DeutscherAnwaltVerein

Position Paper

of the German Bar Association prepared by the Committee on IT Law and CSR and Compliance

on the European Data Protection Board's (EDPB) Guidelines 02/2026 on Anonymisation

Position Paper No.: 73/2026 Berlin/Brussels, October 2026

Members of the IT Law Committee

- Rechtsanwalt Prof. Niko Härting, Berlin (Chair)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main (Rapporteur)
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf (Rapporteur)
- Rechtsanwältin Isabell Conrad, München (Rapporteur)
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln (Rapporteur)
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Rapporteur)

In charge in the Berlin Office

- Rechtsanwältin Nicole Narewski, Director, Berlin

Members of the CSR und Compliance Committee

- Rechtsanwältin Prof. Dr. habil. Birgit Spießhofer M.C.J. (New York University), Berlin (Chair)
- Rechtsanwalt Dr. Olaf Christiansen, Gütersloh
- Rechtsanwältin Dr. Simone Kämpfer, Düsseldorf
- Rechtsanwalt Dr. Marc Löbbe, Frankfurt am Main
- Rechtsanwältin Prof. Dr. Anja Mengel, LL.M., Berlin
- Rechtsanwalt Dr. Björn Nill, Stuttgart
- Rechtsanwältin Dr. Hellen Schilling, Frankfurt am Main

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

- Rechtsanwältin Dr. Anika Schürmann, LL.M., Düsseldorf
- Rechtsanwalt Patrick Späth, LL.M., Berlin
- Rechtsanwalt Dr. iur. Thomas Voland, LL.M., Düsseldorf
- Rechtsanwalt Dr. Christoph Werkmeister, Düsseldorf (Rapporteur)
- Rechtsanwältin Nicole Willms, Frankfurt a.M.

In charge in the Berlin Office

- Rechtsanwältin Christine Martin, Director Berlin

In charge in the Brussels Office

- Rechtsanwältin Eva Schriever, LL.M., Director
- Myra Jockisch, LL.M., Legal Advisor

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising about 60.000 German lawyers and lawyer-notaries in 253 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level. The DAV is registered in the Lobby Registry for the representation of special interests vis-à-vis the German Bundestag and the Federal Government under register number R000952 and in the EU Transparency Register under registration number 87980341522-66.

The DAV welcomes the European Data Protection Board's (EDPB) issuance of guidelines on anonymization (Guidelines 02/2026 on Anonymization, Version 1.0, hereinafter referred to as the "Guidelines"), which build on Opinion 05/2014 of the Article 29 Data Protection Working Party and take into account the subsequent case law of the CJEU, in particular its judgment in *EDPS v. SRB*[1]. The Guidelines are of great practical importance, as the question of anonymization determines whether the GDPR's scope of application applies. Guidelines issued by the EDPB can facilitate the practical application of the law and provide legal certainty for data controllers.

However, guidelines only fulfill their purpose if they remain within the scope of the mandate assigned to the EDPB by the GDPR. Article 70(1) of the GDPR authorizes the Committee to provide guidelines, recommendations, and best practices to ensure the uniform application of the Regulation. The subject matter of the guidelines is thus the GDPR as shaped by the Union legislator; its binding interpretation rests with the CJEU (Art. 19(1) TEU, Art. 267 TFEU).

However, the draft does not stop at interpreting the applicable law. In several places, it sets its own, stricter standards in addition to the standard derived from Article 4(1) GDPR in conjunction with Recital 26 of the GDPR, as specified by the CJEU. The EDPB itself acknowledges this simplified approach, stating that it "can go beyond the legal standard" (Executive Summary; see paras. 45, 48). In doing so, the guidelines overshoot the mark. They deviate from the mandate set forth in Article 70(1)(e) of the

[1] CJEU, Judgment of 4 September 2025, C-413/23 P

GDPR—to ensure the uniform application of the Regulation—and actually create the very legal uncertainty they are intended to eliminate.

Although guidelines are not legally binding, they have a significant de facto binding effect. Supervisory authorities base their practices on them, courts rely on them for interpretation, and contracting parties, auditors, and insurers treat them as a minimum standard. A standard that goes beyond the Regulation shifts the boundaries of its scope of application without a mandate from the European Union legislator. In light of this alone, the EDPB's guidelines should remain strictly within the framework of the competence granted to the EDPB by the GDPR.

In its Helsinki Statement of 2 July 2025[2], the EDPB has also committed itself to providing practical, understandable, and risk-based guidance to facilitate the application of the GDPR and promote responsible innovation. The guidelines on anonymization should also be measured against this self-declared standard.

