Guidelines 01/2025 on Pseudonymisation

Comments by Selbstregulierung Informationswirtschaft e.V. (SRIW), with specific regards to the Draft Code of Conduct on Pseudonymization by GDD-Bitkom-SRIW

March 2025

Guidelines 01/2025 on Pseudonymisation

Herausgeber

Selbstregulierung Informationswirtschaft e.V.
Großbeerenstraße 88
10963 Berlin
https://sriw.de

+49 (0)30 30878099-0
info@sriw.de

Amtsgericht Berlin Charlottenburg
Registernummer: VR 30983 B
USt-Nummer: DE301407624
Deutsche Bank AG
IBAN: DE33 1007 0000 0550 0590 00

Vorstandsvorsitz
Jörn Wittmann

Geschäftsführer
Frank Ingenrieth

1 About the Author

The Selbstregulierung Informationswirtschaft e.V. (SRIW)[1] is a non-profit association with European focus.

Ever since its establishment in 2011 and as the primary of a pan-European ecosystem, SRIW assembled first-hand experiences in the establishment of trusted self- and co-regulatory instruments in the information economy. Additionally, the association benefits from its independent subsidiaries across Europe and its diverse and constantly growing membership.

The everyday business of the association centres on harmonising industry practices with social demands and political requirements. The mechanism considered fit for purpose is balanced and monitored self- and co-regulatory frameworks facilitating effective data and consumer protection. SRIW strives to collect and amplify valuable experiences to improve the necessary and independent structures required for the development, approval and monitoring of Codes of Conduct. By actively connecting experts and bringing together interested stakeholders, SRIW serves as a forum for exchange and discussions, providing the impetus for kicking-off frontrunner initiatives.

The ecosystem includes SCOPE Europe srl[2], most probably Europe's leading independent Monitoring Body. SRIW's subsidiary became known in supporting the first officially approved transnational Code of Conduct, i.e. EU Data Protection Code of Conduct for Cloud Service Providers[3], and becoming the first ever accredited transnational Monitoring Body under Article 41 GDPR as well as the first Monitoring Body which was accredited by more than one data protection supervisory authority and for more than one Code of Conduct.

[1] https://sriw.de
[2] https://scope-europe.eu
[3] https://eucoc.cloud

2 Preliminary Note

We welcome the **EDPB Guidelines 01/2025 on Pseudonymisation** as an important step toward reinforcing pseudonymisation as a key safeguard under the GDPR. By clarifying its role in data minimisation, security, and purpose limitation, the Guidelines provide guidance for controllers and processors.

We recognize the significant alignment between the Guidelines and the GDPR Code of Conduct for Pseudonymisation (Pseudonymisation-CoC), an industry-led initiative that has contributed to the practical implementation of pseudonymisation techniques.[4] Given the complementary nature of both instruments, we believe that further incorporating practical operational insights from the Pseudonymisation-CoC into the Guidelines would enhance their effectiveness and promote broader adoption.

To this end, we respectfully suggest the following key considerations:

- **Practical implementation**: The Pseudonymisation-CoC provides sector-specific methodologies for applying pseudonymisation, whereas the EDPB remains more general.
- **Ensure practical feasibility by aligning regulatory requirements with industry capabilities**.
- **Allow progressive adaptation by organisations before full enforcement**.
- **Identify compliance challenges early, ensuring consistent application across Member States**.
- **Further integrate operational insights and recommendations from the Pseudonymisation-CoC**

As an organisation deeply engaged in the development and implementation of GDPR compliance frameworks, we recognise the significant progress made in defining pseudonymisation's legal and technical dimensions and to ensure effective and harmonized implementation across diverse sectors encourage a co-regulation approach.

[4] See the **Pseudonymisation-CoC Project**: https://sriw.de/projekte-kodizes/pseudonymisierung ; the current version of the Pseudonymisation-CoC is available here: https://sriw.de/fileadmin/sriw/files/pseudonymization/CoC_GDPR_pseudonymisation_v1-1-1.pdf

3 Introduction

On January 16, 2025, the **European Data Protection Board (EDPB)** published its Guidelines 01/2025 on Pseudonymisation, providing a framework for the role of pseudonymisation under the **General Data Protection Regulation (GDPR)**. The Guidelines reaffirm the importance of pseudonymisation as a data protection safeguard, particularly concerning data minimisation, security, and purpose limitation. They also clarify its legal implications and offer guidance on its practical implementation.

