L'Afep

Paris, 30th October 2026

POSITION PAPER

EDPB guidelines on anonymisation

L'Afep welcomes and supports the EDPB's intention to adopt guidelines on anonymization as it considers it as a fundamental concept to define the limits of the GDPR and enable the use of anonymized data to the benefit not only of data security but also of innovation and growth driven by data, namely AI.

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.

L'Afep member companies call the EDPB to adopt **shorter and more operational guidelines** that would provide **real support** for companies in implementing the GDPR, to facilitate their adoption and use by all companies, including SMEs, and avoid creating additional red tape for companies. The draft submitted to consultation is very long and complex to understand even for large companies.

As an illustration, French large companies have noted that, with regard to health data, the Health Data Hub in France has published a shorter guide for documenting the anonymization process and assessing the anonymity of a dataset, which calls for a detailed, step-by-step description of how anonymization techniques are implemented[1].

L'Afep observes that recently the EDPB launched public consultation on draft guidelines or templates, for example its template for Data Protection Impact Assessment (DPIA), which were accompanied by an explainer. **We would suggest that the final guidelines on anonymisation be also accompanied by an explanatory document to make it easier to read, to place it in the context of the case law of the Court of Justice and the work of the EDPB, and, finally, to provide concrete examples.**

[1] https://health-data-hub.fr/sites/default/files/2025-04/Guide%20d'évaluation%20du%20caractère%20anonyme%20d'un%20jeu%20de%20données%20v2.docx

This explanatory guide accompanying the guidelines could therefore begin by referring to the EDPS's previous work, in particular the workshop held on 12 December 2025, as well as the summary document of 18 February 2026, which sets out the concerns raised by the participants at that workshop.

This guide could also refer to the Helsinki commitments made by the EDPB and the national data protection authorities to address the practical concerns raised by data controllers regarding the implementation of the GDPR.

Finally, the issue of examples is a delicate one, in that some stakeholders would obviously like to see more, whilst others would prefer fewer in order to streamline the guidelines. As an illustration, a wider variety of illustrations, particularly in the transport and automotive sectors, would be appreciated.

One solution could be to include these illustrations in the explanatory guide in order to streamline the draft guidelines and make them easier to read. In any case, **large companies expect to find, in the examples, specific cases where the EDPB clearly considers the data to be anonymised**. These examples need to be based on real life use cases. As such, we would suggest referring to the study "From pseudonymous to anonymous data" that provides concrete European industry use-cases of anonymisation in different industry sectors[2]. Data controllers must indeed be able to rely on **positive examples** to understand what is expected of them by the authorities.

1 - General comments

L'Afep invites the EDPB to apply in these draft guidelines a reasonable risk-based approach and avoid issuing guidelines that would end up applying a precautionary principle in practice that would annihilate data and AI driven innovation in Europe.

This reasonable risk-based approach is also necessary to align the GDPR with the evolution of the legal landscape in Europe. Since 2018, the EU has indeed recognised the economic value of data and the organised innovation around it by adopting several key legislations to enable the sharing of data and the development of data driven products and services (Data Governance Act, Data Act, Artificial Intelligence Act, etc.). The EDPB cannot ignore these important legislative developments that call for data to be shared and reused and are positioning data innovation as a central role in our societies and economies.

Anonymisation can contribute to the dual objective of compliance with data protection regulations and technological innovation around data.

[2] https://cabinet-samman.com/wp-content/uploads/2026/06/From-Pseudonymised-to-Anonymous-Data-EU-Industry-Use-Cases-Joint-Policy-Report-2.pdf

L'Afep member companies observe that the French AI commission in its report to the President of the Republic recommended returning to **the initial spirit of the GDPR** to reconcile personal data protection and innovation[3]. This issue has also been clearly identified in the DRAGHI report which states that "*while the ambitions of the EU's GDPR and AI Act are commendable, their complexity and risk of overlaps and inconsistencies can undermine developments in the field of AI by EU industry actors*".

Such draft guidelines offers an opportunity to restore the risk-based approach enshrined in the GDPR to the heart of controllers' compliance processes. This is all the more important if privacy specialists are to focus their time and efforts on the processing operations that present the highest risks, in the interests of data subjects themselves.

Thus, the finalisation of these guidelines should enable data controllers to refrain from applying the GDPR to data that the EDPB actually considers to be anonymous. **Adopting guidelines that are too complex or lack specificity will lead organisations to apply the GDPR by default to all data, including anonymised data**. This would constitute an overly broad application of the **precautionary principle**, running **counter to the GDPR's risk-based approach**. If such a course is taken by the EDPB, it would hinder the implementation of numerous European ambitious texts, notably the Data Act and the AI Act.

2 - An approach that is still too cautious

L'Afep welcomes the fact that these draft guidelines clearly recognise the relative concept of personal data, in accordance with the established case law of the CJEU, in particular in the SRB case.

