The Association for Computing Machinery (ACM) is the world's longest established professional society, consisting of individuals involved in all aspects of computing. It annually bestows the ACM A.M. Turing Award, often popularly referred to as the "Nobel Prize of Computing." ACM's Europe Technology Policy Committee ("Europe TPC") is charged with and committed to providing sound **technical information** to policy makers and the general public in the service of sound public policymaking. Europe TPC has responded to the European Union stakeholders' consultations in the past in the context of the AI Act[1], the Data Act[2], the Digital Services Act[3][4], the Digital Citizen Principles[5], the Cyber Resilience Act[6], amongst others[7]. ACM and Europe TPC are non-profit, non-political, and non-lobbying organisations.

Europe TPC welcomes the opportunity to provide feedback on the European Data Protection Board's *Guidelines 01/2025 on Pseudonymisation*. We appreciate the EDPB's efforts to clarify the role of pseudonymisation in data protection and its implications for compliance with the General Data Protection Regulation (GDPR). Our response will highlight key technical and policy considerations to ensure that pseudonymisation remains an effective tool for data security, innovation, and regulatory compliance.

[1] https://www.acm.org/binaries/content/assets/public-policy/europe-tpc-comments-ai-consultation.pdf
[2] https://www.acm.org/binaries/content/assets/public-policy/acm-eur-tpc-data-act-comments-13may22a.pdf
[3] https://www.acm.org/binaries/content/assets/public-policy/europetpc-digital-services-act-comments.pdf
[4] https://www.acm.org/binaries/content/assets/public-policy/acm-europe-tpc-dsa-comments.pdf
[5] https://www.acm.org/binaries/content/assets/public-policy/europetpc-comments-digital-principles.pdf
[6] https://www.acm.org/binaries/content/assets/public-policy/acm-europe-tpc-cyber-reslience-comments-pdf
[7] https://www.acm.org/public-policy/public-policy-statements

Feedback

Section	Feedback	Notes
General Feedback	1. Scalability Considerations: The guidelines should include recommendations for SMEs, as implementing some of the proposed measures may be resource-intensive. 2. Cross-Border Data Transfers: Further procedural clarity is needed for pseudonymisation when transferring data across jurisdictions with differing privacy laws. Cross-border data transfer is a challenging problem that is faced when dealing with emergencies and crisis response in the European Union. 3. Monitoring and Auditing: Establishing periodic audits and real-time monitoring mechanisms is recommended to ensure ongoing effectiveness of pseudonymisation. 4. Unlearning and Pseudo Unlearning: The concept of *unlearning* in AI and data privacy refers to the ability to remove specific data points from a trained model without compromising the overall integrity of the model. *Pseudo-unlearning* is a weaker form where traces of the original data may still exist, but efforts are made to obscure them. The guidelines should address how pseudonymisation interacts with these concepts, particularly in the context of AI-driven systems where complete data removal may not always be feasible. Consideration should be given to legal and technical challenges in implementing true unlearning mechanisms. 5. A scalable technique for implementing the guidelines to ensure the effort is resourced and constraint-aware should be added. This will allow gradual ratification of the guidelines even for Subject Matter Experts (SMEs), which is necessary for European digital sovereignty.	These additional considerations would improve the guidelines' applicability and robustness in real-world implementations.

EXECUTIVE SUMMARY	Although the guidelines are aimed at controllers and processors, the summary appears to focus only on the controllers' role. ACM Europe TPC suggests the relevance of the guidelines to processors is identified in the summary to address this oversight.	This is a useful summary that highlights the EDPB's position on pseudonymisation in relation to the GDPR, its general obligations, and its emphasis on risk reduction.
Introduction	Apart from the identified aims, the guidelines should also consider advice to controllers and processors about best practices after pseudonymisation has been implemented and mitigations in the event of potential re-identification for the pseudonymised data (since it is treated as personal data as per GDPR).	The guidelines' aims are defined as defining pseudonymisation, showing how controllers and processors can use pseudonymisation, and implementing pseudonymisation.
2 Definitions and legal analysis	No Comment	
2.1 Legal definition of pseudonymisation	No Comment	

2.2 Objectives and advantages of pseudonymisation	No Comment	
2.2.1 Risk reduction	No Comment	
2.2.2 Analysis of pseudonymised data and planned attribution	No Comment	
2.3 Pseudonymisation domain and available means for attribution	Since this considers the prospect of attempts to access data without authorisation, the guidelines should also consider the likelihood of accidental or intentional release of the pseudonymised dataset in the public domain, the World Wide Web, and potentially on the Dark Web. The guidelines should consider a potential safeguard for such a possibility in the form of first-order pseudonymisation within a single organisation unit and second-order pseudonymisation to authorised third parties.	
2.4 Meeting data-protection requirements using pseudonymisation	The consideration given to expanding the role of the controller from an individual to multiple individuals and potentially a collective of individuals is highly relevant. As the complexity, volume, and importance of data in most organisational functions increases, the specialised role of a pseudonymising controller, as identified here, is likely to prove crucial to implementing these guidelines.	