Prior to these regulatory guidelines, **industry-led initiatives** had already developed concrete frameworks for the operationalisation of **GDPR-compliant pseudonymisation**. The GDPR Code of Conduct for Pseudonymisation (hereafter, Pseudonymisation-CoC), developed by **Bitkom**, the **Society for Data Protection and Data Security (GDD)**, and **Selbstregulierung Informationswirtschaft (SRIW) e.V.**, was introduced under the Privacy Focus Group of the "*Security, Protection, and Trust for Society and Business*" platform at the **2019 German Digital Summit**. The Code of Conduct aims to provide an industry-wide standard for pseudonymisation, offering a practical compliance framework to assist organisations in meeting GDPR obligations.

Although the EDPB Guidelines and the Code of Conduct share fundamental principles, differences exist in their interpretation, and application. While the Guidelines appear to incorporate several key concepts first developed within the industry-led Code of Conduct, they remain more theoretical and would benefit from other key concepts developed in the Code of Conduct. The Code of Conduct adopts a risk-based and operational approach, ensuring practical feasibility in real-world data processing.

However, we encourage the EDPB to consider the pending EDPS v SRB judgment before finalizing the Guidelines, ensuring alignment with evolving case law. To ensure legal clarity, we recommend postponing finalisation and using the Pseudonymisation-CoC's operational approach as a key reference. We welcome further dialogue to support a practical and future-proof framework.

We submit this consultation response with the goal of contributing to the continued refinement and alignment of pseudonymisation practices across regulatory and industry frameworks. We therefore examine the EDPB Guidelines in light of the Pseudonymisation-CoC, identifying areas of alignment and opportunities for more practical benefit.

4 General Remarks

We highly welcome the EDPB Guidelines 01/2025 on Pseudonymisation as a key step in reinforcing pseudonymisation as a GDPR safeguard. The Guidelines align with industry-led efforts, particularly the Pseudonymisation-CoC, which provides valuable operational insights.

Authorities, industry and data subjects could have a strong benefited by the initiative for year, already. The authoritative procedures remain unnecessarily halted. To the knowledge of the authors, no material concerns were risen, which seems supported by the strong overlaps of the Guidelines and the draft Code. Approval procedures are paused due to concern regarding the determination of the competent authority. Implementing the Pseudonymisation-CoC as a pilot framework before issuing the EDPB Guidelines could have provided empirical insights into its feasibility, addressing technical, operational, and compliance challenges before formalising regulatory guidance.[5]

By first assessing the Code's effectiveness in everyday situations, regulators could have developed more tailored and practicable requirements, aligning legal obligations with industry capabilities. In this aspect, encouraging self- and co-regulation as a complementary tool would enhance both legal certainty and practical implementation.

4.1 Definitions and Legal Analysis

4.1.1 Legal Definition and Scope of Pseudonymisation

We appreciate the clear articulation of the legal definition of pseudonymisation under Article 4 (5) GDPR. We share the opinion that the Guidelines would benefit from integrating operational considerations from the Pseudonymisation-CoC, ensuring that organisations can easily implement pseudonymisation while meeting legal and technical requirements.

Both the EDPB Guidelines and the Pseudonymisation-CoC adhere to definition of Article 4 (5) GDPR but interpret its scope differently.

The EDPB Guidelines define pseudonymisation strictly under Article 4 (5) GDPR, emphasising that it constitutes a technical and organisational measure designed to reduce the likelihood of personal data being attributed to an individual without additional information.[6]

---

[5] For a practical analysis of the role of pseudonymization within GDPR compliance, see the following article, which discusses the Pseudonymisation CoC and its regulatory implications: SRIW presents "GDPR's 5th Anniversary Resumée – A practical resumée from a co-regulatory perspective, reflecting Codes of Conduct and Monitoring Bodies in particular", June 2023 and the document: 202306_SRIW_5th-Anniversary-GDPR_Resumee.pdf, June 2023.

[6] EDPB Guidelines, Section 1, para. 2, 3; Section 2

- Pseudonymised data remains personal data unless full anonymisation is achieved. Even if additional information is not in the same entity's possession, the potential for re-identification means the data remains within the scope of the GDPR.[7]
- The effect of pseudonymisation is to reduce the likelihood of re-identification while still allowing certain forms of data analysis.[8]

Thus, the EDPB strictly follows the legal definition provided by the GDPR but enhances it with a risk-based framework, focusing on data protection by design and by default. The Pseudonymisation-CoC also follows the GDPR definition but provides a more practical and operational perspective.

