October 2026



Position Paper of La Poste Groupe on the Guidelines 02/2026 on Anonymisation

English Version followed by French version.

Executive Summary

La Poste Groupe welcomes the EDPB Guidelines, which seek to update and clarify the conditions under which data may be considered anonymous. It supports a contextual approach and a high level of protection against re-identification risks, while calling for a framework that is sufficiently predictable, proportionate and practicable to be applied in complex data ecosystems.

In particular, La Poste Groupe recommends:

- basing the assessment of re-identification risks on scenarios that are objectively foreseeable, sufficiently likely and specific to the context under consideration, rather than on purely hypothetical possibilities;
- clarifying the application of the contextual approach to the relationship between the controller and the processor, as well as its interaction with the case-law of the Court of Justice of the European Union, in particular the *SRB* judgment;
- taking into account risks posed by unauthorised or malicious actors only where they are based on a concrete and credible risk scenario, having regard to the security measures effectively implemented;
- giving greater recognition to the combined effect of technical, organisational, contractual and legal safeguards when assessing whether data are anonymous;

LA POSTE
GROUPE

- framing the reassessment of anonymisation through a risk-based approach and clearly identified triggering events, assessed in light of the state of the art and reasonably foreseeable developments; and
- providing further guidance on artificial intelligence models, training data and synthetic data, in particular regarding the level of accuracy and reliability required to establish an actual risk of re-identification.

These clarifications would strengthen legal certainty and facilitate the practical application of the Guidelines, without reducing the level of protection afforded to data subjects.

La Poste Groupe welcomes the initiative of the European Data Protection Board (EDPB) to provide an updated and practical framework for assessing the anonymisation of data.

As a provider of postal, banking and digital services, La Poste Groupe supports a high level of protection against re-identification risks. It nevertheless emphasises the importance of establishing a predictable, proportionate and workable framework that can be applied in complex data ecosystems.

Against this background, La Poste Groupe invites the EDPB to take the following observations into consideration.

1. Ensuring a consistent and risk-based application of the contextual approach

La Poste Groupe welcomes the recognition that whether data are anonymous or personal may vary depending on the perspective and actual capabilities of the entity concerned. This contextual approach is particularly important in data-sharing environments involving controllers, processors, independent recipients and technical service providers.

However, identifying all relevant entities and all chains of means potentially available for the purposes of re-identification may prove particularly complex in practice.

➢ ***La Poste Groupe therefore recommends clarifying that the assessment should focus on scenarios that are objectively foreseeable and sufficiently likely, rather than on purely hypothetical possibilities that could ultimately deprive the contextual approach of its practical effect. The final Guidelines could usefully include further examples illustrating how the contextual approach should be applied in complex processing chains and secure data-sharing environments***.

Furthermore, the Guidelines state that, for an entity processing data on behalf of another entity, the assessment of whether or not the data are personal must be conducted from the perspective of the entity on whose behalf the data are processed. Accordingly, where the data are personal data from the controller's perspective, they must also be regarded as personal data for the processor.

➢ ***La Poste Groupe understands the rationale underlying the EDPB's position. However, the wording used effectively disregards the processor's own perspective and appears difficult to reconcile with the contextual approach, under which the assessment of whether or not data are anonymous should take account of the perspective of the entity concerned and the means reasonably likely to be used by that entity. If the intention is to preclude data from being regarded as anonymous for a processor whenever they are***

processed on behalf of the controller, the Guidelines should state this very clearly: the processor's position must systematically be equated with that of the controller. In such circumstances, the only situation in which data could be anonymous for a processor would be where the processor reuses the data for processing carried out under its own responsibility. This should likewise be clarified.

- ***La Poste Groupe therefore recommends providing further clarification on this central issue concerning the relationship between the controller and its processor.***

2. Adopting a more restrictive interpretation of the contextual approach

La Poste Groupe welcomes the consideration given to the means reasonably likely to be used by each entity to identify an individual.

However, La Poste Groupe notes that certain wording in the Guidelines appears to result in a broad interpretation of the means reasonably likely to be used. This interpretation appears to go beyond that adopted by the Court of Justice of the European Union (CJEU) in Case C-413/23, SRB.

