The Centre for Information Policy Leadership Response to the European Data Protection Board's Public Consultation on Draft Guidelines 01/2025 on Pseudonymisation

The Centre for Information Policy Leadership (CIPL)[1] appreciates the opportunity to comment on the European Data Protection Board (EDPB) Draft Guidelines 01/2025 on Pseudonymisation. CIPL commends the EDPB's efforts to clarify the use and benefits of pseudonymisation for controllers and processors in the EU.

CIPL has consistently emphasised that pseudonymisation plays a vital role in data protection, by reducing the risk of exposing personal data and sensitive data to unauthorised third parties and threat actors.[2]

More broadly, pseudonymisation enables organisations to ensure personal data is protected when shared internally and with third-party recipients in situations where it is not possible or necessary to fully anonymise datasets. In clinical trials, for example, pseudonymisation is used to analyse patient data for research purposes without compromising the identity of participants. Where a patient's data needs to be revisited due to adverse effects or for follow-up treatments, it remains possible for approved parties to re-identify the data.

In this context, CIPL welcomes the EDPB's explicit recognition that pseudonymisation is a technical and organisational measure that helps controllers and processors mitigate risks to data subjects, which, as such, does not require a separate legal basis.[3] We caution not to interpret this to mean that in cases where consent is the legal basis, separate consent would be required to create the pseudonymous data.

CIPL further supports the EDPB's acknowledgement that pseudonymisation is an appropriate and effective safeguard that controllers and processors can use to comply with key data protection principles under the GDPR, such as data minimisation and confidentiality, while also serving as an effective tool for ensuring data protection by design and by default.[4]

This being said, CIPL has identified several topical areas of concern in the Guidelines and offers targeted recommendations for the EDPB's consideration. Our comments are set out in seven sections:

---

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] See CIPL's PETs paper for our research on privacy-enhancing techniques and tools, "Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age", December 12, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

[3] EDPB Guidelines 01/2025, para 23.

[4] ibid para 3 and 45.

I. Timing of the draft Guidelines.
II. The complexity and lack of readability of the draft Guidelines;
III. Pseudonymisation and anonymisation;
IV. Assessing and measuring pseudonymisation;
V. Data subject rights;
VI. Data transfers; and
VII. The role of Privacy-Enhancing Technologies (PETs).

In the context of the EDPB Draft Guidelines 01/2025, CIPL recommends to:

- **Delay the finalisation of the Guidelines until the CJEU issues its judgment in the SRB v. EDPS case.** To provide legal clarity, the final Guidelines should be published after the Court of Justice issues its decision on this case. The Guidelines should adopt a risk-based approach to pseudonymisation and anonymisation, focusing on the data holder's perspective, to encourage responsible data use.
- **Simplify the final Guidelines to improve clarity and accessibility, particularly for SMEs.** Simplifying the language and including practical tools and clear examples from a wide range of industries will enable businesses to more readily understand their obligations and the opportunities of pseudonymisation.
- **Clarify and appropriately differentiate between the standards and expectations for anonymisation and pseudonymisation**. To ensure consistency and clarity, the Guidelines should recognise their distinct purposes and varying levels of risk mitigation. This will help avoid ambiguity, reduce potential inconsistencies, and provide clearer guidance to organisations. Guidance for pseudonymisation and anonymisation should be combined.
- **Provide more flexible and practical criteria for assessing pseudonymisation effectiveness**. The current requirements and lack of clarity on what constitutes "reasonable means" for re-identification may discourage organisations from adopting pseudonymisation. The EDPB should provide clearer guidance, including examples of techniques, resources, costs, and legal processes to aid the assessment.
- **Expand on the benefits of pseudonymisation for privacy compliance, particularly in relation to data subject access requests**. The Guidelines should reconsider whether pseudonymous data may be excluded from such requests when it can no longer be linked to a specific individual and the obligations of controllers to inform data subjects.
- **Remove overly prescriptive conditions related to data transfers, especially those that impose new obligations beyond what is outlined in the GDPR.** The Guidelines should focus on avoiding impractical requirements and refrain from introducing obligations already addressed in existing EDPB transfer guidelines.
- **Address how PETs can be integrated with pseudonymisation in the final Guidelines, recognising their role as important technologies that can complement and strengthen pseudonymisation.** By providing clear guidance on how PETs can complement pseudonymisation, the EDPB would encourage the adoption of PETs, support responsible data use and drive innovation within the privacy landscape.

