Response to the EDPB public consultation on Guidelines 1/2025 on Pseudonymisation

The undersigned associations have taken note of the European Data Protection Board's (EDPB) draft "Guidelines 1/2025 on Pseudonymisation" (Guidelines), which have been circulated for public consultation until 14th March, 2025. We are grateful for the opportunity to provide comments on the draft Guidelines.

Executive summary

We welcome the fact that the Guidelines rightly recognise pseudonymisation as a privacy-enhancing technology that supports compliance with the General Data Protection Regulation (GDPR). However, the Guidelines set a very high bar for personal data to be considered properly pseudonymised and appear to confuse it with the conditions for personal data to be considered anonymised. This confusion leads to an overly restrictive approach that is contradictory to the requirements indicated in the GDPR and the case law of the Court of Justice of the European Union (CJEU). The Guidelines take an overly restrictive approach to pseudonymisation, one that would make it very challenging for most companies to achieve pseudonymisation and ultimately disincentivises controllers from using pseudonymisation. This might significantly limit innovations and investments by companies in privacy-preserving practices or in technologies based on artificial intelligence (AI).

Additionally, the Guidelines have been issued while the appeal in the *European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB)*[1] case is still pending, i.e. a case involving one of the members of the EDPB. The outcome of this case is crucial to the subject-matter of these Guidelines, as the issue of whether information is personal data or not from the perspective of a recipient - a fundamental question in the context of the legal implications of pseudonymisation - is at the heart of that case. As a body that brings together various data protection authorities, including the EDPS, the EDPB's adoption of Guidelines that reflect the view of the EDPS (as party to the *EDPS v SRB* case) creates the impression of an attempt to influence the judgment of the Court of Justice. This appearance of partiality is made even stronger by the latest Advocate General's opinion[2] in the *EDPS v SRB* case, issued on 6 February 2025, which rejects the views of the EDPS on this fundamental issue and supports

[1] General Court, *SRB vs EDPS,* T-557/20, ECLI:EU:T:2023:219.

[2] Opinion of Advocate General Spielmann, *European Data Protection Supervisor vs Single Resolution Board*, Case C -413/23 P.

instead the relative interpretation of the notion of personal data. Should the CJEU follow the Advocate General's Opinion, therefore, the Guidelines would become irrelevant and in contradiction not only with earlier case law (see hereunder) but also with a new CJEU judgment. This would trigger a high level of legal uncertainty for businesses that innovate with data and AI.

In this context, in accordance with the principles of good administration, the expectation would have been for the EDPB *not* to adopt any such Guidelines prior to the judgment of the CJEU, or to mitigate legal uncertainty by wording its Guidelines in a manner that accommodates not only the EDPS's view but also the opposing view (which has so far been taken by not only the other parties but also the EU General Court and now the Advocate General to the CJEU). In the present case, therefore, it would be advisable for the EDPB to withdraw its Guidelines and pause further work on them until the CJEU delivers its final judgment. Furthermore, once adopted, the final Guidelines should align with the Court's ruling and offer clear distinctions between pseudonymisation and anonymisation to ensure legal clarity and consistency in their application.

Areas of concern

- The Guidelines support an absolute approach to the notion of "personal data" that assumes the "mere possibility" of re-identification by anyone as sufficient to categorise data as personal data, even if there is no reasonable link between a controller (or any other party in the "pseudonymisation domain" described by the EDPB) and this set of personal data. This interpretation fundamentally misaligns with Recital 26 GDPR and current case law of the CJEU, in particular the *Breyer* judgment of the CJEU[3] and the *SRB vs EDPS* judgment of the General Court. What is more, it appears that the Guidelines are confusing the requirements for anonymisation with pseudonymisation. This confusion and overly broad interpretation create significant practical burdens for controllers attempting to implement effective pseudonymisation in line with GDPR principles.
- The Guidelines impose absolute criteria for the effectiveness of pseudonymisation that are in effect more akin to anonymisation, and inconsistent with the principles of proportionality and reasonableness enshrined in the GDPR. This approach also conflicts with Art. 32 GDPR, which requires security measures to be appropriate to the risk, taking into account the 'state of the art' and the 'costs of implementation'. In addition, the current draft Guidelines do not address PETs and the potential for combining pseudonymisation with Privacy-Enhancing Technologies (PETs) to strengthen the protection of personal or sensitive data. The Guidelines do also not deal with how pseudonymisation can practically be applied in unstructured data. We think that this is a

[3] CJEU *Breyer*, C-582/14, EU:C:2016:779.

missed opportunity to be forward looking in a fast-moving technology environment and particularly the AI evolutions.

