Report on stakeholder event on anonymisation and pseudonymisation of 12 December 2025

1. Background

The EDPB organised a remote stakeholder event on 12 December 2025 to collect stakeholders' input on anonymisation and pseudonymisation, following the Court of Justice of the European Union ("CJEU") judgment in case EDPS v SRB[1]. The objective was to engage with stakeholders to inform the EDPB's ongoing work on its guidelines 01/2025 on pseudonymisation and forthcoming guidelines on anonymisation.

The target audience was the general public, with a focus on sector associations, NGOs, individual companies, law firms and academics. Participants were provided with a Discussion paper published prior to the event[2]. Participants were divided in four break-out rooms and all of them were able to share their views on four questions presented in the Discussion paper.

This report aims to summarise the main ideas and issues raised by participants, acknowledging that some topics were discussed in response to multiple questions. While the views expressed during the event and reflected in this report will inform the EDPB's work, the Board remains free to determine if and how perspectives shared will be incorporated in its future guidelines.

[1] Judgment of 4 September 2025 in case C-413/23 P European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB) ("EDPS v SRB judgment").

[2] The Discussion paper and background information, e.g. about the registration process and criteria for the selection of participants, are available here: https://www.edpb.europa.eu/news/news/2025/stakeholder-event-anonymisation-and-pseudonymisation-express-your-interest_en

2. Amount and nature of contributions received

Total number of participants: 115

Number of participants by category:

Business association/ company	NGO/ consumer organisation	Academia	Law office	Public sector	Other (e.g. professional association, research organisation, think tank)
61	8	14	17	7	8

3. Main outcomes of the public consultation

<u>Question 1:</u> According to the Court, the relevant perspective for assessing identifiability depends, in essence, on the circumstances of each individual case[3]. Based on your experience, what are the use cases where further guidance could be beneficial regarding the contextual assessment of the relevant perspective(s)? Further, are there any specific GDPR provisions which pose particular challenges for this assessment? For example, what open questions remain in practice considering different roles in processing, e.g. controller-processor relationship, joint controllership?

Participants highlighted the need for further guidance on the controller-processor relationship, with differing opinions on the relevant perspective for assessing identifiability in this scenario. Some advocated for considering only the specific “processor's” perspective, suggesting data could be deemed anonymous if effective pseudonymisation is applied and an appropriate assessment done by the controller concludes that the data subjects could not be re-identified by that “processor”. They urged to provide clear guidance on how to achieve this. Others disagreed emphasising that processors act on behalf of controllers and therefore the perspective of the controller should also apply to them. Some argued that the relevant GDPR provisions always require the assessment from the side of the controller. A specific use case where an organisational unit of the controller is acting as a processor was also mentioned.

Many participants underlined the need for clarity regarding the necessity to conclude data processing agreements between the controller and a “processor”, in particular when the party receiving the data would not have the means reasonably likely to be used to identify the data subjects. Some participants considered that controllers might rely on contractual obligations to prevent re-identification, noting limited visibility into processors’ identification methods. Others however cautioned against over-reliance on contracts only.

Additional guidance was also sought for joint controllership scenarios and controller to controller/ third-party data sharing, with complexities arising from varying access to data / data sets and identification capabilities among parties. Several participants requested clarity on

[3] *EDPS v SRB* judgment, paragraphs 100–111.

assigning responsibilities and using contractual obligations to manage risks. Some suggested that not all parties involved should bear the same level of responsibilities. A scenario lacking contractual links was also flagged as problematic in that context.

Challenges were noted in assessing changes over time, for example due to subsequent data sharing, mixing of data sets/ generation of new data, changes in roles of processing or new information becoming available.

Concrete examples requiring guidance included research and research consortiums, in particular in health, clinical trials and online advertising. In the context of online advertising, there was debate over online identifiers as personal data, with some participants asking EDPB to reconsider the singling out criterion while others insisted that such identifiers are personal data as they allow to take action on individuals, i.e. targeting advertising.

Guidance was also requested for intra-group data sharing and clarification on the role of data trustees or trusted third parties.

GDPR provisions causing difficulties included Articles 6, 28, 32-34, and Chapters III and V. Some participants highlighted the role of Article 11 GDPR and suggested revisiting the EDPB's position on this Article as expressed in its pseudonymisation guidelines. They also debated the need for a separate legal basis under Article 6 for transmission of data after pseudonymisation or for anonymisation of data.

Participants requested clear and practical guidance, including suggestions for a concrete methodology rather than case-focused advice, cautioning against generalisation. It was noted that the contextual assessment will be in practice very burdensome, especially for smaller organisations. Some argued that it should be possible to assess if the data is personal or not without considering the roles in data processing. Opinions varied on whether the identifiability assessment should take into account only legal means. Some stakeholders insisted that the identifiability assessment should be principles based and take into account proportionality and risk, while others highlighted the importance of consequences for data subjects and that their rights should not be undermined.