- ***The EDPB is invited to clarify how its approach relates to the findings of the SRB judgment, so as to avoid effectively establishing a presumption that data remain personal data whenever a possible chain of re-identification can be envisaged. A technique should be taken into account only where there is an objectively demonstrable likelihood that a specific entity could gain access to it, use it in the context under consideration and obtain a sufficiently reliable result to identify an individual.***

Similarly, La Poste Groupe acknowledges that developments in artificial intelligence may reduce the effort required for re-identification, particularly in terms of time, cost and human resources. However, that consideration alone should not lead to the presumption that all theoretically conceivable means thereby become reasonably likely to be used.

- ***The EDPB should clarify the extent to which developments in artificial intelligence may materially affect the assessment of the means reasonably likely to be used. More broadly, the Guidelines should establish a concrete threshold for distinguishing plausible use from a purely hypothetical possibility.***

3. Clarifying the assessment of risks of access by unauthorised actors

The Guidelines indicate that unauthorised or malicious actors may, depending on the circumstances, be relevant when assessing whether means of re-identification are reasonably likely to be used. They also acknowledge that it is not necessary to systematically take into account the perspective of all such actors and that effective security measures may limit the number of entities considered likely to gain access to the data.

- ***La Poste Groupe recommends clarifying that risks associated with malicious actors should be taken into account only where they are based on a concrete and credible risk scenario, having regard in particular to:***
- ***the nature and sensitivity of the data;***
- ***the threat landscape;***

- ***the resources available for the purposes of re-identification; and***
- ***the technical and organisational measures implemented.***

➢ ***The mere theoretical possibility of unauthorised access should not, in itself, preclude data from being regarded as anonymous where state-of-the-art security measures appropriate to the risks have been implemented.***

4. Giving greater recognition to the combined effect of the various safeguards

La Poste Groupe acknowledges that contractual restrictions cannot, on their own, ensure that data are anonymous. However, contractual commitments may constitute an important component of a broader framework combining technical, organisational and legal safeguards, together with oversight mechanisms, in order to objectively reduce the likelihood that a given means will be used.

➢ ***The final Guidelines should provide further clarification on how the cumulative effect of the following measures may be taken into account in the assessment:***

- ***access control and data segregation mechanisms;***
- ***access logging and monitoring;***
- ***encryption and secure processing environments;***
- ***restrictions governing any subsequent disclosure of the data;***
- ***legally enforceable prohibitions on re-identification; and***
- ***audit rights, oversight mechanisms and applicable sanctions.***

➢ ***Such clarification would enhance legal certainty for secure arrangements for data sharing between professional parties, without reducing the level of protection afforded to data subjects.***

➢ ***Similarly, the final Guidelines could usefully expand on the EDPB's analysis of contractual measures and provide further guidance on the characteristics required for contractual commitments to be considered sufficiently reliable, verifiable and effective to have a meaningful bearing on the assessment of whether data are anonymous. Contractual restrictions may objectively reduce the likelihood of re-identification. To consider otherwise would be to suggest that contractual commitments have only residual value, which would be difficult to reconcile with the requirement to include clauses compliant with Article 28 of the General Data Protection Regulation (GDPR) in the relationship between a controller and a processor.***

5. Providing proportionate guidance on the periodic reassessment of anonymisation

La Poste Groupe supports the principle that the risk of re-identification may need to be reassessed in the light of technological developments, the availability of new data or the occurrence of a security incident.

To ensure that this requirement is implemented in a proportionate and workable manner, La Poste Groupe recommends adopting a risk-based approach centred on clearly identified triggering events.