- The Guidelines suggest requiring from controllers more than what the law itself prescribes, such as a requirement to consider means that might not be reasonably accessible (e.g. legal or illegal means available to cybercrime actors or third countries public authorities) in order to assess the risk of re-identification of data subjects. If these actors lack reasonable means to identify data subjects, the data should not be considered as personal data from their perspective at all. This approach is especially visible when it comes to an overly broad interpretation of a “pseudonymisation domain”.
- The Guidelines finally appear to suggest that Art. 11 GDPR broadly applies even when a controller lacks means to identify data subjects, contradicting GDPR's identifiability precondition. This is a misinterpretation that paradoxically increases burdens on controllers regarding data subject rights: instead of reducing obligations when identifiability is lacking as intended by Art. 11, the Guidelines require re-identification upon pseudonym provision, even for controllers without independent means to identify. This directly opposes the text and spirit of Art. 11 GDPR.

Key Recommendations

- The EDPB should not develop separate guidelines for pseudonymisation and anonymisation - instead EDPB should issue consolidated guidance encompassing both techniques. Given the inherent overlap between these techniques and their shared goal of reducing identifiability risks, a unified approach would enhance clarity, ensure consistency, and facilitate more streamlined compliance for controllers.
- The EDPB should withdraw the current Guidelines to avoid legal uncertainty and potential contradiction with the forthcoming CJEU ruling in *EDPS v SRB* case or at least refrain from issuing the final version until the CJEU delivers its ruling. If the CJEU follows the AG’s Opinion, a new public consultation would be needed to ensure the Guidelines align with the ruling, particularly on the distinction between pseudonymisation and anonymisation.
- The Guidelines should ensure that the understanding of pseudonymisation aligns with current CJEU case law and the relevant provisions of the General Data Protection Regulation, without conflating it with anonymisation. This approach would enhance legal certainty and provide a stronger incentive for the adoption of pseudonymisation techniques.
- The Guidelines should not overextend provisions of the GDPR by introducing unjustified additional requirements for data controllers. In particular, the Guidelines should encourage innovations and provide directions on how to develop new technologies, such as PETs, in accordance with the law instead of overly limiting possibilities to do so by

imposing unreasonable requirements or assumptions that certain practices, industries or use cases cannot effectively rely on pseudonymised data.

- The Guidelines should avoid suggesting that pseudonymisation may be insufficient for certain use cases or industries. Statements implying that pseudonymisation prevents data from being processed for incompatible purposes, such as personalised advertising, go beyond the scope of Article 6(4) GDPR, which requires a context-specific compatibility assessment.
- The Guidelines should be reviewed to provide more actionable examples that do not focus only on health sector use-cases where large quantities of sensitive personal data are being processed. A broader range of examples would be in particular relevant for small and medium-sized enterprises (SMEs).

1) The concept of “pseudonymisation”

The Guidelines confuse the conditions for pseudonymisation with the conditions for anonymisation. Purposely the GDPR separates these two concepts and sets the higher bar for the latter one, a fact that the Guidelines appear to ignore. Art. 4(5) of the GDPR defines the process of pseudonymisation by indicating that “additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.[4] This clearly indicates that this additional information must be within the “pseudonymisation domain”, to use the wording of the Guidelines, and not outside it, focusing only on actors covered by it. Pseudonymised data is only pseudonymous if the additional data enabling identification is available; if it is unavailable, i.e. is not among the lawful and reasonable means at the disposal of a given person or entity, that data must necessarily be viewed as anonymised data from the perspective of that person or entity. Recital 26 of the GDPR[5] confirms this, as it indicates that all objective factors have to be taken into account to determine whether a natural person *is identifiable.* If a data subject can no longer be identified by a party (using reasonable means), then from the perspective of that party, we are not talking anymore about pseudonymised data but anonymous data. That is also supported by Recital 29 of the GDPR, which states that, for the purpose of incentivising pseudonymisation, pseudonymisation “should [...] be possible within the same controller.” However, the Guidelines' proposed “pseudonymisation domain” approach, if interpreted to

[4] We would like to point out that the executive summary of the Guidelines at para 7 uses a definition of pseudonymisation that paraphrases rather than replicates the definition in GDPR Article 4. Considering many non-expert readers will focus on the executive summary, we recommend for consistency and clarity that para 7 uses the full GDPR definition instead.

[5] “*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”*

systematically require consideration of any and all third parties globally, would effectively undermine this incentive and render meaningful pseudonymisation within a single controller virtually impossible in many real-world scenarios. Additionally, the introduction of the new terms such as “pseudonymisation domain” does not clearly add value. Wherever possible, the EDPB should rely on established terminology from the GDPR or EU law to maintain consistency and avoid conflicting definitions.