Question 2: According to the case law[4], a controller may need to assess the means of identification available through a transmission of the data in question to third parties. In relation to this, the data could possibly change its nature (e.g. data considered anonymous could become personal) due to (potential) transmissions between different parties, which may also have consequences for the initial controller. Which types of use cases (e.g. connected with third country transfers, publication to the general public) present practical challenges to ascertain the presence or absence of means of indirect identification? Which kind of measures could controllers take to recognise the presence of such means?

Many participants considered that "potential transmissions" refer to actual or foreseeable transmissions and not theoretical transmissions.

In discussing the case law, they emphasised the CJEU requirement for a circumstantial assessment, advising the EDPB to consider concrete cases (like *OC v Commission* (C-479/22 P), *Scania* (C-319/22) and *Breyer* (C-582/14)) carefully based on their specific factual circumstances without overgeneralisation.

Stakeholders agreed on the need for greater legal certainty but differed on achieving it. Some advocated for a toolbox or a clear list of criteria for identifiability assessment. Others argued

[4] C-319/22 *Gesamtverband Autoteile-Handel v Scania*, paragraph 49; *EDPS v SRB* judgment, paragraphs 84–85.

that organisations should be able to make predictable/reasonably foreseeable decisions based on a list of factors and measures. Others cautioned against a check list approach and/or suggested a principles-based assessment. One idea was to include a reasonableness test or a specific methodology for such assessment in DPIAs. Some stakeholders suggested to define common assessment criteria applicable to all sectors, while others asked the EDPB to issue sector-specific guidance.

For assessing whether the recipient is getting personal data, a layered approach considering data type and recipient use of data, alongside technological aspects, was suggested. In addition, the state of the art and the specific circumstances of each case should be considered. Some referred to the utility of data as a relevant factor.

Several participants urged to consider proportionality and focus on higher-risk scenarios rather than fringe cases with minimal re-identification risk.

The burden of proof was also debated, with concerns. Some noted that the controller or the transmitting party cannot be presumed to know all capabilities of receiving parties/ entire value chain, especially when it comes to further/ multiple transmissions. However, other stakeholders recalled the accountability principle applicable to the controller. Avoiding loopholes in responsibility was highlighted.

Several participants considered contractual clauses as an important element in the identifiability assessment, for example, to put in place measures to ensure that the data is used as intended by the transmitting party, even there the data is considered to be non-personal. Others, however, noted limitations of contractual measures, especially in cases of asymmetry, e.g. in terms of market power or information, between different parties. Also, some participants raised the need to include in contracts third party beneficiary clauses.

Regarding transfers to third countries, participants asked to clarify the obligations incumbent on controllers with differing views on the impact for the identifiability assessment. Some noted that an international transfer does not affect identifiability, and some stakeholders stressed that Chapter V GDPR should always apply when pseudonymous data are transferred. It was also reminded that, even when an adequacy decision exists, there could be access to data by law enforcement authorities and some participants considered that this should not impact the identifiability assessment.

Stakeholders also requested clarifications on various examples, for instance, related to research, statistics, clinical trials, health data sharing, online advertising and situations of joint controllerships. Examples where data is published were also mentioned, however, there were different views on how the publication impacts the identifiability assessment.

Some participants suggested greater accessibility and incentives for GDPR certification or codes of conducts and recommended considering other digital regulations, such as the Data Act and the European Health Data Space, as well as the Digital Markets Act (DMA), having in mind that they also refer pseudonymisation or anonymisation.

Finally, some referred to examples from other jurisdictions, e.g. Health Insurance Portability and Accountability Act (HIPAA) which includes the notion of “limited data sets”, or existing practical guidance on identifiably, e.g. from ISO and data protection authorities of Canada and Singapore.

As a general remark, it was noted that consistent and correct terminology should be used, i.e. the GDPR terminology should be avoided if no personal data is involved.

<u>Question 3</u>: The Court emphasised the restriction of the analysis to means reasonably likely to be used by the controller or another person[5]. Circumstances determine which means are 'reasonably likely' to be used. What kind of measures can a controller implement to limit the means 'reasonably likely' to be used? How can this be done in the case of subsequent transmissions by intended recipients to third parties who may be able to identify the data subject?

Stakeholders considered that the concept of "means reasonably likely to be used" ("MRLTBU"), as well as all the relevant concepts need to be sufficiently and clearly defined, by also taking into account the previous case-law of the CJEU and the role of different participants in the data chain.

When discussing MRLTBU, they identified different categories of measures: legal (including contractual), organisational and technical. These measures are complementary and equally important. Participants referred to a range of measures, including data processing agreements, audits, access restrictions, and privacy enhancing technologies (PETs) such as trusted execution environments. Most participants recognised the usefulness of the PETs but agreed that they are not sufficient and do not remove the (personal) data from the scope of the data protection legislation. In this regard, some participants requested the EDPB to include concrete examples of PETs that can be relied upon. It was suggested that tokenisation, encryption, hashing techniques and data masking deserve attention. Others recommended to rely on a case-by-case assessment of MRLTBU, avoiding overly prescriptive but instead reflecting the state of the art.