➢ ***In particular, the final Guidelines could recognise the following as events that may warrant a reassessment:***

- ***a material change to the dataset or to the list of its recipients;***
- ***the availability of new external data sources that may enable data matching;***

- ***a significant development in re-identification techniques;***
- ***a security incident affecting the confidentiality of the relevant information; and***
- ***a change to the applicable technical or organisational measures.***

➢ ***In the context of technological developments, La Poste Groupe recommends confirming that the periodic reassessment should be carried out on the basis of the state of the art available at the time of the assessment and of reasonably foreseeable developments. Otherwise, the reassessment could lead to hypothetical and as yet unknown technological developments being taken into account, and thus to anonymisation being invalidated on the basis of hypothetical capabilities that do not yet exist or whose future availability remains uncertain.***

6. Facilitating the application of the framework to artificial intelligence models and synthetic data

The Guidelines acknowledge that artificial intelligence models and synthetic data may enable specific information to be inferred when queried using prompts or instructions combined with additional information. They also refer to membership inference attacks and other techniques that may enable information to be extracted from datasets or models presented as anonymous.

➢ ***La Poste Groupe recommends providing further guidance on:***
- ***the distinction between the anonymisation of a training dataset and the assessment of whether an artificial intelligence model contains or constitutes personal data, or may be regarded as anonymous;***
- ***the level of accuracy and reliability required for a re-identification or inference technique to be considered sufficiently effective;***
- ***appropriate methods for assessing whether synthetic data may be regarded as anonymous; and***
- ***the relationship between these Guidelines and EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.***

➢ ***Such guidance would support the development of trustworthy and privacy-preserving artificial intelligence, while ensuring effective protection for data subjects.***

➢ ***Furthermore, the EDPB could usefully provide guidance on how to assess, in practice, whether a re-identification or identification technique is sufficiently accurate and reliable.***

Conclusion

La Poste Groupe supports the EDPB's objective of strengthening legal and technical certainty in relation to anonymisation.

Further clarification regarding risk-based assessments, complex processing chains, the combined effect of the various safeguards, the reassessment of anonymisation and artificial intelligence-related use cases would facilitate the consistent implementation of

the Guidelines, while maintaining a high level of protection for data subjects.

As currently drafted, however, the cumulative effect of the various elements addressed in the draft Guidelines could suggest that anonymisation is, in practice, unattainable or achievable only in exceptionally limited circumstances. In particular, the application of the contextual approach to the relationship between controllers and processors requires further clarification in order to provide the various stakeholders with greater legal certainty following the CJEU's judgment in Case C-413/23, SRB, rather than perpetuating the uncertainty that the draft Guidelines currently leave unresolved.



Position du Groupe La Poste sur les lignes directrices 02/2026 du CEPD relatives à l'anonymisation

Version française

EN RÉSUMÉ

Le Groupe La Poste accueille favorablement les lignes directrices du CEPD, qui visent à actualiser et à clarifier les conditions dans lesquelles des données peuvent être considérées comme anonymes. Il soutient une approche contextuelle et un niveau élevé de protection contre les risques de réidentification, tout en appelant à un cadre suffisamment prévisible, proportionné et opérationnel pour être appliqué dans des écosystèmes de données complexes.

Le Groupe La Poste recommande en particulier :

- De fonder l'évaluation du risque de réidentification sur des scénarios objectivement prévisibles, suffisamment probables et propres au contexte considéré, plutôt que sur des possibilités purement hypothétiques ;
- De clarifier l'application de l'approche contextuelle dans la relation entre le responsable du traitement et le sous-traitant, ainsi que son articulation avec la jurisprudence de la CJUE, notamment l'arrêt *SRB* ;
- De ne prendre en compte les risques liés à des acteurs non autorisés ou malveillants que lorsqu'ils reposent sur un scénario concret et crédible, en tenant compte des mesures de sécurité effectivement mises en œuvre ;
- De mieux reconnaître l'effet combiné des garanties techniques, organisationnelles, contractuelles et juridiques dans l'évaluation du caractère anonyme des données ;

- D'encadrer le réexamen de l'anonymisation par une approche fondée sur les risques et sur des événements déclencheurs clairement identifiés, appréciés au regard de l'état de l'art et des évolutions raisonnablement anticipables ;
- De fournir des orientations supplémentaires concernant les modèles d'intelligence artificielle, les données d'entraînement et les données synthétiques, notamment sur le niveau de précision et de fiabilité requis pour caractériser un risque effectif de réidentification.

Ces clarifications permettraient de renforcer la sécurité juridique et l'application opérationnelle des lignes directrices, sans réduire le niveau de protection accordé aux personnes concernées.