The Pseudonymisation-CoC expands the definition upon it by establishing specific conditions under which pseudonymisation effectively minimises risks.[9] A significant addition within the Code of Conduct is the concept of **functional pseudonymisation**, which adapts pseudonymisation techniques to sector-specific use cases.[10]

We therefore encourage the EDPB to draw further inspiration from the Pseudonymisation-CoC in this regard.

4.1.2 Objectives and Advantages of Pseudonymisation

We support the Guidelines' recognition that pseudonymisation contributes to risk mitigation by:

- Preventing the immediate identification of data subjects.
- Reducing the impact of unauthorised access.
- Enhancing purpose limitation by restricting unintended data linkages.

The Pseudonymisation-CoC complements this approach by providing structured methodologies for classifying and mitigating risks across different processing contexts.

The Guidelines should include a structured risk classification framework, as provided in the Pseudonymisation-CoC. Moreover, such a framework should align with the broader risk-based approach enshrined in the GDPR itself.[11] Pseudonymization plays a critical role in mitigating risks associated with data processing and should be considered as part of a holistic data protection strategy.[12] Any such

[7] EDPB Guidelines, Section 2.2.1, para. 22
[8] EDPB Guidelines, Section 2.2.1, para. 26
[9] Pseudonymisation-CoC, Section 1.2
[10] Pseudonymisation-CoC, Section 2.1.1
[11] Recitals 76, 77, 78, and 83; Articles 24, 25, 32, and 35 GDPR
[12] Article 32(1)(a), Recital 28 GDPR

risk analysis shall remain operationally feasible and integratable into already existing and implemented efforts by industry.

4.1.3 Pseudonymisation Domain and Available Means for Attribution

The introduction of the Pseudonymisation Domain concept is a valuable addition to the Guidelines, as it provides a framework for defining controlled processing environments.

The EDPB guidelines introduce the concept of a **pseudonymisation domain**,[13] which refers to the context in which pseudonymised data is processed and which parties must be prevented from re-identifying the data.[14] This is one significant adoption from the Pseudonymisation-CoC. This notion aligns with the industry's approach, which views pseudonymisation as a means of segmenting access to identifiable information rather than as a method of eliminating re-identification risk entirely.

Furthermore, the EDPB has incorporated sector-specific use cases into the Guidelines, including examples from medical research, cybersecurity, and data analytics, reflecting scenarios that were initially addressed in the Pseudonymisation-CoC.[15]

4.2 Meeting Data Protection Requirements Using Pseudonymisation

4.2.1 Pseudonymisation as a Safeguard for Data Protection Principles

The EDPB Guidelines highlight the role of pseudonymisation in ensuring compliance with:

- **Data minimisation** – Article 5 (1) (c) GDPR
- **Privacy by design** – Article 25 GDPR
- **Security obligations** – Article 32 GDPR

The Guidelines highlight that pseudonymisation should be part of a broader data protection strategy rather than being considered a standalone solution.[16] The Guidelines incorporate several key concepts originally introduced in the Pseudonymisation-CoC.

[13] Pseudonymisation-CoC, Section 2.1.4
[14] EDPB Guidelines, Section 2.3, para. 35
[15] EDPB Guidelines, Annex – Examples of the Application of Pseudonymisation and Pseudonymisation-CoC, Section 3 – Application Examples of Pseudonymisation
[16] EDPB Guidelines, Section 2.2, para. 28

The Pseudonymisation-CoC, in contrast, not only acknowledges pseudonymisation as a key privacy safeguard but also introduces concrete procedural steps for integrating pseudonymisation into organisational compliance programs.[17] These include:

- **Technical requirements for secure implementation**[18]
- **Mechanisms for preventing unauthorised attribution**[19]

Both frameworks acknowledge the importance of pseudonymisation, yet the Pseudonymisation-CoC provides clearer procedural guidance, ensuring operational certainty.

4.2.2 Lawful Processing and Pseudonymisation

A key distinction between the EDPB Guidelines and the Pseudonymisation-CoC concerns the role of pseudonymisation as a tool for lawful processing under the GDPR.

The EDPB Guidelines acknowledge that pseudonymisation can reduce risks and contribute to lawful processing under Article 6 (1) (f) GDPR (legitimate interest) and Article 6 (4) GDPR (compatibility assessment).[20]. However, they do not explicitly endorse pseudonymisation as a compliance mechanism, leaving ambiguity in how organisations can rely on it in specific processing environments.