Many participants considered that the means envisaged should always be lawful, proportionate and foreseeable. Several stakeholders took the view that purely hypothetical and speculative threats, and illegal attacks (such as hacker attacks) should be excluded from the assessment. Others, to the contrary, pointed out that hacker attacks cannot be disregarded. It was emphasised that while the assessment of the MRLTBU should be adapted to the context, it should be based on objective, well-defined factors. In this regard, several participants drew attention to Recital 26 GDPR which already provides valuable guidance. Several participants highlighted that the assessment should also factor in, for instance, auxiliary datasets, data brokers, public registers and commercial enrichment services, not only isolated datasets. It was stated that a range of factors should be taken into account, including data retention limits, technical means for identification, time, cost, computing power, contractual barriers, access and retention controls, data metrics and potential access in the transmission chain, having regard to both the controller and other relevant third parties. Some stakeholders emphasised that the guidelines should clearly set out the safeguards and clarify the terminology used. They also noted that the assessment of the means should not rely on the promises of future developments.

While some stakeholders would like the EDPB to explain the steps and content of the assessment of MRLTBU, others argued that the EDPB should not be too prescriptive and leave some leeway to the business. The need for practical, not theoretical, guidelines on MRLTBU was raised, with stakeholders welcoming examples of lawful practice.

Many participants agreed that controllers have the main responsibility in line with the accountability principle, while advocating for a fair liability distribution among processing chain actors, given the complexity of situations and processing chains involved. Some insisted on reconciling the accountability principle with what is realistic and feasible in practice.

[5] *EDPS v SRB* judgment, paragraphs 79–85.

Next, several stakeholders stressed that the nature of the personal data itself should also be considered (it was noted that the EDPS v SRB case is very particular in this regard). In some cases, the data may be highly detailed and precise, resulting in a high risk of re-identification; in other cases, the nature of the data means the likelihood of re-identification is very low.

Finally, some participants flagged that the EDPB should reflect on the specific needs of SMEs and NGOs.

Question 4: In your experience, in which use cases would a controller processing data that has undergone pseudonymisation (pseudonymised data) have problems in deciding whether they are personal for a given recipient? What would be technical and organisational means that the pseudonymising controller could apply and that a recipient could not lift?[6]

Two main types of use cases were discussed.

The first type involved challenges in identifying all recipients and assessing their means. This included cases where recipients-processors use sub processors covered by business secret; when recipients are not known in advance and change over time; where receiving parties are very stratified, like in consortium or in online advertising; where some recipients have contracts (unknown to the controller) with other organisations regarding data that, once linked with the received pseudonymised data, could be cross-referenced and change the identifiability of the shared data set; when there is a major asymmetry of means or knowledge between the controller and the eventual recipients, with large providers (or cloud / AI providers) having substantial re-identification capacities. For such use cases, several participants underlined that the lack of knowledge should not be used as an excuse to ignore or overlook risks and that data transferred should be presumed personal data for the recipient unless anonymity is proven and documented.

The second type focused on complexities related to the data themselves either because of the complexity of the data set or because of the technicity of the data. One such example was the identifiability of genetic data for different kinds of recipients, another one related to additional information being broadly available.

While opinions varied on technical and organisational measures a pseudonymising controller might apply, all agreed that no zero-risk solution exist, and that open-ended situations (that might equal to public disclosure) require a higher resistance to re-identification. Some participants expressed that various ways of identifying a data subject exist as soon as some singling out is possible, and that they consider that the EDPS v SRB case only open the possibility of pseudonymised data to be anonymous but that those case will be extremely rare.

Regarding organisational measures, participants discussed what “cannot be lifted with reasonable means to be used” should entail. Some stated that policy or contract might suffice while some others considered contractual clauses might be lifted by laws or renegotiations. They then mentioned different measures of policy, contract and law: strict access control, oversight of secondary use, contractual obligation to notify controller of further sharing, contractual prohibition to attempt reidentification or to compare data against other data sets, NDAs but also legal obligations of specific actors. Finally, they insisted on the importance of a robust audit framework, which might include third-party audits, and regular re-evaluation every 2 to 3 years.

Participants shared multiple technical measures, including (homomorphic or classical) encryption with proper key management, multi-party computation, tokenisation, PETs

[6] *EDPS v SRB* judgment, paragraph 77.

synthetic data generation, classical anonymisation techniques, AI model as a form of pseudonymisation technique, APIs, data clean rooms as well as various classical security measures. On the contrary, some participants advised against overlooking quasi-identifier or of a naive use of hashing functions. Finally, emphasising core GDPR principles, they highlighted proper data minimisation and deletion of any unnecessary information.

From a technical point of view, participant asked for guidance on how to use those techniques properly, especially regarding PETs, key management or resistance to quantum computing, and defining clear thresholds.

Participants also inquired about the extent to which they should anticipate the future. In particular, they asked whether they should anticipate (and how to react) in the case of a personal data breach at a (sub)recipient, where data was assumed anonymous for them.

Additionally, participants raised a need of general clarification regarding the terminology, the notion of pseudonymisation domain, as well as on the interaction between “singling out” and “identification”, with no consensus on whether one implies the other.