Le Groupe La Poste salue l'initiative du Comité européen de la protection des données (CEPD) visant à proposer un cadre actualisé et pratique pour évaluer l'anonymisation des données.

En tant que fournisseur de services postaux, bancaires et numériques, le Groupe La Poste soutient un niveau élevé de protection contre les risques de réidentification. Il souligne toutefois l'importance de disposer d'un cadre prévisible, proportionné et opérationnel, susceptible d'être appliqué dans des écosystèmes de données complexes.

Dans ce contexte, le Groupe La Poste invite le CEPD à prendre en considération les observations suivantes.

1. Garantir une application cohérente et fondée sur les risques de l'approche contextuelle

Le Groupe La Poste accueille favorablement la reconnaissance du fait que le caractère anonyme ou personnel des données peut varier en fonction de la perspective et des capacités effectives de l'entité concernée. Cette approche contextuelle est particulièrement importante dans les environnements de partage de données faisant intervenir des responsables du traitement, des sous-traitants, des destinataires indépendants et des prestataires de services techniques.

Toutefois, l'identification de l'ensemble des entités pertinentes et de toutes les chaînes de moyens potentiellement disponibles aux fins d'une réidentification peut s'avérer particulièrement complexe en pratique.

- ***Le Groupe La Poste recommande donc de préciser que l'évaluation devrait se concentrer sur des scénarios objectivement prévisibles et présentant une probabilité suffisante, plutôt que sur des possibilités purement hypothétiques qui pourraient aboutir à priver l'approche contextuelle de son effet. Les lignes directrices définitives pourraient utilement comporter des exemples supplémentaires illustrant la manière dont l'approche contextuelle doit être appliquée dans les chaînes complexes de traitement et les environnements sécurisés de partage de données.***

Par ailleurs, les lignes directrices indiquent que le caractère personnel ou non des données, pour l'entité qui traite des données pour le compte d'une autre, doit être évalué en se référant à la perspective de l'entité pour le compte de laquelle les données sont traitées. Ainsi, dès lors que les données sont personnelles pour le responsable de traitement, elles doivent être considérées comme étant personnelles pour le sous-

traitant.

- ***Le Groupe La Poste comprend la logique poursuivie par le CEPD mais la formulation retenue conduit à écarter la perspective propre du sous-traitant, et apparaît difficilement conciliable avec l'approche contextuelle qui suppose d'apprécier le caractère anonyme ou non des données au regard de la perspective et des moyens raisonnablement susceptibles d'être utilisés par l'entité concernée. S'il s'agit d'exclure la possibilité de retenir le caractère anonyme des données pour un sous-traitant dès lors qu'il les traite pour le compte du responsable de traitement, les lignes directrices doivent alors l'écrire très clairement : le sous-traitant doit être systématiquement assimilé au responsable du traitement. Dans ce cas, la seule possibilité de données anonymes pour un sous-traitant résiderait dans l'hypothèse d'une réutilisation des données par le sous-traitant pour un traitement sous sa propre responsabilité, ce qui devrait là encore être précisé.***

- ***Le Groupe La Poste recommande donc que des précisions soient apportées sur ce point central qu'est la relation entre le responsable du traitement et son sous-traitant.***

2. Proposer une conception plus restrictive de l'approche contextuelle

Le Groupe La Poste accueille favorablement la prise en compte des moyens raisonnablement susceptibles d'être utilisés par chaque entité pour identifier un individu.

Le Groupe relève cependant que certaines formulations des lignes directrices semblent conduire à une conception extensive des moyens raisonnablement susceptibles d'être utilisés. Cette conception paraît aller au-delà de celle retenue par la Cour de Justice de l'Union européenne (CJUE) dans l'arrêt C-413/23 (SRB).