The DAV therefore suggests focusing the guidelines on the interpretation of the legal standard and refraining from recommendations that go beyond—or, at the very least, clearly labeling such recommendations as such. Specifically, we propose

- to clarify that the anonymization of lawfully processed data is supported by the legal basis of the preceding processing and does not require a separate legal basis;
- to delete all references to the "simplified approach," or at the very least to clearly separate this approach from the description of the legal situation in all sections;
- to apply the probability standard set forth in Recital 26 of the GDPR as specified by the CJEU, and to correct the examples that use merely hypothetical risks, unlawful conduct by third parties, or the state of the art as a benchmark;
- to assign independent weight to contractual and organisational safeguards when determining the means likely to be used; and
- reduce legal uncertainty through concrete B2B case studies and their brief assessments, because some GDPR provisions are not designed to account for the fact that, when multiple parties are involved in a given set of facts, the anonymity of the data may be interpreted subjectively in different ways.

[2] https://www.edpb.europa.eu/documents/reports-statements-and-letters/the-helsinki-statement-on-enhanced-clarity-support-and_en?utm_source=chatgpt.com

I. Lack of Incentives for Anonymization

From the DAV's perspective, the current draft fails to achieve the most meaningful and important effect the guidelines could have: it provides no incentive for anonymizing data—quite the contrary.

It is likely undisputed that the anonymization of personal data is one of the most important tools for reconciling data protection objectives with other objectives—for example, when making data available for innovation and value creation, as well as for research or to promote transparency and freedom of information.

From the perspective of data protection itself, it also makes sense for organisations to anonymize personal data. Anonymisation is the "ultimate" form of data protection, as it completely removes any personal reference and thus minimizes the risk of harmful or abusive data processing—at least with regard to the personal reference[3]—as much as possible.

Nevertheless, there is a lack of incentive for anonymisation not only in the wording of the guidelines themselves but also in the overall tone of the guidelines.

There is reason to fear that organisations will refrain from anonymisation because it is not practically feasible or because it entails excessive organisational demands and still creates legal uncertainty even then. From the DAV's perspective, these guidelines unfortunately align with various previous statements by the EDPB and other data protection authorities regarding so-called Privacy Enhancing Technologies (PETs). PETs can be methods for using technological means to protect the interests of data subjects as effectively as possible. However, companies will only choose this path if it makes sense for them, offers advantages, and leads to legal certainty.

In practice, it often happens that companies evaluate the implementation of PETs but do not proceed with them after the evaluation because the legal requirements are too stringent, meaning the hoped-for legal advantages of PETs (e.g., no personal reference or no status as a data controller) do not materialise.[4] Conversely, companies that wish

[3] Other risks associated with data processing remain, such as those related to consumer protection (e.g., dynamic pricing), manipulative data processing (e.g., manipulative advertising), or intrusions into privacy and confidentiality (e.g., disclosure of private or trade secrets). In this regard, however, there are specific protective laws outside the scope of data protection that do not require the underlying data to be personally identifiable.

[4] On the contrary, in such cases, PETs can result in companies effectively losing control over the data they process, while remaining legally responsible for it. This can actually increase legal risks rather than reduce them.

to use a PET are “burdened” with the responsibility and risk of liability for its flawless functioning, which, from the companies’ perspective, makes the use of PETs riskier than not using them.

The current draft version of the guidelines could have precisely this effect, as it describes almost exclusively disincentives to anonymisation. From the DAV’s perspective, however, a *practical* solution for anonymising personal data is the most important “key” to applying data protection law in a way that hinders innovation and economic growth as little as possible. Recent case law from the CJEU has opened a “window of opportunity” in this regard, because the CJEU’s earlier case law was unclear and therefore invited divergent interpretations. From the perspective of Europe’s innovation-driven economy, this was highly problematic, since data protection law—*when* applied—restricts, prevents, or at least imposes significant additional burdens on data processing within its scope. As a result, one of the most important “raw materials” for innovative business models—namely, data—is often available only to a limited extent or at considerable additional cost.

From the DAV’s perspective, this is not a reason to roll back data protection standards, as data protection is a fundamental right and serves the interests of the people. However, it is a reason not to apply data protection where it is not needed—namely, where the processed data is effectively no longer at risk under data protection law because it is no longer personally identifiable. In these areas, it makes sense *not* to apply data protection law so that the data can at least be processed freely in this respect.

II. Proposal: Clear Description of a Legal Basis for Anonymization

The foundation for such a *practical* approach, while simultaneously achieving the objectives of data protection law, is the permission—and thus the fundamental incentive—to anonymise personal data. In paragraph 38 of the Guidelines, the EDPB assumes that anonymisation constitutes processing within the meaning of Article 4(2) of the GDPR and therefore requires a legal basis under Article 6 of the GDPR as well as, where applicable, an exception under Article 9(2) of the GDPR. The view that anonymisation itself is a processing operation requiring its own legal basis or a strict compatibility assessment under Article 6(4) GDPR is also held by supervisory

authorities[5] and some legal scholars.[6] It follows (presumably) that anonymising data is not possible under all circumstances or, at any rate, requires a more detailed examination of the legal situation as well as additional compliance requirements (e.g., informing data subjects).

