Contribution to the EDPB's guidelines on pseudonymisation

February 2025

AFEP member companies welcome the opportunity to take part to the public consultation opened by the European Data Protection Board (hereinafter referred to as "**EDPB**") on its draft guidelines 1/2025 on pseudonymisation as they consider it as a fundamental technique to comply with the GDPR and enable the safe use of data.

Nevertheless, companies question the calendar to adopt new guidelines on this subject as (i) the draft submitted to consultation makes numerous references to the notion of anonymous data as well as the conditions for data to be anonymous without indicating clearly what are these conditions, and (ii) the Court of justice should issue a decision on the subject of pseudonymisation and anonymisation in the near future[1].

On this last point, **they urge the EDPB not to adopt these guidelines before the issuance of the Court's decision in order to ensure that these guidelines are consistent with the latest case law of the Court**.

In addition, AFEP member companies call the EDPB to adopt **shorter 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. A harmonised analysis tool, a toolbox or a decision tree for the whole EU would be a useful aid for companies.

Companies are also surprised that the guidelines do not mention the relevance of pseudonymised data for AI. Pseudonymisation is often used by companies as a way to reduce risks in the context of AI development and deployment.

They also regret the focus of the examples and use case mostly on the health sector. More examples in various sectors are needed (telecommunications, advertising, commerce, manufacturing, energy, etc.).

[1] Case C-413/23P.

1. General comments

As a preliminary comment, AFEP member companies would like to remind the EDPB that they already called the attention of the European Commission in November 2023 on the fact that personal data protection authorities (hereinafter "**DPAs**") and the EDPB are reluctant to implement the **risk-based approach on which the GDPR is based**. In this respect, they observe that DPAs and EDPB have a particularly restrictive approach, applying the GDPR to the letter and even adopting a position of maximum protection of personal data without consideration for the day-to-day business life and economic models of companies.

It should be remembered that Recital 4 of the GDPR states that **the right to protection of personal data is not an absolute right**. It must be considered in relation to its function in society and balanced against other fundamental rights, in accordance with the **principle of proportionality**, which requires this protection to be weighed against all other fundamental rights, in particular the freedom to conduct a business. AFEP therefore considers that companies are faced with an **overly rigid and dogmatic interpretation of the GDPR**.

Thus, **AFEP member companies invite 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.**

This reasonable risk-based approach is also made possible by the development of new technologies that hold great promises for the protection of personal data.

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

AFEP member companies also 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[2].

[2] 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.

This issue has also been clearly identified in the recently issued 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*". It also stresses **the risk of European companies being excluded from early AI innovations because of the uncertainty of regulatory frameworks as well as higher burdens for EU researchers and innovators to develop homegrown AI**.

Moreover, it is necessary to take into account the risk that many AI models will be excluded from the European market due to overly strict regulations or legal uncertainty generated by a conservative interpretation of these texts. This will put European companies at a competitive disadvantage with their non-EU competitors as they will not be able to use or rely on certain AI models to develop their own AI systems or applications. **Ultimately, this will be detrimental to European society as a whole**.

2. The need to precisely define new notions

AFEP observes that the draft guidelines introduce the new concept of "*pseudonymisation domain*", which it would seem useful to clarify. Its objective seems to be to limit the notion of pseudonymisation to a perimeter defined by the recipients of the pseudonymised data. This choice has the advantage of circumscribing a context and a risk assessment, but the principle should not be limited to a simple description of the recipients of the pseudonymised data to be processed, without a suitable risk analysis method that takes into account the risks associated with unauthorised reversal of the pseudonymisation, depending on the techniques chosen and the needs in terms of the usefulness of the data. The text could be more explicit on these points.

AFEP also notes the reference to "*that freedom*" related to the pseudonymisation domain (see §10, page 8). This reference is unclear and should be specified.