Furthermore, the Guidelines, particularly in paragraph 47, appear to establish absolute criteria for judging the effectiveness of pseudonymisation, a stance that is both impractical and inconsistent with the GDPR. Rather than adopting a risk-based approach as mandated by Article 32 GDPR, which requires considering the 'state of the art' and implementation costs, paragraph 47 seems to demand a level of irreversibility more characteristic of anonymisation. This not only blurs the crucial distinction between these two concepts but also fails to acknowledge that 'state-of-the-art' pseudonymisation techniques, and the means to potentially reverse them, will inevitably evolve over time. Imposing absolute standards today risks rendering current best practices obsolete tomorrow, stifling innovation and creating a chilling effect on the adoption of valuable privacy-enhancing measures.

Additionally, at the very beginning (as part of their Executive Summary), the Guidelines indicate that “*The pseudonymisation domain does not have to be all-encompassing, but may be restricted to defined entities, most often to the set of all authorised recipients of the personal data that will process the data for a given purpose”.* Later, however, the Guidelines indicate that a controller should, for pseudonymisation to be effective, also take into account actors with a criminal intent and the measures that those bad actors might deploy (para 37-38,42-43,60 of the Guidelines).

This reference to bad actors raises two key issues: (i) the *Breyer* judgment of the CJEU made it clear that account must not be taken of all means reasonably likely to be used to enable identification **but rather of *legal*, i.e. *lawful* means reasonably likely to be used** (revealing another point on which the Guidelines are incompatible with CJEU case law - see more hereunder on this point); and (ii) there are inherent contradictions within the Guidelines on what the pseudonymisation domain is supposed to be and which means are supposed to be taken into account. This type of wording in the Guidelines is therefore both legally problematic and unclear, which gives rise to legal uncertainty.

What is more, the conditions set in section 2.4.3 of the Guidelines are overly prescriptive, not only regarding pseudonymisation but also in imposing new obligations that go beyond Chapter V of the GDPR. For instance, the Guidelines[6] require the inclusion of foreign national security agencies from non-adequate third countries in the ‘pseudonymisation domain’ effectively

[6] Para 64-68 of the Guidelines.

renders the practice unfeasible at the required threshold. The broad scope of entities—including any public authorities with access under foreign law or practice—requires an assessment of what information they may obtain, even through legally questionable means. Expecting private companies to determine potential illegitimate access by foreign authorities is unrealistic. Furthermore, as such assessments are already covered in the EDPB's transfer guidance[7], it is unclear why the pseudonymisation guidelines impose a seemingly stricter standard. Additionally, para 64 of the Guidelines refers to a jurisdiction offering protection equivalent to the European Economic Area, which suggests an adequacy decision scenario. However, adequacy means no additional security measures are needed, making this reference potentially misleading and unnecessary.

Similarly, para. 60 of the Guidelines suggests that for pseudonymisation to be effective, a controller should also take into account additional information outside the pseudonymisation domain[8]. Indeed, by saying that pseudonymisation will only be effective if the additional information required for attribution *"goes beyond"* what can be obtained *"with reasonable effort"*, the Guidelines are in effect stating that pseudonymisation is only effective if an actor *does not* have access to any reasonable means to identify a natural person - i.e. the very definition of information that is not personal data (any longer). This is therefore anonymisation from the perspective of those actors. It is worth stressing in this respect that the analysis of effectiveness of pseudonymisation should not require the controllers to analyse all possible and hypothetical scenarios that might affect the selected actors in the pseudonymisation domain, as only objective factors should be taken into account (as per recital 26 GDPR). Reading it differently creates an additional burden for the pseudonymising controllers that is not required by law and such interpretation requires analysis where there is in fact no personal data even from the perspective of other actors due to lack of reasonable means and objective links. The Guidelines should clarify that a controller can achieve pseudonymisation through binding organisational and technical safeguards, such as policies preventing data combination.

