un exercice assimilable à une évaluation complète de conformité.

Si les autorités de contrôle ont légitimement besoin d'informations suffisantes pour apprécier une violation, le CEPD pourrait envisager que certaines informations particulièrement détaillées ne soient que facultatives – dès lors qu'elles ne sont pas exigées par l'article 33 du RGPD – et, le cas échéant, sollicitées à un stade ultérieur du processus d'investigation. Le maintien d'une distinction claire entre la notification et l'évaluation ultérieure réalisée par l'autorité contribuerait à la sécurité juridique et favoriserait des notifications rapides de la part des responsables de traitement.

Une plus grande clarté quant à l'usage attendu de ces informations aiderait les organisations à fournir des informations pertinentes et proportionnées dans les premiers stades de gestion d'un incident tout en évitant une charge déclarative excessive.

À cet égard, le modèle devrait veiller à ce que le processus de notification demeure centré sur son objectif premier : permettre à l'autorité de contrôle de comprendre la nature de la violation, ses conséquences potentielles pour les personnes concernées ainsi que les mesures prises ou envisagées par le responsable du traitement afin d'en limiter les effets.

4. Retrait d'une notification précédemment soumise (point 4 du modèle)

La possibilité, prévue au point 4 du modèle, de retirer une notification précédemment soumise mériterait d'être davantage explicitée. En particulier, des clarifications seraient utiles quant aux situations dans lesquelles les organisations sont censées procéder à une notification initiale avant de la retirer ultérieurement.

L'existence de ce mécanisme soulève des interrogations quant à son articulation avec l'obligation de notifier une violation de données personnelles dans les 72 heures lorsqu'elle est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. Des précisions seraient notamment bienvenues sur les situations dans lesquelles une notification pourrait être effectuée puis retirée à la lumière d'éléments obtenus au cours de l'enquête.

À défaut, ce mécanisme pourrait créer une incertitude quant au seuil approprié de notification et inciter certaines organisations à adopter une approche excessivement prudente en notifiant des incidents alors même que la nécessité d'une notification n'est pas encore établie.

Le modèle devrait éviter de créer une telle incertitude, notamment lorsque les investigations sont encore en cours et que les circonstances de l'incident continuent d'évoluer. Des orientations complémentaires sur l'objectif poursuivi par ce mécanisme contribueraient à une application plus cohérente de l'obligation de notification.

5. Nécessité de préserver une certaine flexibilité au niveau national

Enfin, certains éléments figurant dans la section 2 (« Identification du responsable du traitement et de la personne effectuant la notification ») ne semblent pas pleinement adaptés à certaines spécificités administratives nationales, notamment dans le contexte français.

Si l'harmonisation constitue un objectif important, une certaine marge de manœuvre

devrait être préservée afin de permettre aux autorités de contrôle d'adapter certains aspects pratiques du modèle à leur contexte national lorsque cela apparaît nécessaire.

Conclusion

Le Groupe La Poste soutient pleinement l'objectif visant à renforcer la cohérence des notifications de violations de données personnelles au sein de l'Union européenne. Toutefois, l'atteinte de cet objectif suppose un cadre qui demeure étroitement aligné sur l'article 33 du RGPD, proportionné au délai de notification de 72 heures et suffisamment flexible pour tenir compte des réalités opérationnelles de la gestion des incidents.

Si l'objectif d'harmonisation est pleinement soutenu, le modèle devrait veiller à ne pas accroître involontairement les obligations déclaratives au-delà de ce qui est nécessaire pour atteindre les objectifs de l'article 33 du RGPD. Une approche proportionnée et fondée sur les risques demeure essentielle afin de garantir des notifications rapides, cohérentes et efficaces dans l'ensemble de l'Union.

Nous invitons donc le CEPD à simplifier certaines demandes d'information, à clarifier le statut des rubriques complémentaires et à renforcer la distinction entre les informations nécessaires à la notification initiale et celles seulement facultatives pouvant être, le cas échéant, communiquées ultérieurement au fur et à mesure de l'avancement des investigations.

***

Nous contacter

Christelle DEFAYE-GENESTE, Directrice des Affaires Européennes et Douanières, Représentation de La Poste à Bruxelles - christelle.geneste@laposte.fr

Gaëlle KULIG, Responsable des Affaires Européennes Numériques – gaelle.kulig@laposte.fr

Damien LEGOFF, Group Data Protection Officer, damien.legoff@laposte.fr