This approach is further qualified by the limitations set out by the EDPB in its risk assessment. This is particularly the case with regard to datasets containing a mix of anonymous and personal data (§36). French large companies do not agree with the view that such a dataset, in its entirety, should be regarded and treated as containing personal data. This should be left to the organisation to decide to manage the situation in compliance with the law.

Likewise, the last sentence of paragraph 48 introduces a **precautionary standard** that is not required by the GDPR and that goes beyond the risk-based approach of the GDPR. No more cautious approach is required than strictly necessary. **Subjecting data to the GDPR "in cases of doubt" goes against providing the legal certainty organisations are asking for and reinforces the waste in resources.** In doing so, the draft guidelines encourage organisations to apply the list of obligations of the GDPR to data where it may not be in fact necessary to do so.

[3] Commission de l'intelligence artificielle, mars 2024, IA : notre ambition pour la France, https://www.economie.gouv.fr/files/files/directions_services/cge/commission-IA.pdf.

3 - Accept that there is no such thing as zero risk

L'Afep welcomes and shares the EDPB's view that "*for information to be anonymous, the lihelihood of the individual being successfully distinguished from others within the given context does not need to be zero; instead, that likelihood should be insignificant in reality*" (§22).

This statement is consistent with a reasonable interpretation of the GDPR's risk-based approach and should be encouraged. Above all, it reflects the practical reality in the field of IT, and in particular cybersecurity. Indeed, **when it comes to cybersecurity, absolute security and zero risk do not exist**.

Nevertheless, subsequent developments in the draft guidelines on the assessment of the resources reasonably likely to be used by an entity adopt a broad interpretation, thereby undermining this original acceptance of the absence of zero risk (§29 and 30).

Thus, the draft sets out a list of entities capable of identifying natural persons that is particularly broad and out of touch with the reality of the overwhelming majority of situations faced by data controllers. This list places data controllers and their business partners on the one hand, and intelligence agencies, cybercriminals and rogue employees on the other, on an equal footing.

The approach of including scenarios involving the commission of illegal acts in risk analysis makes the process of ensuring the security of anonymization largely unrealistic. It is difficult to reconcile with the criterion of reasonableness set forth in Recital 26 of the GDPR and with the requirement of legal certainty, which is nevertheless essential for stakeholders to innovate with confidence.

Footnote 25 only states that not all of them need to be considered systematically. Without a shared typology, each organisation and each authority builds its own list, which makes assessments hard to compare.

Placing all these actors on the same footing, in the context of the application of the GDPR, is unreasonable and does not correspond to the GDPR's risk-based approach. If one were to follow the EDPB's reasoning, **the most stringent standards regarding the protection of national defence secrets would have to be applied to personal data – after anonymisation –used for commercial marketing or scientific research purposes**.

It is unreasonable to ask data controllers to take all these potential actors into account without distinction, namely in connection with the transfer of data to a third party. On the contrary, it is up to the EDPB to distinguish between these actors based on their interests and the sensitivity of the data in question, and to consider for example the potential involvement of foreign intelligence agencies only in the most extreme cases. Thus, in certain situations, the recipient organisations will have **no interest in re-identification** (namely recipient organisations acting in accordance with the law, employees, service providers): the risk will be strictly limited to an accident or negligence.

For each category of recipients, the EDPB should indicate the means to be presumed and the situations in which it must be considered, depending on the sensitivity of the data and how it is released. Moreover, the EDPB should explain clearly how organisations are supposed to conduct such assessment in practice as well as concrete and real examples of data passing muster this requirement.

The **notion of an "entity"** should be further clarified. The Guidelines should specify whether different subsidiaries within the same group, or different departments or units within the same legal entity, may be assessed separately for the purposes of anonymisation where they have significantly different access capabilities, knowledge or means of re-identification. Such clarification would ensure that the assessment takes into account the actual context in which the data is accessed and the means reasonably likely to be used to re-identify the data subjects. The Guidelines would also benefit from including a practical example illustrating such a situation.

In reality, **the standards set out in these draft guidelines are too high, to the detriment of legal certainty for businesses**, which are thus left without clear guidance on effective ways of anonymising data. Consequently, this will encourage data controllers to treat anonymised data as personal data within the meaning of the GDPR.

L'Afep is particularly surprised by the wording proposed in **paragraphs 32 and 33 as they are contrary to the CJUE case law** according to which means do not need to be considered if they are prohibited by law. Any further development in these paragraphs does not comply with this case law and has only the effect of creating more legal uncertainty for organisations.