I. Timing

CIPL believes that the timing of the draft Guidelines is of concern. The Guidelines were published while the SRB v. EDPS case, which is pivotal to pseudonymisation, is still pending appeal. The Guidelines were also published before Advocate General Spielmann's Opinion on this case,[5] which presents a legal interpretation that fundamentally challenges the arguments presented in the case in front of the first instance Court. The outcome of this case will have a significant effect on the draft Guidelines at hand, and thus, CIPL emphasises that the Guidelines should be built on legal clarity, which can only be achieved after the Court of Justice issues its decision on this case.

In the Guidelines, the EDPB, in accordance with the GDPR, takes the view that pseudonymous data is considered personal data where it can be combined with additional information by means reasonably likely to be used by the controller or a third party, regardless of whether the pseudonymous data and the additional data are held by separate parties.[6] However, the Guidelines go beyond the GDPR and state that even where the additional information has been removed, the pseudonymous data only becomes anonymous if it satisfies the test for anonymity.[7]

This is not consistent with the position of the EU General Court in SRB v. EDPS, which ruled that determining whether data has been anonymised should be assessed by the controller from the perspective of the data holder or recipient.[8] In addition, the Advocate General now opined that pseudonymised data shared with a recipient is not automatically personal data for the recipient, and that an assessment is required by the pseudonymising controller about whether the recipient has reasonable means at its disposal (e.g., legal or technical) to identify the individuals concerned.[9] Such discrepancy between the draft Guidelines and developing case law creates significant legal uncertainty for organisations about when personal data will be considered anonymous.

CIPL strongly recommends that the EDPB delays the finalisation of the Guidelines until the CJEU has issued its final judgment in the EDPS v. SRB case. We further encourage a risk-based approach to determining the threshold for pseudonymisation and anonymisation, in line with the General Court ruling in SRB v. EDPS and the recent Advocate General's Opinion. Rather than evaluating re-identification risk broadly, the focus should be on the data holder's perspective. This approach would not only enhance legal clarity but also facilitate greater data use, thereby fostering innovation and encouraging responsible data practices.[10]

II. Complexity and Lack of Accessibility of the Draft Guidelines

---

[5] Opinion of Advocate General Spielmann in Case T-557/20, 26 April 2023, *Single Resolution Board v. European Data Protection Supervisor*, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=295078&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=28929862.

[6] EDPB Guidelines 01/2025, para 22.

[7] ibid para 22.

[8] Case T-557/20, 26 April 2023, *Single Resolution Board v. European Data Protection Supervisor*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020TJ0557%20%20%20%20%20, paras 97 and 100.

[9] Opinion of Advocate General Spielmann in Case T-557/20, 26 April 2023, *Single Resolution Board v. European Data Protection Supervisor*, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=295078&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=28929862 (para 96).

[10] This would also remain consistent with Recital 29 GDPR which states that pseudonymisation should be possible within the same controller. If the process required considering every potential third party, pseudonymisation would often not be feasible within the same controller.

The EDPB plays a crucial role in ensuring legal clarity by providing guidance to controllers and processors in compliance with the GDPR in an already complex regulatory landscape. Therefore, it is important that the Guidelines are accessible, practical, and easy to understand, particularly for smaller organisations that do not have the resources for extensive legal support.

In contrast, the current draft Guidelines are lengthy, overly complex and, in parts, repetitive. The Guidelines consequently fall short of actually providing clarifying guidance for the appropriate use and benefits of pseudonymisation for controllers and processors. For example, the considerations on how controllers should manage "quasi-identifiers" are complex,[11] difficult to follow and could ultimately disincentivise the application of pseudonymisation especially for organisations with more limited resources.[12] The Guidelines also go beyond the requirements of the GDPR and existing case law in some instances, introducing a level of uncertainty.

Furthermore, the Guidelines create new terms, such as "pseudonymisation domain". We encourage the EDPB to rely on the terms already present in the GDPR or defined elsewhere in the EU law, to ensure consistency and legal clarity.

For example, the Guidelines introduce a complex concept of a "pseudonymisation domain". While this concept aims to enhance security, the Guidelines should express that this concept is not a legal concept and should, therefore, not create any new obligations.