As was indicated in the CJEU's *Breyer*[9] judgment in para 46, if the identification of the data subject requires an unreasonable effort, making the risk of identification insignificant in reality or if a certain activity is forbidden by law, the data would not be considered personal data. Additionally, in para 45 of its judgment the CJEU highlighted that to determine whether a set of data constitutes personal data depends on whether the necessary additional information held by the other party can be **reasonably used** to identify the data subject by another party. This

[7] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

[8] *"Based on this assessment, for it to be effective, the controller needs to design the pseudonymisation procedure in such a way that additional information is required for attribution that goes beyond what the selected actors possess or could obtain with reasonable effort."*

[9] CJEU *Breyer*, C-582/14.

reading of Recital 26 of the Data Protection Directive 95/46/EC, which is nearly identical in this respect to Recital 26 of the GDPR, was also confirmed by the CJEU in its *Scania*[10] and *IAB Europe*[11] judgments. These judgments support the relative approach to the notion of personal data, where the perspective of a certain actor, analysed with the use of the conditions set in *Breyer* ruling, determines whether a set of data constitutes information about "identifiable persons" for this certain actor. As a consequence, if a controller was supposed to analyse even unreasonable and hypothetical means (as suggested in para 21,22 and 60 of the Guidelines) from the perspective of all actors that could try to re-identify the data subject, such a requirement would go far beyond even the requirements for anonymisation as the aforementioned CJEU rulings refer to.

Yet para 21 and 22[12] of the Guidelines take an overly restrictive approach and suggest that pseudonymised data remains personal even when no party in the processing chain (or pseudonymisation domain) can reasonably combine it with additional information. In particular, para 21 introduces an expanded interpretation of "additional information." Under the GDPR, the definition of pseudonymisation (Art. 4(5)) does not specify what constitutes "additional information"; it merely states that such information should be kept separately with appropriate organisational and technical measures. This implies that "additional information" refers to data already held by the controller, rather than information they could potentially seek out—such as publicly available resources like social media or online forums, as the Guidelines suggest and try to define what the "additional information" is.

Put differently, they set out requirements normally reserved for anonymisation and make them applicable to pseudonymisation. The Guidelines seem to suggest that the data may not be considered pseudonymous from the perspective of an authorised third party if other, unauthorised entities could potentially access the data and re-identify individuals using means available to them but not to the authorised third party (see para 22, 43[13] of the Guidelines). Following this interpretation, though, data will not be deemed pseudonymous due to the theoretical risk of re-identification by external actors, and it can therefore also never be considered anonymous.

[10] CJEU *Scania*, C-319/22, ECLI:EU:C:2023:837, para 45-49.

[11] CJEU *IAB Europe*, C-604/22, ECLI:EU:C:2024:214, para 49-51.

[12] *"If pseudonymised data and additional information could be combined having regard to the means reasonably likely to be used by the controller or by another person, then the pseudonymised data is personal. Even if all additional information retained by the pseudonymising controller has been erased, the pseudonymised data becomes anonymous only if the conditions for anonymity are met."*

[13] *"For instance, pseudonymisation may be performed prior to transmission of the data to a processor or third party that ensures only a level of security that would not be appropriate for the processing of the original data, but is appropriate for the risk connected with the processing of data that cannot be attributed to data subjects. In this case, all means available to unauthorised parties that might access the pseudonymised data while the (authorised) recipient of that data processes them need to be considered."*

This approach fails to recognise a crucial distinction - if the authorised third party itself lacks any reasonably available means to re-identify individuals, the data should be properly understood as anonymous in relation to that party, not merely pseudonymous. By applying an absolute approach, which considers the theoretical possibility of re-identification by any actor rather than assessing the practical means available to the specific party handling the data (as required by *Breyer, Scania, IAB Europe* CJEU rulings indicated above), the Guidelines risk overextending the definition of personal data. This could lead to unnecessary restrictions on data use and sharing, even in scenarios where the data pose no real risk of identification in the hands of the receiving party.

The relative approach is also supported by the General Court (GC) ruling in the *European Data Protection Supervisor vs Single Resolution Board* case[14]. The case referred to a situation where pseudonymous data was transferred to an entity that was within the pseudonymisation domain. The GC applied the test from *Breyer* and indicated that the perspective of the recipient has to be taken into account while assessing whether the data relates to "identifiable persons" for this recipient[15]. This particular view is contrary to what the Guidelines seem to suggest in particular in para 22, 43 as pointed out earlier. The General Court's judgment is under appeal, but the Opinion of the Advocate General (AG) in this case[16] confirms the aforementioned understanding of earlier case law, including the interpretation set out by the GC in its judgment[17]. In his Opinion, AG Spielmann rightly pointed out that *"it seems to me disproportionate to impose on an entity, which could not reasonably identify the data subjects, obligations arising from Regulation 2018/1725, obligations which that entity could not, in theory, comply with or which would specifically require it to attempt to identify the data subjects"* [18] - the undesirable outcome highlighted being precisely what appears to be the consequence of the Guidelines. Additionally, according to the AG under certain circumstances pseudonymous data can fall outside the scope of the concept of "personal data"[19] - again, it is an outcome that the Guidelines appear to exclude (or to make highly uncommon and challenging to accomplish). What is more, the Guidelines seem to miss the point that pseudonymisation is a *"process for putting in place a safeguard or technical and organisational measure"*[20] that involves processing personal data in

[14] General Court, *SRB vs EDPS,* T-557/20.