In addition, AFEP observes that the draft guidelines introduce several new notions which are unclear:

- The notion of "*pseudonymising controllers*" which can lead to confusion with the notion of data controller, or the notion of pseudonymisation entity used by the ENISA;
- the notion of "*group of collaborating controllers*" and "*participating controllers*" (see §52, page 14) which can lead to confusion with the notion of "*joint controllers*" (see article 26 GDPR);
- the notion of "*lookup tables*" (see §87, page 21) which can lead to confusion with the notion of "*mapping table*" in accordance with the technical documents issued by the ENISA;
- the notion of "*risk of attribution*" (see §131, page 30) which could be clarified with the use of re identification.

Furthermore, AFEP member companies note that the draft guidelines recommend the employment of vetted personnel for the operation of the systems used for the execution of the pseudonymising transformation and the storage of the pseudonymisation secrets (see §109, page 25) and invite the EDPB to clarify this notion of "*vetted personnel*".

Finally, AFEP observes the use of new notions "*quasi-identifiers*" (see §101, page 23) "*perso pseudonyms*" (see §116, page 26) and "*relationship pseudonyms*" (see §117, page 26) which are not defined in the GDPR nor in any other documentation issued by the EDPB. As the draft guidelines seem to refer to an established doctrine, AFEP encourages the EDPB to indicate its sources.

3. The benefits of pseudonymisation

AFEP member companies welcome the fact that the EDPB explicitly recognizes in the draft guidelines that pseudonymisation "*can reduce the risks to the data subjects by preventing the attribution of personal data to natural persons in the course of processing the data, and in the event of unauthorized access or use*" (see page 3).

As regard the affirmation that "*pseudonymizing data reduces risk for data subjects while allowing general analysis*" (see §26, page 10), AFEP also notes it can "*help controllers and processors to meet their data protection obligations*"[3].

AFEP also shares the view of the EDPB that "*Pseudonymisation may lower the severity of the consequences of unauthorized access to data*" (see §59, page 15) and that "*it may be regarded as an appropriate technical and organizational measure that limits the impact of a personal data breach*" (see §62, page 16).

AFEP believes that this analysis is aligned with the risk-based approach of the GDPR.

Pseudonymised data convey less risk than directly identifying data. The GDPR contains fourteen provisions recognising that pseudonymisation reduces risks for data subjects. The reliance on de-identification techniques such as pseudonymisation must be part of the balancing exercise to show that the data has a less personal character than directly identifiable data. The more sensitive the data, the greater the risk of a negative impact on the data subjects and conversely, **the less identifiable the data, the less the risk of a negative impact on the data subjects.**

Indeed, pseudonymisation should be considered as a mitigating factor contributing to reducing the risk for data subjects in enforcement cases. Pseudonymized data cannot be treated as "data in clear" and should be recognized at least as a separate category of data. This would incentivize market players to implement such techniques.

[3] Recital 28 of the GDPR.

Nevertheless, AFEP member companies consider that the EDPB stopped in the middle of the road and did not fully draw the consequences of the risk-based approach in its draft guidelines.

As such, large companies draw the EDPB's attention to the fact that if "*The risk reduction resulting from pseudonymisation may enable controllers to rely on legitimate interests under Art. 6(1)(f) GDPR as the legal basis for their processing provided they meet the other requirements of that subparagraph*" (see page 3), this should not mean that pseudonymisation will be a prerequisite for data controller to use legitimate interest as legal basis.

Although pseudonymisation reduces the risks to personal data, EDPB still considers pseudonymised data as personal data, and applies disproportionate restrictions and conditions of use to them.

As an illustration, AFEP member companies do not share the view of the EDPB that "*as is true for any personal data, the flow of pseudonymised data should be tightly controlled*" (see §112, page 25). Here again, AFEP considers that companies are faced with an **overly rigid interpretation of the texts**.

Finally, Afep believes that §8 (page 8) contains an error "*It is clear that direct identifiers **don't** need to be removed from data if those data are not to be attributed to individuals*".

4. The necessity of distinguishing pseudonymised data and anonymised data

AFEP member companies consider that the draft guidelines should clarify more strongly the difference between pseudonymisation and anonymisation. In some instances, the pseudomymisation will be set up so that it is impossible to revert to the original data and raise the question as to whether the data would not become anonymous.