The Guidelines also enforce a strict and, in some instances, practically unattainable separation between individuals who have access to pseudonymous data but should not be able to re-identify it. For instance, re-identification could potentially occur by combining pseudonymous data with publicly available information, which is accessible to anyone, including those within the defined pseudonymisation domain, through standard internet access. Enforcing an absolute separation in such cases becomes practically challenging.

A better approach would be to acknowledge that separation can be more effectively managed within a role- or capacity-based framework. Implementing appropriate technical, organisational, contractual, and policy measures to govern data access and usage within the pseudonymisation domain would support this approach rather than enforcing a strict and absolute separation of personnel and information in all cases.

Finally, the Guidelines rightfully emphasise that controllers should conduct risk assessments when applying pseudonymisation, but it is not clear whether it is compulsory for such assessments to systematically refer to this "pseudonymisation domain" concept. The Guidelines should clarify that in most cases, where the processing does not constitute high-risk processing, such risk assessments are not required.

Given that pseudonymous data holds significant potential to drive the use of data benefiting society at large, especially in research and AI, organisations need clear accessible guidance and legal certainty to innovate. We respectfully urge the EDPB to consider simplifying the final Guidelines with more practical examples that can support organisations, particularly SMEs, in more easily assessing compliance.

III. Pseudonymisation and Anonymisation

[11] See for example the approach outlined in EDPB Guidelines 01/2025, para 103.
[12] EDPB Guidelines 01/2025, paras 101-104.

CIPL regrets that the draft Guidelines have been published separately from the planned guidelines on anonymisation. This distinction is problematic, given the inherent connection and conceptual similarities between these two data processing techniques. Anonymisation and pseudonymisation both aim to limit the ability to identify individuals, and the criteria for evaluating their effectiveness largely overlap. Issuing separate guidelines could create inconsistencies, confusion, and complicate practical implementation. CIPL notes that there are excellent examples for the benefit of setting out common guidance such as from the Irish Data Protection Commissioner,[13] and the UK Information Commissioner's Office[14].

The draft Guidelines impose abstract anonymisation standards on pseudonymisation that would be challenging to implement in practice. For instance, the Guidelines state that for pseudonymisation to be effective, those handling pseudonymised data must not be able to identify individuals in "other contexts" based on what they have learned from the data.[15] However, the Guidelines do not define or offer examples of what constitutes "other contexts."

The standards for anonymisation are also applied to the interpretation of pseudonymisation in the Guidelines' requirement that, for pseudonymisation to be an effective security measure, the process must ensure that the additional information required for re-identification should not be obtainable with reasonable effort.[16]

First, this "reasonable effort" standard, while relevant to anonymisation, creates a conceptual tension. If the additional data is indeed inaccessible with reasonable effort, then it raises the question of whether such data should instead be considered anonymous. Recital 26 GDPR and CJEU case law demonstrate that assessing whether an individual could be identified directly or indirectly, considering all means reasonably likely to be used, is a legal test for anonymisation, not pseudonymisation.[17]

Secondly, the term "identify" is unclear in the context of pseudonymisation. In anonymisation, "identification" is typically evaluated through risks like "singling out," "linkability," and "inference." However, these concepts do not directly apply to pseudonymisation. Pseudonymous data may still contain unique identifiers that allow for the "singling out" of an individual within the dataset. CIPL encourages the EDPB to clarify this issue and ensure that the Guidelines properly distinguish between the standards and expectations for anonymisation and pseudonymisation, acknowledging their distinct purposes and varying levels of risk mitigation.

Furthermore, when applied to the pharmaceutical sector, the EDPB's conceptual approach to pseudonymisation may prove challenging to implement. Clinical trial data are pseudonymous by the hospital or site, but the data remain highly detailed in the hands of the study sponsor and its processors. This level of detail is essential to assess the risks and benefits of treatment based on the

---

[13] Guidance Note: Guidance on Anonymisation and Pseudonymisation, Data Protection Commission (DPC), available at https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf.

[14] Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, Information Commissioner's Office (ICO), available at https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf.

[15] EDPB Guidelines 01/2025, para 47.

[16] ibid para 60.