[15] Ibid, para 97-105.

[16] Opinion of Advocate General Spielmann, *EDPS vs SRB*, Case C -413/23 P.

[17] Ibid, para 59.

[18] Ibid, para 58.

[19] Ibid, para 52; "*In other words, it is not a matter of automatically excluding pseudonymised data from the scope of that regulation. (23) However, in the light of recital 16 thereof, it cannot be ruled out that such data may, under certain conditions, fall outside the scope of the concept of 'personal data'."; para 51: I infer from the wording of those provisions that pseudonymisation leaves open the possibility that the data subjects may not be identifiable, otherwise the wording of recital 16 of that regulation would be pointless. [...] If it is impossible to identify those data subjects, they are therefore legally considered to be sufficiently protected by the pseudonymisation process, notwithstanding the fact that the additional identification data have not been completely erased."*

[20] Ibid, para 48.

a way that removes certain identifying information, making it impossible to attribute the data to a specific individual without access to the separated information.

This means that in practice, the Guidelines apply the threshold for anonymisation to pseudonymisation, all the while considering that pseudonymous data is still personal data. Put differently, the Guidelines impose all of the requirements for proper anonymisation, without however excluding the thus pseudonymised data from the scope of the GDPR.

Yet the Guidelines are specifically intended to be about pseudonymisation, not anonymisation. It is our view that they should not apply the same standard to pseudonymisation as is required for anonymisation, unless the appropriate and consistent conclusions are drawn regarding the (non-)applicability of the GDPR to the resulting data. The Guidelines could then either (i) cover the issue of when pseudonymous data becomes non-personal data for one party or another, explicitly addressing (and taking into account) the aforementioned case law of the CJEU, without pre-empting the appeal in the *EDPS v SRB* case, or (ii) not include any considerations on the impact of pseudonymisation on the quality of information as personal data or non-personal data (and thus focus instead purely on pseudonymisation as a security measure, without applying the same standard as that for anonymisation).

In their current state, the Guidelines place a significant burden on pseudonymisation efforts without recognising the positive impact of pseudonymisation, notably the fact that any recipient who is unable to reidentify a data subject should be able to treat that information without applying the whole range of obligations under the GDPR. This approach will likely significantly reduce the possibilities for companies to innovate (in particular in the fields relying on AI) and at the end of the day even disincentive enterprises from investing in privacy-preserving technologies.

In addition, considering the fact that the appeal in the *EDPS vs SRB* case is still pending and the outcome is crucial for the topic of this Guidelines, it appears problematic from the perspective of legal certainty for the EDPB to issue guidelines that (i) contradict the current line of case law and (ii) embody only the view of one of the parties to that case, namely the EDPB member that is the EDPS. The role of the EDPB is to support the consistent application of the GDPR in the EU countries, not to create uncertainty or adopt partial views with the effect of pre-empting CJEU judgments, while these might well be the consequences if the Guidelines remain unchanged. Not only do they differ from CJEU case law, but they also create confusion as to how to understand the notions of pseudonymisation and anonymisation under the GDPR, concepts that are of a particular importance for the current EU digital economy.

Further complicating this matter is the EDPB's decision to issue separate guidelines addressing pseudonymisation and anonymisation. These two data processing techniques are inherently intertwined, both serving to mitigate the risks associated with the identifiability of individuals. Given the often subtle distinctions between them and the considerable overlap in the criteria for assessing their effectiveness, the publication of separate guidelines presents a potential for inconsistencies and operational uncertainties for controllers. A preferable approach, and one that aligns with established practices of several prominent data protection authorities, including the Irish Data Protection Commissioner and the UK Information Commissioner's Office, would be the development of consolidated guidance encompassing both pseudonymisation and anonymisation. Such an approach would arguably offer enhanced clarity and promote more streamlined compliance efforts.

Pseudonymised data may be personal data from the perspective of the (initial) controller, but the relative approach has to be applied, as has already been shown by the current case law of the CJEU. Pseudonymisation can lead to anonymisation, and this circumstance should be acknowledged by the EDPB instead of setting unrealistic standards and confusing the two concepts. It should be clear that the requirement of “having regard to the means reasonably likely to be used by the controller or by another person[21]” should be limited to parties within the pseudonymisation domain - there has to be a link between the possibility of re-identification and a certain party; it cannot be “any” party.