- ***Le CEPD est invité à préciser comment son approche s'articule avec les enseignements de l'arrêt SRB afin d'éviter que ne soit en réalité posée une présomption pratique selon laquelle les données restent personnelles dès qu'une chaîne de réidentification peut être imaginée. Une technique ne doit être retenue que s'il existe une probabilité objectivement démontrable qu'une entité déterminée puisse y accéder, l'utiliser dans le contexte considéré et obtenir un résultat suffisamment fiable pour identifier une personne.***

De même, le Groupe La Poste comprend que le développement de l'intelligence artificielle puisse réduire les efforts à fournir pour la réidentification, notamment en matière de temps, de coût et de main d'œuvre. Toutefois, cette seule considération ne devrait pas conduire à présumer que l'ensemble des moyens théoriquement envisageables deviennent, de ce seul fait, raisonnablement susceptibles d'être utilisés.

- ***Le CEPD devrait préciser dans quelle mesure les évolutions de l'intelligence artificielle peuvent effectivement modifier l'analyse des moyens raisonnablement susceptibles d'être utilisés. Plus largement, le texte devrait fournir un seuil concret permettant de distinguer un recours plausible d'une simple hypothèse.***

3. Clarifier l'évaluation des risques d'accès par des acteurs non autorisés

Les lignes directrices indiquent que des acteurs non autorisés ou malveillants peuvent,

selon les circonstances, être pertinents pour apprécier si des moyens de réidentification sont raisonnablement susceptibles d'être utilisés. Elles reconnaissent également qu'il n'est pas nécessaire de prendre systématiquement en considération la perspective de l'ensemble de ces acteurs et que des mesures de sécurité efficaces peuvent limiter le nombre d'entités considérées comme susceptibles d'accéder aux données.

- ***Le Groupe La Poste recommande de préciser que les risques liés à des acteurs malveillants ne devraient être pris en compte que lorsqu'ils reposent sur un scénario de risque concret et crédible, en tenant compte notamment :***
- ***De la nature et de la sensibilité des données ;***
- ***Du contexte de menace ;***
- ***Des ressources disponibles aux fins d'une réidentification ;***
- ***Des mesures techniques et organisationnelles mises en œuvre.***

- ***La seule possibilité théorique d'un accès non autorisé ne devrait pas, à elle seule, empêcher de considérer les données comme anonymes lorsque des mesures de sécurité correspondant à l'état de l'art et adaptées aux risques ont été mises en œuvre.***

4. Mieux reconnaître l'effet combiné des différentes garanties

Le Groupe La Poste convient que des restrictions contractuelles ne peuvent, à elles seules, garantir l'anonymisation des données. Toutefois, les engagements contractuels peuvent constituer une composante importante d'un dispositif plus large associant des garanties techniques, organisationnelles et juridiques, ainsi que de contrôle afin de réduire objectivement la probabilité qu'un moyen soit raisonnablement utilisé.

- ***Les lignes directrices définitives devraient préciser davantage la manière dont l'effet cumulé des mesures suivantes peut être pris en considération dans l'évaluation :***
- ***Les dispositifs de contrôle des accès et de cloisonnement des données ;***
- ***La traçabilité et le suivi des accès ;***
- ***Le chiffrement et les environnements sécurisés de traitement ;***
- ***Les restrictions encadrant toute communication ultérieure des données ;***
- ***Les interdictions opposables de réidentification ;***
- ***Les droits d'audit, les mécanismes de contrôle et les sanctions applicables.***

- ***Une telle clarification renforcerait la sécurité juridique des dispositifs sécurisés de partage de données entre professionnels, sans réduire le niveau de protection accordé aux personnes concernées.***

- ***De même, les lignes directrices définitives pourraient utilement compléter l'analyse du CEPD relative aux mesures contractuelles et fournir des orientations complémentaires sur les caractéristiques permettant de considérer que des engagements contractuels sont suffisamment fiables, vérifiables et effectifs pour avoir une réelle incidence sur l'appréciation du caractère anonyme des données. En effet, les restrictions contractuelles peuvent réduire objectivement la vraisemblance d'une réidentification, sauf à considérer qu'un engagement contractuel n'a qu'une valeur résiduelle, ce qui entrerait en contradiction avec la nécessité de prévoir des clauses conformes à l'article 28 du Règlement général sur la protection des données (RGPD) dans***

la relation responsable du traitement / sous-traitant.

5. Fournir des orientations proportionnées sur le réexamen périodique de l'anonymisation

Le Groupe La Poste soutient le principe selon lequel le risque de réidentification peut devoir être réévalué à la lumière des évolutions technologiques, de la disponibilité de nouvelles données ou de la survenance d'un incident de sécurité.