While **Example 8** in the Guidelines aims to illustrate a scenario under Article 6 (4) GDPR, it presents an unusual case that does not align with typical industry practices.[21] In reality, most companies collect personal data primarily for customer insights, where a change of purpose is rarely required. Additionally, the inclusion of health data in the example may cause confusion, as such data would have originally been collected based on explicit consent under Article 9 (2)(a) GDPR, making the compatibility assessment under Article 6 (4) inapplicable. Since data collected based on consent cannot later rely on Article 6 (4) GDPR for further processing, the example may not provide meaningful guidance for organizations seeking clarity on pseudonymization.

By contrast, the Pseudonymisation-CoC **explicitly** promotes pseudonymisation as a means to support lawful processing and provides regulatory safeguards to ensure its effective implementation while maintaining GDPR principles.[22] The Code of Conduct outlines practical measures that enable controllers to integrate pseudonymisation into legitimate interest assessments and data compatibility

[17] Pseudonymisation-CoC, Section 2.1.3
[18] Pseudonymisation-CoC, Section 2.2.1
[19] Pseudonymisation-CoC, Section 2.1.5
[20] EDPB Guidelines, Section 1, para. 12; Section 2.3, 42
[21] Guidelines 01/2025 on Pseudonymisation, Example 8: Risk reduction justifying further processing, p. 48
[22] Pseudonymisation-CoC, Section 2.1.6

evaluations, offering greater clarity and predictability for organisations using pseudonymised data in their processing activities.

While both frameworks recognise pseudonymisation as a risk-reduction measure, the EDPB Guidelines would benefit from a clearer position on how pseudonymisation can serve as a compliance tool. Further guidance on its role in meeting legal requirements would provide greater legal certainty for organisations seeking to use pseudonymisation as a basis for processing under the GDPR. In the absence of such clarity, organizations may be reluctant to adopt or maintain pseudonymization measures, as the regulatory benefits and compliance advantages remain uncertain. This lack of legal certainty may discourage broader adoption of pseudonymization, despite its potential to enhance data protection and security.

4.2.3 Risk Assessment and Effectiveness of Pseudonymisation

The EDPB Guidelines assert that controllers must assess the risks they aim to mitigate through pseudonymisation.[23] We support the Guidelines' recognition that pseudonymisation contributes to risk mitigation by:

- The separation of identifying data from pseudonymised data[24]
- Robust technical and organisational safeguards[25]
- Contextual limitations within a processing environment[26]

The Pseudonymisation-CoC provides a structured, flexible and risk-based approach for evaluating pseudonymisation effectiveness.[27] It offers sector-specific risk classifications and practical recommendations for pseudonymisation techniques tailored to different levels of data sensitivity. Concrete by categorizing risk levels based on data sensitivity and processing context.

We acknowledge that the EDPB has adopted a risk classification approach similar to that of the Code of Conduct, even though it remains more general in its formulation. The Guidelines also remain unnecessarily vague, to what extent this additional risk analysis can be incorporated or even covered by already implemented industry procedures.

4.3 Technical measures and safeguards for pseudonymisation

The Guidelines rightly underscore the role of pseudonymisation in ensuring data protection by design and by default under Article 25 GDPR. Further elaboration on operational best practices for

[23] EDPB Guidelines, Section 2.3, para. 40
[24] EDPB Guidelines, Section 2.4, para. 44
[25] EDPB Guidelines, Section 2.4.1.1, para. 46
[26] EDPB Guidelines, Section 2.2.1, para. 27-30; Section 2.4.1.2, para. 49
[27] Pseudonymisation-CoC, Section 2.1.2

implementing pseudonymisation by design would support controllers in embedding GDPR compliance into their data processing workflows.

The Pseudonymisation-CoC introduces concrete organisational measures, including:

- **Governance framework**: The Pseudonymisation-CoC establishes organisational roles and responsibilities, including the designation of a **Pseudonymisation Officer** to oversee compliance and implementation.[28]
- **Risk-based approach**: The Pseudonymisation-CoC defines different pseudonymisation techniques depending on the sensitivity of data and the risks involved.[29]

While both frameworks agree that pseudonymised data remains personal data, the Pseudonymisation-CoC provides concrete, operational guidance on how to implement pseudonymisation in real-world settings.