2) Application of art. 11 GDPR

Under certain conditions data subject rights indicated by the GDPR in Art. 15-20 do not apply to pseudonymised data, as the Guidelines rightly underline. However, it seems that para 77-79 of the Guidelines misinterpret the text of Art. 11 GDPR.

Art. 11(1) GDPR explicitly mentions that the controller is not obligated to maintain, acquire, or process additional information to identify the data subject solely for GDPR compliance if “the purposes for which [the] controller processes personal data do not or do no longer require the identification of a data subject by the controller”. The reference to “acquiring additional information” assumes that the data subject is initially identifiable, at the beginning of the processing activity.

The Guidelines, on the other hand, suggest that Art. 11 GDPR applies even if the data subject was not originally identifiable by the controller. This interpretation creates significant practical hurdles. For instance, it is unclear how a data subject could, in practice, obtain the necessary pseudonyms to facilitate re-identification by a controller who never possessed the original identifying information. This process would likely require the data subject to first approach the

[21] Guidelines, Para 22.

entity that originally pseudonymised the data, which may be unwilling or even unable to provide the pseudonyms (e.g., if it is not subject to the GDPR or relies on available exemptions). This renders the suggested application of data subject rights in such scenarios largely theoretical and unworkable.

The Guidelines' approach, as illustrated by the problematic requirement for controllers to re-identify data upon presentation of pseudonyms by the data subject, reverses the intended logic of Article 11 - namely the fact that the data subject has to be identifiable at the time of data collection (*ab initio*) and a controller ceases to have the means (or purpose) to identify them over time. The Guidelines suggest that Art. 11 applies broadly to pseudonymised data, even when the controller never had a reasonable means to identify the data subject; this, however, is a wrong assumption, as pseudonymised data presumes prior identifiability (as indicated in recital 26 of the GDPR or in the CJEU's *Breyer* ruling). Additionally, the obligation to inform data subjects about the applicability of the Art. 11(1) GDPR arises only if the controller engages in processing personal data, not merely by holding data that does not require identification. Additionally, para 78 suggests that controllers can always use pseudonymisation keys provided by data subjects. However, this expectation does not account for controllers' data retention policies, which may limit their ability to retain or process such keys over time.

The Guidelines also misinterpret the obligations of controllers under Art. 11(2) GDPR regarding the information that they must provide to data subjects. Specifically, the Guidelines suggest that controllers should inform data subjects about how to obtain their pseudonyms and use them for identification, potentially even providing the identity or contact details of the source of the pseudonymised data[22]. This exceeds the clear text of Art. 11(2), which merely requires controllers, where possible, to inform data subjects that they cannot be identified—nothing more. Additionally, the Guidelines' suggestion that controllers should provide pseudonyms contradicts Art. 11(2) GDPR, which places the responsibility on the data subject to supply additional information for identification. The Guidelines' interpretation of this provision does not have any basis in law or in CJEU case law. Furthermore, the EDPB should provide concrete examples or guidance on how controllers can effectively verify that the individual asserting their rights is indeed the person to whom the pseudonymised data relates, ensuring compliance while preventing misuse.

[22] Guidelines, para 79: *"Therefore, in order to give full effect to the rights of the data subjects, the controller should indicate in the information provided to data subjects according to Art. 11(2) GDPR how they can obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity. In this case, the controller may need to provide the identity and the contact details of the source18 of the pseudonymised data or of the pseudonymising controller."*

3) Pseudonymisation as a tool that lowers the risk of personal data processing

a) More examples of standard use-cases

We appreciate that the Guidelines cover many examples of the possible use-cases in the Annex.

However, a source of concern regarding the positions taken by the EDPB in the Guidelines is that half of them relate to the healthcare sector, with an emphasis on the processing of special categories of data, and some of the remaining examples also involve special categories of data. There are ultimately very few examples that are relevant to most organisations. Especially SMEs would benefit from simpler examples, as these enterprises usually have less resources to understand and ensure proper pseudonymisation. In addition, it would be useful to reference widely adopted standards that many companies implement, as standardisation is typically a key factor in corporate compliance—for example, ISO/IEC 20889:2018 or ISO/IEC 27559:2022.

The Guidelines also omit any significant discussion of Privacy Enhancing Technologies (PETs). This is an unfortunate oversight, given the increasing adoption of PETs across various sectors and their potential to achieve a high standard of pseudonymisation that may be difficult or impossible to attain through traditional techniques alone. The inclusion of practical examples demonstrating how PETs can be utilised to effectively pseudonymise data would significantly enhance the Guidelines' relevance and utility for organisations striving to innovate responsibly while complying with the GDPR. Referencing PETs in the Guidelines would better reflect the current state of the art in privacy-protective data handling.