[17] See for example, C-582/14 (*Patrick Breyer v. Bundesrepublik Deutschland)*, Case T-799/17 (*Scania and Others v. European Commission*), and Case C-604/22 (*IAB Europe v. Gegevensbeschermingsautoriteit).*

demographic characteristics of clinical trial participants, which may, in some cases, allow individuals to be re-identified even though direct identifiers have been removed.

Additionally, the EDPB's standard for pseudonymisation may conflict with the long-established *lex specialis* standards outlined in the EU Clinical Trial Regulation (CTR) and Good Clinical Practice (GCP). Since CTR and GCP pseudonymisation requirements are legally mandated, they take precedence over the EDPB's Guidelines. However, the Guidelines could still adversely affect secondary research conducted under Article 89(1) GDPR, where no specific pseudonymisation requirements are defined under health research laws. A restrictive interpretation of what constitutes pseudonymous data, as proposed in the draft Guidelines, could impede research by rendering the data either unusable or unsuitable for research.

IV. Assessing and Measuring Pseudonymisation

The Guidelines' approach to evaluating the effectiveness of pseudonymisation could create unnecessary complications for organisations, due to the challenging nature of the assessment process and the rigid criteria applied. If proving that data are pseudonymous becomes difficult in practice, it will discourage organisations from adopting pseudonymisation practices.

Firstly, the Guidelines require controllers to assess re-identification based on "reasonably likely to be used" methods,[18] but they offer limited guidance on what qualifies as "reasonable means." CIPL encourages the EDPB to provide more concrete examples, including on potential techniques, re-identification costs, and the legal processes that would be considered "reasonable" for accessing information that could aid re-identification. Additionally, it should be made clear that illegal means deployed by bad actors cannot factor into considerations of "reasonably likely to be used".

Secondly, CIPL is concerned about the EDPB's use of absolute criteria for measuring pseudonymisation effectiveness. The rigid requirements, such as the complete inability of third parties to reconstitute original values or link the pseudonymous data to other data related to the same individual,[19] conflict with the Guidelines' general recognition of a "reasonable likelihood" approach. CIPL advocates for a more flexible approach, focused on the "state-of-the-art" at the time of pseudonymisation, consistent with Article 32 GDPR, to better balance data protection and innovation.

V. Data Subject Rights

CIPL also welcomes the recognition that pseudonymisation can enable controllers to rely on legitimate interests as a legal basis for processing personal data and help to establish the compatibility of further processing.[20] We encourage the EDPB to identify other benefits from a privacy compliance standpoint, such as the possibility of excluding pseudonymous data from data subject access requests when it can no longer be linked to a specific individual. This is consistent with Recital 57 GDPR, which indicates that a data controller should not be obliged to acquire additional information in order to identify a data subject for the sole purpose of complying with access requests.

---

[18] EDPB Guidelines 01/2025, para 22.
[19] ibid para 43.
[20] ibid pg 3.

Moreover, under Article 11(1) GDPR, when controllers process personal data that does not require identifying data subjects, they are not obligated to maintain, acquire, or process additional information to identify the data subject solely for GDPR compliance. However, the draft Guidelines go beyond the GDPR and seem to impose extra requirements on controllers to prove they cannot identify the data subject. These include demonstrating they are unable to lawfully access additional information that could attribute the data to a specific individual, and that they cannot reverse the pseudonymisation with the help of another controller.[21] These abstract standards will make it difficult for controllers to rely on Article 11 GDPR in practice, most prominently, where the controller does not (or has never) required the re-identification of data.

Similarly, while we acknowledge the importance of data subjects exercising their rights, we question the proposal to oblige controllers to indicate to the data subjects how they can obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity.[22] This goes beyond the text of Article 11(2) GDPR, which only requires controllers to inform data subjects when they cannot identify them. It is unclear how controllers could fulfil this obligation without re-identifying the data to link a pseudonym to an individual, which would undermine the effectiveness of pseudonymisation. In addition, the Guidelines' suggestion that controllers provide pseudonyms directly contradicts Article 11(2) GDPR which places the responsibility on the data subject to supply additional information to enable identification.

Lastly, the Guidelines appear to set the unrealistic expectation that controllers will always be able to act on pseudonymisation keys provided by data subjects.[23] This does not, for example, take data retention schedules of controllers into consideration, creating unrealistic expectations beyond what is intended in Chapter III of GDPR.