The Guidelines would benefit from integrating operational considerations from the Pseudonymisation-CoC, ensuring that organisations can easily implement pseudonymisation while meeting legal and technical requirements. We therefore encourage the EDPB to draw further inspiration from the Pseudonymisation-CoC in this regard.

4.4 Internal Governance

The Pseudonymisation-CoC introduce **specific organisational roles** in the internal governance, including the **Pseudonymisation Officer**, who is tasked with overseeing pseudonymisation processes, ensuring proper implementation, and maintaining ongoing compliance.[30] As in the Pseudonymisation-CoC, the EDPB Guidelines on Pseudonymisation also emphasize that internal governance structures must incorporate distinct roles and responsibilities to maintain the integrity of pseudonymisation mechanisms while ensuring compliance with legal and technical obligations.[31]

The EDPB Guidelines outline the necessity of establishing a **Verification Centre** as a dedicated unit responsible for handling pseudonymisation and controlled re-identification, ensuring that personally identifiable information (PII) is securely stored and that pseudonyms are randomly assigned to prevent correlation across datasets.[32]

---

[28] Pseudonymisation-CoC, Section 2.1.9
[29] Pseudonymisation-CoC, Section 2.2.2
[30] Pseudonymisation-CoC, Section 2.1.9
[31] EDPB Guidelines, Section 4, para. 44
[32] EDPB Guidelines, Section 3.1.4, para. 105; Annex – Examples of the application of pseudonymisation

The EDPB Guidelines on Pseudonymisation do not specify whether the Verification Centre must be a separate unit or if its functions can be integrated into an existing role, such as the DPO. This lack of clarity may create uncertainty and lead organisations to view it as an administrative burden rather than a compliance benefit. Therefore, the Guidelines could either define its structure more clearly or assign these responsibilities to a Pseudonymisation Officer, as established in the Pseudonymisation-CoC.

4.5 Monitoring and Compliance Mechanisms

We recognise the EDPB's efforts in providing guidance on pseudonymisation as a GDPR safeguard.

The nature of these Guidelines, intentionally generic, allows for flexibility in their enforcement by DPAs across different sectors. While this decentralized approach is beneficial for applying the Guidelines in varied regulatory contexts, it risks leading to inconsistent enforcement and varying interpretations across EU Member States, depending on the discretionary authority and resources of individual DPAs.

Against this background, industry initiatives can complement the EDPB's Guidelines by offering more specific solutions. A **co-regulatory framework**, integrating independent monitoring with regulatory co-operation, could provide an additional layer of accountability, ensuring continuous alignment with evolving regulatory expectations while fostering industry-driven compliance, regardless of resources of public authorities.

In this context, the Pseudonymisation-CoC establishes a structured **framework**, requiring organisations to undergo ongoing assessments by an independent **Monitoring Body**.[33] This mechanism ensures continuous oversight, reinforcing adherence to pseudonymisation standards through regular compliance reviews, best practice evaluations, and implementation guidance. By complementing the inherently generic nature of the EDPB Guidelines such industry initiatives can positively contribute to the protection of data subjects.

This approach not only supports and enhances GDPR enforcement but also contributes to the protection of data subjects and should be encouraged in the EDPB Guidelines. Therefore, we suggest considering a co-regulatory framework to have standardized mechanism across EU Member States and ensuring practical feasibility.

[33] Pseudonymisation-CoC, Section 2.1.9.2

5 Conclusion

The EDPB Guidelines on Pseudonymisation provide a regulatory endorsement of pseudonymisation, following the spirit of the Code of Conduct and building on principles developed over the past five years. While the Guidelines align with the Code's fundamental objectives, they do not fully address the practical implementation challenges that organisations face.

Furthermore, the finalisation of the Guidelines should await the Court's decision to provide greater clarity on the scope of pseudonymisation. A clear and consistent definition, without discrepancies between the EDPB and the CJEU, is essential for legal certainty. The Advocate General's Opinion suggests that pseudonymised data may not constitute personal data for third-party recipients if re-identification is not reasonably possible. Should the CJEU confirm this, the Guidelines may require revision to ensure alignment in the legal interpretation.

In this context, the continuity between the Guidelines and the Code of Conduct is a positive development, reaffirming the Code's relevance as a compliance instrument. Moving forward, the EDPB should continue working with industry stakeholders to refine its guidance, address practical challenges, and establish clear standards for pseudonymisation effectiveness.

selbstregulierung
informationswirtschaft e.V.