2.4.1 Pseudonymisation as an effective measure for data protection by design and by default	To limit the prospect of accidental or intentional re-constitution or re-identification of the original value of the attributes, ACM Europe TPC recommends using second- or third-order pseudonymisation, each with built-in safeguards to strengthen the pseudonymisation domain.	
2.4.2 Ensuring a level of security appropriate to the risk	No Comment	
2.4.3 Pseudonymisation as a supplementary measure for third country data transfers	No Comment	
2.5 Transmission of pseudonymised data to third parties	No Comment	
2.6 Implications for the rights of the data subjects	No Comment	
2.7 Unauthorised reversal of pseudonymisation	No Comment	

3 Technical measures and safeguards for pseudonymisation	The measures and safeguards defined here overlook the prevalence of practices related to the distillation and generation of synthetic data from a larger dataset. Both of these practices retain the essential characteristics of the original dataset and are likely to gain further currency as the discourse on ‘peak data’ becomes commonplace. These practices have two potential use cases relevant to these guidelines: permissible and authorised use of the pseudonymised dataset and unauthorised use of the pseudonymised dataset. In case of permissible, authorised use of the pseudonymised dataset for distillation and synthetic data generation, the currently promulgated measures need to be extended to identify suitable measures, boundaries of the pseudonymisation domain, and the role of controllers and processors in ensuring legal and legible uses of the underlying pseudonymised dataset. In case of unauthorised use of the pseudonymised dataset, for scenarios such as the transfer of the pseudonymised data to authorised third parties and potentially outside the EEA, these measures need to consider prevention and mitigation strategies to restrict how practices such as distillation and synthetic data generation could enable the third parties to use and establish commercial gain from the pseudonymised datasets in ways not previously envisioned. ACM Europe TPC recognises that such practices or uses may be outside the purview of these guidelines. However, given data science practitioners' increased visibility, acceptance, and adoption of these practices, their risks to underlying pseudonymised datasets need	

	to be better understood and subjected to detailed and critical investigation. ACM Europe TPC recommends extending the measures to include pseudonymised dataset use for distillation and synthetic data generation, defining legal and permissible use cases. That item is clear in certain Large Language Model cases where distillation was used to harvest training data and introduce it in an AI system or AI artifact.	
3.1 Pseudonymising transformation	No Comment	
3.1.1 Structure of the pseudonymising transformation	No Comment	
3.1.2 Types of pseudonymising transformations	K-anonymisation (e.g. generalisation) might be good to mention in this section.	
3.1.3 Modification of original data necessary for the objectives of pseudonymisation	No Comment	
3.1.4 Pseudonymisation in the course of data collection	No Comment	

3.2 Technical and organisational measures preventing unauthorised attribution of pseudonymised data to individuals	No Comment	
3.2.1 Preventing reversal of the pseudonymising transformation	ACM Europe TPC recommends relying on stronger cryptographic methods and suggests key rotation strategies and out-of-bound key distribution strategies to prevent brute-force attacks on pseudonymised datasets.	This can help maintain long-term security effectiveness. Yet addressing the Q day/ Quantum day has not been analysed and might require revisiting for the guidelines to stay relevant, applicable, and current. ACM Europe TPC recommends adding a follow-up to address the guidelines' soundness in case the quantum day materialisation takes place.

3.2.2 Securing the pseudonymisation domain	While the pseudonymisation domain concept is well-defined, additional measures should be included to prevent unauthorized actors from correlating pseudonymised data with external datasets for re-identification.	Ensuring strict controls on data linkage would mitigate the risk of data correlation attacks and reduce the chances of re-identification of targets.
3.3 Linking pseudonymised data	No Comment	
3.3.1 Controlling the scope for the linkage of pseudonymised data	No Comment	
3.3.2 Linking data pseudonymised by different controllers	ACM Europe TPC recommends expanding the outline for best practices for securely linking pseudonymised data from different sources while maintaining privacy and security.	This would be beneficial for research and regulatory compliance scenarios.
3.4 Summary of procedures for pseudonymisation	Where paragraph 131 specifies that a method is 'used in order to guarantee that the personal data are not attributed', it would be helpful either to moderate that (e.g. 'minimise the risk to an acceptable level', cross-referencing an appropriate definition), or to provide a pragmatic technical definition or methodological approach for 'guarantee', or to provide a footnote expressing how that could practically be interpreted. This is because 'guarantee' is a strong term, and a concern would be that it would often be challenging to demonstrate that this level had been met. Proposing concrete tests in some examples in the Annex would be helpful.	