4 - The need to refer to international standards

L'Afep observes that there are debates taking place all over the world on the concept of anonymised data, particularly in Canada, Singapore and the United Kingdom. **The debates taking place in Europe would benefit from being conducted in the light of the insights and solutions identified by countries that share our principles and values.**

The draft states that the state of the art for re-identification techniques "*is always evolving*" and that the EDPB "*encourages the development, dissemination and application of scientifically grounded expertise on this topic*", without designating a reference method. Each organisation therefore builds its own demonstration without knowing whether it will be judged sufficient in case of an inspection (§84).

As an illustration, the EDPB could for instance provide references to available resources on how to conduct a "**motivated intruder test**" to help organisations determine whether anonymous information is likely to result in the identification of a person when it is shared with other organisations. It should also clarify what is the methodology (or methodologies) used by the DPAs when they conduct their own assessment. This would raise the level of legal certainty by aligning risk assessments methodologies[4].

Moreover, French large companies also observe that existing international standards already deal with the question of information security, cybersecurity and privacy protection.

Instead of rewriting standards that risk being disconnected from the risk-based approach and the economic reality of companies, EDPB could usefully rely on the following standards:

- **ISO/IEC 20889:2018(en)** – Privacy enhancing data de-identification terminology and classification of techniques. This document provides a description of privacy-enhancing data de-identification techniques, to be used to describe and design de-identification measures in accordance with the privacy principles in **ISO/IEC 29100**. In particular, this document specifies terminology, a classification of de-identification techniques according to their characteristics, and their applicability for reducing the risk of re-identification.
- **ISO/IEC 27559:2022(en)** – Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework. This document provides a framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data.

In addition, L'Afep strongly encourages the EDPB to submit these draft guidelines to ENISA. The implementation of the GDPR must not be viewed in isolation, separate from other regulations and public authorities. ENISA's role appears to be crucial in these matters.

5 - The need to ensure the robustness of anonymization techniques

L'Afep observes that data controllers need to test and ensure the robustness of their anonymisation techniques and use cases. Indeed, **legal certainty is key to allow data controllers to be able to innovate around data**.

Therefore, L'Afep encourages both EDPB and DPAs to develop codes of conduct, certifications and regularity sandboxes to encourage research and development around anonymisation.

This need for legal certainty requires that DPA do not only assess the robustness of the anonymisation technique at the enforcement stage. Cooperation and dialogue between controllers and DPA are fundamental and must benefit all stakeholders, from big corporations to SMEs and start-ups.

[4] See the ICO guidance on anonymisation explaining how the test works, providing official links and confirming that the ICO and the UK courts rely on this test https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/how-do-we-ensure-anonymisation-is-effective/#applythemotivatedintrudertest

6 - The need to precisely define new notions

French large companies observe that the draft guidelines introduce a distinction between individual and natural person, which it would seem useful to clarify.

In addition, the draft guidelines do not clarify anonymisation **in relation to other key concepts** such as pseudonymised data, deidentified data, non-personal data, synthetic data or other Privacy Enhancing Technologies (PETs). This could be done by the insertion of a glossary as annex of the Guidelines.

As such, the definitions of key concepts in the guidelines should also form part of a coherent and integrated regulatory framework, taking into account both existing and future regulatory instruments, including the Digital Omnibus currently under consideration by the co-legislators. Discrepancies in the interpretation of key concepts, such as anonymisation and pseudonymisation, between the guidelines and the Digital Omnibus could create significant legal uncertainty for the parties concerned and undermine the consistent application of the relevant rules. In these circumstances, **French large companies suggest that the EDPB should wait until the co-legislators have completed their work on the Digital Omnibus before finalising its work on these guidelines**.

In conclusion, L'Afep considers that EDPB does not apply the risk-based approach of the GDPR to anonymisation and in particular to the risk of reidentification. **There is a certain bias in the document towards always treating the worst-case risk as not only possible but realistic**, without clarifying the mitigation measures available to organisations. Yet it is precisely clarification on this last point that businesses need (i.e. **positive examples**).

Thus, **the discussion on AI reflects a doomsday view of the technology**, which is said to increase the risks of re-identification (§92). The risks are real and must not be ignored, but it is unfortunate that the positive aspects of AI for the development of cybersecurity are, in turn, overlooked. **Artificial intelligence is, in fact, both a risk factor and a tool for enhancing security**. While the guidelines note that AI systems can significantly reduce the time, cost, and expertise required to cross-reference datasets and re-identify individuals, it is precisely through tools of this nature that this risk will be mitigated. Yet AI entails many risks but also presents opportunities in the field of cybersecurity.

In doing so, **the EDPB seems to overlook the fact that there is no such thing as absolute security or anonymity**, and that there will always be a potential risk of unauthorised access to data. This interpretation goes beyond the risk-based approach of the GDPR, which, by definition, does not rule out all risks, but merely requires that they be anticipated and mitigated. Consequently, L'Afep urges the EDPB to refrain from imposing on businesses additional formalities that are not provided for in the GDPR or that are disproportionate.

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