Article 11(1) GDPR clearly states that controllers are not obligated to collect and process additional information to identify the data subject solely for GDPR compliance. Controllers should therefore not be made to re-identify pseudonymous data for the sole purpose of complying with the Regulation, in direct conflict with the explicit intent of Article 11(1).

VI. Data Transfers

CIPL welcomes the recognition that pseudonymisation can help establish essential equivalence for data transfers.[24] However, the conditions listed are overly prescriptive and add new obligations which go beyond Chapter V GDPR. For example, the Guidelines require controllers to assess the potential access or ability of public authorities in the recipient country to obtain certain information, even if such actions might infringe on local legal norms.[25] It is not feasible for private companies to ascertain whether or how public authorities in a third country might unlawfully access specific types of information.

More broadly, since the assessment of the rule of law and adequate protections in third countries is already addressed in existing EDPB transfer guidelines, we question the necessity of revisiting this issue in the current Guidelines in a way that seems more burdensome than what is outlined in those guidelines.

---

[21] ibid para 77.
[22] ibid para 79.
[23] ibid para 78.
[24] ibid para 63.
[25] ibid para 65.

VII. The Role of Privacy-Enhancing Technologies (PETs)

Despite increased attention to PETs by regulators and organisations alike,[26] and growing adoption by business across all sectors, the current draft Guidelines make no reference to PETs nor do they address their benefits to strengthen the protection of personal or sensitive data.[27] Specifically, the Guidelines do not consider whether PETs could be employed alongside pseudonymisation to enable the recipient of the pseudonymous data to demonstrate that reidentification is highly unlikely or even impossible, ensuring that the data remains effectively anonymous in their hands. The Guidelines also do not cover how pseudonymisation can practically be applied in unstructured data. This is a missed opportunity to be forward looking in a fast-moving technology environment.

For example, in the case of data transfers, PETs such as trusted execution environments could be integrated with pseudonymisation to offer a robust solution for protecting data as it moves across different jurisdictions. Similarly, differential privacy techniques could be applied to pseudonymous data, introducing noise that makes re-identification virtually impossible, even when combined with other available information. By combining pseudonymisation with PETs, organisations can significantly reduce the risk of re-identification and enhance overall data protection for individuals.

We encourage the EDPB to explicitly recognise the role of PETs in the Guidelines, not merely as supplementary tools but as essential technologies that can work in tandem with pseudonymisation and, in some cases, even replace pseudonymisation. The Guidelines should also acknowledge the relevance of PETs within the context of AI applications. PETs are increasingly critical for enabling the responsible development and deployment of AI, particularly in training models with pseudonymous data while minimising re-identification risks and fostering innovation in this crucial field. Official regulatory guidance addressing PETs in the context of specific legal obligations or concepts (such as pseudonymisation or anonymisation) will significantly drive their adoption. In fact, there are many examples of tokenisation approaches that resemble pseudonymisation, and understanding how the Guidelines would apply to these methods would be helpful. By positioning PETs as a complementary layer of protection, the EDPB can provide organisations with a more comprehensive and practical solution to data protection. This would act as an important safeguard, ensuring that pseudonymous data, even when transferred or shared, remains shielded from the risk of re-identification.

Finally, on AI more broadly, generative AI typically relies on stacking user queries to ensure consistency, such as linking a follow-up question to a prior response. While the AI might identify a device rather than an individual user, the CJEU in *Breyer* ruled that device and network identification data qualify as personal data. It would be beneficial if the Guidelines could clarify whether such data should be treated as pseudonymised personal data.[28]

---

[26] See Privacy-enhancing technologies (PETs), Information Commissioner's Office (ICO), June 2023, available at https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf. See also AI how-to sheets, Commission Nationale de l'Informatique et des Libertés (CNIL), June 7, 2024, available at https://www.cnil.fr/fr/ai-how-to-sheets. See also Emerging privacy-enhancing technologies: Current regulatory and policy approaches, Organisation for Economic Co-operation and Development (OECD), March 2023, available at https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html.

[27] See some examples and use cases of PETs in practice in CIPL's "Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

[28] This also applies to backpropagation, a process in neural networks where errors are sent backwards through the network to adjust weights and improve the model's accuracy in future predictions.