Afin de garantir une mise en œuvre proportionnée et opérationnelle de cette exigence, le Groupe La Poste recommande de retenir une approche fondée sur les risques et sur des événements déclencheurs clairement identifiés.

- ***Les lignes directrices définitives pourraient notamment reconnaître comme événements susceptibles de justifier un réexamen :***
- ***Une modification substantielle du jeu de données ou de la liste de ses destinataires ;***
- ***La mise à disposition de nouvelles sources externes de données susceptibles de permettre des recoupements ;***
- ***Une évolution significative des techniques de réidentification ;***
- ***Un incident de sécurité affectant la confidentialité des informations pertinentes ;***
- ***Une modification des mesures techniques ou organisationnelles applicables.***

- ***Le Groupe La Poste recommande, dans le contexte de l'évolution des technologies, de confirmer que le réexamen périodique doit être effectué sur la base de l'état de l'art disponible au moment de l'évaluation et des évolutions raisonnablement anticipables. A défaut, le réexamen pourrait conduire à prendre en compte des développements technologiques hypothétiques et inconnus, et devoir alors invalider une anonymisation sur la base de capacités hypothétiques qui n'existent pas encore ou dont l'accessibilité future est inconnue.***

6. Faciliter l'application du cadre aux modèles d'intelligence artificielle et aux données synthétiques

Les lignes directrices reconnaissent que des modèles d'intelligence artificielle et des données synthétiques peuvent permettre d'inférer des informations spécifiques lorsqu'ils sont interrogés au moyen de requêtes ou d'instructions combinées avec des informations complémentaires. Elles évoquent également les attaques par inférence d'appartenance et d'autres techniques susceptibles d'extraire des informations à partir de jeux de données ou de modèles présentés comme anonymes.

- ***Le Groupe La Poste recommande de fournir des orientations supplémentaires concernant :***
- ***La distinction entre l'anonymisation d'un jeu de données d'entraînement et l'évaluation du caractère personnel ou anonyme d'un modèle d'intelligence artificielle ;***
- ***Le niveau de précision et de fiabilité requis pour qu'une technique de réidentification ou d'inférence soit considérée comme suffisamment efficace ;***
- ***Les méthodes appropriées pour évaluer le caractère anonyme des données***

synthétiques ;

- ***L'articulation entre les présentes lignes directrices et l'avis 28/2024 du CEPD relatif à certains aspects de la protection des données dans le contexte des modèles d'intelligence artificielle.***

➢ ***De telles orientations favoriseraient le développement d'une intelligence artificielle de confiance et respectueuse de la vie privée, tout en garantissant une protection effective des personnes concernées.***

➢ ***Par ailleurs, le CEPD pourrait utilement ajouter des orientations sur la manière d'apprécier le caractère suffisamment précis et fiable d'une technique de (ré)identification en pratique.***

Conclusion

Le Groupe La Poste soutient l'objectif du CEPD consistant à renforcer la sécurité juridique et technique en matière d'anonymisation.

Des précisions supplémentaires concernant les évaluations fondées sur les risques, les chaînes complexes de traitement, l'effet combiné des différentes garanties, le réexamen de l'anonymisation et les cas d'usage liés à l'intelligence artificielle faciliteraient une mise en œuvre cohérente des lignes directrices, tout en maintenant un niveau élevé de protection des personnes concernées. En l'état, la combinaison de l'ensemble des points abordés dans le projet conduit à considérer que l'anonymisation est un objectif qui ne serait pas atteignable en pratique, ou dans des hypothèses particulièrement rares. En particulier, le cas de la relation entre le responsable de traitement et son sous-traitant doit être clarifié et précisé afin de sortir les différents acteurs de l'incertitude créée par la CJUE dans son arrêt C-413/23 (SRB) et que le projet de lignes directrices ne fait qu'entretenir.

***

Nous contacter

Sonia SCHARFMAN, Directrice des Affaires Européennes, Représentation de La Poste à Bruxelles – sonia.scharfman@laposte.fr

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

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