Finally, the Guidelines fail to address the development of the technologies based on artificial intelligence where pseudonymisation plays a crucial role in the AI development and model training. A bridge between the latest EDPB opinion on AI models and GDPR[23] - which explicitly acknowledges the role of pseudonymisation - and these Guidelines in the form of additional examples covering this use case would be appreciated. Such a bridge is essential not only to ensure coherence between both Opinions but also to determine the extent to which pseudonymisation is relevant and useful in the processing of personal data within AI models. Additionally, para 47 of the Guidelines states that effective pseudonymisation requires individuals handling the data not to "single out the data subjects in other contexts". However, the Guidelines do not define "other contexts." The EDPB should clarify this term and provide examples to help companies implement pseudonymisation effectively.

[23] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.

b) Case-by-case assessment

The Guidelines should refrain from indicating that for some particular use cases or industries pseudonymisation might not be a sufficient measure to lower the risk. Paragraph 48 of the Guidelines suggests that pseudonymisation can prevent data from being processed and linked for incompatible purposes and specifically cites personalised advertising as an example. However, this interpretation exceeds the scope of art. 6(4) GDPR, which requires a context-specific analysis to assess compatibility. Linkage risks are theoretical if the pseudonymisation process is robust and follows the guidance in the Guidelines document (for instance para 5,18, 83–85 of the Guidelines) or data protection laws in general. Rather than making broad generalisations, the Guidelines should acknowledge that compatibility must be determined based on the specific circumstances of each case. Moreover, they provide no guidance on how companies can test the robustness of their pseudonymisation techniques or ensure adequate protection in practice. The EDPB should address this gap by offering practical testing methods, for instance how to conduct a risk analysis properly. Other approaches risk discouraging investment in pseudonymisation and other technical and organisational measures, as organisations may perceive a predetermined stance rather than a balanced and case-by-case assessment. Ultimately, this omission undermines the very privacy-enhancing approach the Guidelines seek to encourage.

c) Pseudonymisation as a mitigating factor

The Guidelines rightly underscore the fact that pseudonymisation supports controllers' efforts to comply with their obligations under the GDPR and might minimise risks to data subjects. Pseudonymised personal data provide greater protection to data subjects, and this should be taken into account by supervisory authorities during the investigation and decision process in the course of an enforcement action, a circumstance that the Guidelines should underline. As a consequence, pseudonymisation should be treated as a mitigating factor in enforcement cases if a controller has applied these measures.

There are already ingredients in support of this in the current text of the Guidelines, such as the emphasis on pseudonymisation as a key measure to support data protection by design and default (Art. 25 GDPR) and security obligations (Art. 32 GDPR), and the GDPR lists it as one of the conditions to be assessed while deciding about the fine by a supervisory authority (Art. 83(2)(d)), but a more explicit reference thereto in the Guidelines would be welcome.

Additionally, this could be also covered by Art. 83(2)(g) GDPR, as pseudonymised data should not be treated as "data in clear" but as data that reduce the risk for the data subject. We invite the EDPB (and supervisory authorities) to highlight the fact that the less identifiable the data is (such as pseudonymised data), the lower the likelihood of adverse effects on data subjects.

Finally, pseudonymisation could also be invoked under Art. 83(2)(k) GDPR as a mitigating factor, acknowledging the efforts and investments made by organisations in implementing such techniques. It is crucial for supervisory authorities to explicitly acknowledge that pseudonymised data carries a lower risk compared to directly identifiable data. The GDPR explicitly acknowledges this through its provisions (e.g. Recitals 28, 78, 156 of the GDPR) and recognises pseudonymisation as a measure reducing risks for data subjects. Recognising pseudonymisation in enforcement decisions is essential to incentivise its adoption, which in any event presents benefits for data subjects for the reasons set out above. Failure to take into account the investments of the data controller to effectively reduce the risks for data subjects through pseudonymisation would actually lead to disincentivising such techniques as controllers would be treated in the same manner, regardless of whether they have processed data in clear or whether they have pseudonymised the data and effectively reduced the risk. This would lead to a weakening of personal data protection which would be completely at odds with the purpose of the GDPR itself.

