Comments on EDPB draft guidelines on pseudonymisation

13 March, 2025

Workday appreciates the opportunity to comment on the EDPB's draft Guidelines on pseudonymisation. Workday is the AI platform that helps organisations manage their most important assets – their people and money. The Workday platform is built with AI at the core to help customers elevate people, supercharge work, and move their business forever forward. Workday is used by more than 11,000 organisations around the world and across industries – from medium-sized businesses to more than 60% of the Fortune 500. Workday has over 4,300 employees in 19 European offices and more than 2,100 customers headquartered in Europe.

Please contact Marco Moragón, Senior Public Policy Manager, at marco.moragon@workday.com if you have any questions or would like further information.

General remarks

- Workday welcomes the EDPB's objective for the Guidelines to clarify the use and highlight the benefits of pseudonymisation for controllers and processors, and more broadly, that pseudonymisation is a practical and user-friendly tool to enhance security.
- To achieve the above stated purposes the Guidelines must:
    - drive consistency across national authorities
    - support controllers and processors
    - be accessible and practical, including to SMEs.
- If the Guidelines are not consistent with EU jurisprudence, and fail to acknowledge the evolution of the EDPS vs. SRB case by the General Court and the Advocate General Opinion, they will cause more confusion than clarification. As such, the EDPB should delay the publication of the Guidelines until the CJEU issues its final judgement to ensure full alignment.

Pseudonymisation, anonymisation and 'additional information'

The scope for what constitutes 'additional information' in the draft Guidelines is overly broad and would require controllers to consider all possible information, including data on social media, which is impractical and goes beyond the GDPRs Article 4. This could lead to controllers being held liable for information they cannot (and should not) reasonably access.

- Recommendation: Narrow the definition of 'additional information' - focusing on reasonably accessible information and acknowledging the limitations of controllers' knowledge regarding publicly available data.

The scope of the draft Guidelines is intended to be pseudonymisation, with separate guidelines on anonymisation expected to follow later this year. However, at times, the draft Guidelines opine on anonymisation, and do not acknowledge CJEU rulings that establish tests for anonymisation, particularly

regarding the accessibility of 'additional information' needed for re-identification. By implying that the mere existence of 'additional information' prevents data from being considered anonymous, even if inaccessible, the draft Guidelines undermine anonymisation efforts and contradict CJEU decisions.

- Recommendation: The Guidelines must clarify the distinction between pseudonymisation and anonymisation, ensuring the Guidelines don't impose anonymisation requirements on pseudonymised data. To prevent future contradiction and confusion, we recommend removing references to anonymisation and saving them for the separate guidance on anonymisation, or at a minimum, the Guidelines must incorporate the 'reasonable likelihood' test for reidentification, as established in Case C-582//14 and Case T-557/20, recognising that data without accessible 'additional information' should be considered anonymised.

Data subject rights

Point 79 of the draft Guidelines indicates that controllers would be required to help data subjects find their pseudonyms. Requiring the controller to access, identify and share the pseudonym introduces security risks in terms of reidentifying the data. GDPR Art.11(1) states that if the purposes for data processing no longer require identification of the data subject, the controller shall not be obliged to maintain, acquire or process additional information.

- Recommendation: We recommend not imposing new requirements for the controller to gather information to share the pseudonym with the data subject, and therefore to delete point 79.

Role of privacy-enhancing technologies (PETs)

The Guidelines are a clear opportunity to refer to the value of Privacy Enhancing Technologies (PETs) and their use with pseudonymisation, to strengthen the protection of personal or sensitive data and reduce the risk of re-identification.

- Recommendation: The EDPB should explicitly recognise PETs in the Guidelines and encourage their use, together with pseudonymisation, to achieve data-driven innovation without compromising privacy and data protection.

International data transfers

We welcome the recognition in Chapter 2.4.3 that pseudonymisation may constitute a 'supplementary measure' to ensure compliance with Article 44 and 46(1) GDPR. However, we are concerned that the conditions in points 64-67, in the context of transfers to third countries, are overly prescriptive and would appear to add requirements to Chapter V GDPR by requiring exporters to assess the information available to third country authorities, including its security services.

- Recommendation: We recommend deleting conditions 64-67, which are inconsistent with the GDPR and replacing this section with a direct reference to the EDPB's Guidance on international transfers of personal data.