AFEP also recommends mentioning existing references or future guidance on anonymisation. References to the 2014 WP29 Opinion or the replacement text of the 2014 WP29 Opinion are missing.

As mentioned above, AFEP observes that the Court of justice should issue an important decision related to pseudonymisation and anonymisation in the near future. They note that the Advocate General considers that "*pseudonymisation leaves open the possibility that the data subjects may not be identifiable*" and "*it cannot be ruled out that such data may, under certain conditions, fall outside the scope of the concept of 'personal data'*"[4]. Thus, where the risk of identification is non-existent or insignificant that data can legally escape classification as "personal data"[5].

[4] Opinion of the Advocate General Spielmann, 6 February 2025, Case C-413/23P, §51 and 52.
[5] Opinion of the Advocate General Spielmann, 6 February 2025, Case C-413/23P, §57.

5. The need to ensure the robustness of pseundonymisation techniques

AFEP observes that controllers need to test and ensure the robustness of their pseudonymization techniques and use cases. Indeed, controllers need to have legal certainty to be able to innovate around data. Therefore, AFEP encourages EDPB and DPA to develop codes of conduct, certifications and regularity sandboxes to encourage research and development around pseudonymisation.

This need for legal certainty requires that DPA do not only assess the robustness of the pseudonymization 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.

6. The risk-based approach applied to the possibility of re-identifying data

As mentioned above, AFEP member companies consider that EDPB does not apply the risk-based approach of the GDPR to pseudonymization and in particular to the risk of reidentification.

Indeed, the EDPB bases its analysis on the worst-case scenarios instead of taking into account the advantages of pseudonymization. See namely:

- "*the effect of pseudonymisation will have to be measured against the capabilities of persons or parties acting without authorisation*" (see §11, page 8). This requirement is too high a standard instead of looking at all the instances pseudonymisation has in fact effectively reduced the risk of unlawful access.
- "*Additional information may also exist beyond the immediate control of the pseudonymising controller or processor. The pseudonymising controller or processor should take such information into account in the assessment of the effectiveness of pseudonymization*" (see §21, page 10) – which is contradictory.
- "*the controller may define the pseudonymisation domain to encompass (...) a range of or all external entities that may attempt to gain access to the data without authorisation*" (see §38, page 12).

In so doing, the EDPB seems to be forgetting that there is no such thing as absolute security or anonymity, and that there will always be a potential risk of access to data. **This interpretation goes beyond the risk-based approach of the GDPR, which by definition does not exclude all risks, but only requires that risks are anticipated and mitigated**. Therefore AFEP urges the EDPB to avoid adding additional not foreseen by the GDPR or disproportionate formalities for companies.

As regard the rights of the data subjects, AFEP believes that it must be impossible for individuals to exercise their rights on data that is not in clear text - unless they have the key.

7. The need to refer to international standards

AFEP member companies observe that existing international standards already deal with the question of information security, cybersecurity and privacy protection.

Instead of rewriting standards that are 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, AFEP questions the advisability of submitting this project to ENISA. The application of the GDPR must not be designed in silo, in isolation from other regulations and public authorities. The role of ENISA appears to be crucial on these issues.

Finally, AFEP would like to have concrete recommendations from the EDPB on how to ensure that the person exercising his/her GDPR rights on pseudonymised data is effectively the person to whom the pseudonymized data relates to avoid providing data to an unauthorized person. Indeed, some DPAs have been refusing reliance on a national ID, and controllers need alternative robust methods to effectively mitigate the risk of data breach.

ABOUT AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalisation is AFEP's core priority. AFEP has over 113 members. More than 8 million people are employed by AFEP member companies and their annual combined turnover amounts to €2,600 billion. 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.

Contacts:
Jocelyn Goubet – Director for Economic Law - j.goubet@afep.com
Alix Fontaine – European Affairs Deputy Director– a.fontaine@afep.com

Transparency Register identification number: 953933297-85