Given the complexity of these techniques, promoting investment in them is crucial to making them accessible to a broader range of market players, including SMEs and start-ups, which are key drivers of innovation. Unfortunately, the Guidelines suggest that proving personal data to be pseudonymous, let alone anonymous, will be highly challenging in practice. They adopt an overly restrictive interpretation of pseudonymisation (and anonymisation even though the Guidelines should not concern that notion) while introducing complex technical discussions that imply significant technical difficulties in achieving pseudonymisation. This approach creates unnecessary barriers, limiting the ability of organisations to demonstrate compliance. Furthermore, the ability to classify data as pseudonymous serves as a strong incentive for organisations to innovate and invest in data protection measures. By imposing such restrictive standards, the Guidelines risk discouraging these efforts and hindering technological advancement.

List of signatories:

IAB Europe: IAB Europe is the European-level association for the digital marketing and advertising ecosystem. Through its membership of national IABs and media, technology and marketing companies, its mission is to lead political representation and promote industry collaboration to deliver frameworks, standards and industry programmes that enable business to thrive in the European market.

Alliance Digitale: Alliance Digitale is dedicated to representing all professions and professionals related to data and print and digital marketing in France, with the aim of promoting their development, defending their interests and actively contributing to national, European and international discussions on societal issues, the creation of new work standards and the consideration of specific constraints. Digital Alliance's mission is to represent the interests of all its 300 members, regardless of their size or position in the value chain. Digital Alliance is a privileged interlocutor of public authorities and regulators at French and European levels. The association is also an important partner of the media and other professional associations in the digital ecosystem. Digital Alliance is the representative in France of three emblematic international networks of print and digital marketing and data professions: IAB, FEDMA, GDMA.

IAB Italia: IAB Italia is the Italian chapter of the Interactive Advertising Bureau, the leading association of digital marketing and advertising. For 25 years it has significantly contributed to the diffusion of digital culture and to the acceleration of market growth in Italy through the development of ethical and sustainable communication. IAB Italia pursues its mission through the realisation of vertical events, special projects, training activities and with IAB Forum, the largest Italian event dedicated to marketing and digital innovation on the most relevant issues for the industry, involving top national and international speakers. The Association has more than two hundred members, among the main Italian and international operators active in the interactive advertising market.

IAB Polska: IAB Polska is a Polish advertising industry organisation that unites and represents entities of the interactive industry. IAB Poland members include more than 230 companies, including the biggest web portals, global media groups, interactive agencies, media houses and technology providers. In 2012 the organisation received the MIXX Awards Europe, honouring the best IAB bureau in Europe.

IAB Spain: IAB Spain undertakes a comprehensive mission as a forum for meeting and representing the digital advertising industry in Spain. Since its inception in 2001, IAB Spain has played a crucial role in the promotion and development of digital advertising. IAB Spain's mission unfolds on various strategic fronts: With the aim of contributing to the proper regulation of the sector, by contributing, assisting, and fostering conversations with public administrations. Furthermore, IAB Spain proactively works on creating industry standards, with the goal of establishing guidelines and best practices that promotes the sustainable and ethical growth of digital marketing, advertising and therefore promoting innovation and positivities for the society.

Members of IAB Spain encompass a wide range of stakeholders in the digital advertising ecosystem, including digital and audiovisual publishers, platforms, media agencies, marketing and advertising agencies, advertisers, consulting firms, technology providers, advertising networks, and others, such as eCommerce and research institutes.

IAB Sweden: IAB Sweden is the leading association for interactive advertising and digital marketing in Sweden. By gathering stakeholders throughout the nations digital marketing ecosystem, IAB Sweden advances the progression of a well-functioning and sustainable industry. The fundamental mission of IAB Sweden is to unite, educate and promote the market for digital and interactive advertising in Sweden.

SPIR: For over 20 years, the Association for Internet Progress (SPIR) represents the most important players of the Czech Internet economy from among media publishers, media agencies and technology companies with an annual turnover of more than 37 billion Czech crowns (1,5 billion EUR). The services offered by SPIR members are used by over 90% of the population of the Czech Republic. Member companies pay 3 billion Czech crowns (120 million EUR) a year in taxes and other fees to the state budget and employ 7,500 people throughout the Czech Republic. SPIR operates the only official measurement of Czech Internet traffic NetMonitor, monitoring of Internet advertising AdMonitoring and provides expert analyses of the development of the Czech Internet market.

VIA Nederland: VIA is the industry association that looks, thinks and works more broadly. We believe that connection is the engine of progress. By bringing together a wide variety of persons and disciplines, an environment is created in which people, companies and the marketing profession can continue to grow. By working together intensively and by sharing knowledge and experiences we seek to predict and interpret developments and trends in the market and where possible determine or influence standardisation, legislation and (self-)regulation.