Annex – Examples of the Application of Pseudonymisation	The Annex provides valuable real-world applications, but additional examples should be included to demonstrate pseudonymisation's role in AI and machine learning contexts. Additional practical examples could include: 1. Federated Learning and Privacy-Preserving AI - Demonstrating how pseudonymisation can be applied when training AI models across decentralized datasets without compromising personal data. 2. Healthcare Data Sharing - Illustrating pseudonymisation techniques for sharing patient data across institutions while ensuring compliance with GDPR and avoiding re-identification risks. 3. Smart Cities and IoT - Exploring the role of pseudonymisation in anonymising data collected from smart city sensors to protect citizen privacy. 4. Financial Data Aggregation - Showcasing how pseudonymisation supports secure sharing of financial transactions among regulatory bodies and fraud detection agencies. 5. Blockchain and Decentralized Data Privacy - Examining how pseudonymisation can be used in blockchain applications to protect user identities while ensuring data integrity and traceability. 6. AI Agents and Automated Decision-Making - Exploring how pseudonymisation can be applied to AI-driven decision-making processes to balance privacy protection and model interpretability. 7. 'Minimising' is potentially a pragmatic term. In this domain, practitioners find that in some cases it can be impractical to guarantee that no residual risk remains, given that so many of our datasets contain extensive biometrics	This would make the guidelines more applicable to modern data-driven environments, with clear examples of domains and scenarios for applying them.

Example 1: Data minimisation and confidentiality in internal analysis	No Comment	
Example 2: Separation of functions allowing for data minimisation, purpose limitation, and confidentiality	No Comment	
Example 3: Data minimisation and purpose limitation in the course of external analysis	No Comment	
Example 4: Safeguarding identity – confidentiality and accuracy	No Comment	
Example 5: Secondary use for research	Secondary use cases are crucial, but the guidelines should include examples of risk assessment methods to determine the appropriateness of reusing pseudonymised data in research.	
Example 6: Reduction of confidentiality risks	This section could benefit from additional best practices on how to mitigate confidentiality risks when handling large-scale datasets. Examples of appropriate	

	tests or methods to establish an acceptable level of residual risk would be welcome.	
Example 7: Risk reduction as a factor in the balancing of interests, and ascertainment of compatibility of purposes	The criteria for balancing interests should be more clearly defined, including examples of situations where risk reduction justifies further data processing.	
Example 8: Risk reduction justifying further processing	Including specific methodologies to assess risk reduction effectiveness would make this example more actionable.	
Example 9: Supplementary measure	No Comment	
Example 10: Granting access rights to pseudonymised data	No Comment	

Consulted References

- European Data Protection Board. *Guidelines 01/2025 on Pseudonymisation*. EDPB, 2025, https://edpb.europa.eu/sites/default/files/files/document/pseudonymisation_guidelines_2025.pdf.

- European Union. *General Data Protection Regulation (GDPR) (EU) 2016/679*. Official Journal of the European Union, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

- European Union. *Directive (EU) 2016/680 - Law Enforcement Data Protection Directive*. Official Journal of the European Union, 2016,

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.

- European Union. *Directive 2002/58/EC - ePrivacy Directive*. Official Journal of the European Union, 2002, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058.

- European Union. *Regulation (EU) 2018/1725 - Protection of Personal Data by EU Institutions*. Official Journal of the European Union, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725.

- European Union. *Directive (EU) 2019/770 - Digital Content and Services Directive*. Official Journal of the European Union, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770.

- European Union. *Directive 95/46/EC (Repealed) - Data Protection Directive*. Official Journal of the European Union, 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

- European Network and Information Security Agency (ENISA). *Pseudonymisation Techniques and Best Practices*. ENISA, 2021, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

- Article 29 Data Protection Working Party. *Opinion on Anonymisation Techniques*. European Commission, 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

- National Institute of Standards and Technology (NIST). *Special Publication 800-122 - Guide to Protecting the Confidentiality of PII*. NIST, 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.