This legal interpretation is counterproductive. As already pointed out at the outset, anonymisation serves precisely to protect personal data and is particularly consistent with the objectives of the GDPR. According to Article 1(1) and (2), the GDPR aims to protect fundamental rights and freedoms, in particular the right to the protection of personal data (Art. 8 CFR). Properly conducted anonymisation does not impair these rights; rather, it serves to protect them and creates a state of affairs that the GDPR itself seeks to achieve in numerous provisions. Through anonymisation, the controller fulfills its obligation to data minimisation under Article 5(1)(c) GDPR, as well as the obligation under Article 5(1)(e) GDPR to store personal data in a form that allows for the identification of data subjects only for as long as is necessary for the purposes for which it is processed. This also applies in light of the controller's obligation to implement appropriate technical and organizational measures to protect personal data (Art. 25 and 32 GDPR). Finally, anonymisation can also be regarded as a data protection-friendly equivalent to erasure.[7]

Anonymisation must not be burdened by excessive requirements regarding a permissible change of purpose. The presumption set forth in paragraph 38 of the Guidelines is therefore a correct approach. However, it falls short because it is limited to anonymisations within the same processing activity and for the same purposes.

A practical approach would be a presumption under which the anonymisation of personal data that was lawfully processed on the basis of Article 6(1) GDPR and, where applicable, an exception under Article 9(2) GDPR—is supported by that legal basis and, where applicable, that exception. This should also apply even if the anonymisation takes place only in a second step, outside the scope of the original processing activity and for other purposes.

[5] See GPDP, Provvedimento No. 710 of 23 September 2026 (IQVIA), paras. 90, 106; BfDI, Position Paper on Anonymization under the GDPR with Special Consideration of the Telecommunications Industry, 29 June 2020, p. 5.
[6] Gola/Heckmann/Rost/Gola/Ziegler, 4th ed. 2026, GDPR Art. 4, para. 60.
[7] See also Art. 6(1) of the ePrivacy Directive, which equates erasure with anonymisation.

Irrespective of this, the guidelines in paragraph 38 take the view that, for the anonymisation of Special Categories of Data (SCD), it is necessary to have not only the legal basis of Article 6 but also an exception under Article 9(2) GDPR. This view is not legally substantiated and, in the opinion of the DAV, highly debatable. After all, the point of anonymisation is precisely to prevent any inferences from the data regarding, for example, the health status of data subjects; thus, the data is not processed "as" SCD. Furthermore, it is legally incomprehensible why SCD should be more difficult to anonymize than "normal" personal data. This results in the very data for which anonymisation is particularly important being the hardest to anonymise. Anonymisability is especially important for SCD because, due to the strict standards of Article 9, it is often the only way to put such data to meaningful secondary use (e.g., for medical research or AI training).

From a technical standpoint as well, anonymisation techniques are conceivable that do not access data fields containing SCD in the first place.[8] This possibility should at least be mentioned.

To help highlight the positive effects of anonymisation in this regard, the guidelines should be amended as follows (changes are *not* highlighted):

1) **Proposed wording for Recital 34:** *"[…] Binding contractual commitments (such as strict anti-re-identification covenants, non-linkage obligations, confidentiality undertakings and purpose limitations) constitute significant objective factors when assessing the means reasonably likely to be used by a receiving entity. Where contractual prohibitions are enforceable, subject to monitoring and backed by dissuasive penalties, they can render any re-identification attempt practically and economically disproportionate. In the absence of concrete evidence demonstrating a tangible risk of breach it should be presumed, as for legal prohibitions, that the contracting parties act in compliance with such obligations, provided that these obligations are reliable, verifiable and enforceable and cannot be unilaterally amended or waived."*

   The clarification in paragraph 34 that we propose aims to make the risk-based approach enshrined in the GDPR operational in practice. By recognizing binding

[8] For example, only the identifiers (e.g., name, patient numbers) may be removed from a data set without requiring read or write access to SCD (e.g., treatment information).

contractual obligations—provided they are backed by effective control mechanisms and deterrent sanctions—as relevant objective factors in assessing the measures likely to be used, a realistic analysis of re-identification risks is made possible. This does not result in a lowering of the level of protection, but rather in a more nuanced assessment that views technical measures and legal governance structures as a complementary system designed to enable data exchange in secure, controlled environments in a legally compliant manner.

2) **Proposed wording for Paragraph 38:** *"[…] Where personal data has been lawfully collected and processed in accordance with Article 6(1) GDPR (and, where applicable, Article 9(2) GDPR), anonymisation constitutes a direct implementation of the principles of data minimisation (Article 5(1)(c) GDPR) and storage limitation (Article 5(1)(e) GDPR) as well as of data protection by design (Article 25 GDPR) and security of processing (Article 32 GDPR). The legal basis and, when applicable, the relevant Article 9(2) exemption should therefore be presumed to coincide with those of the processing preceding anonymisation, and anonymisation should, as a rule, be considered compatible with the original purposes within the meaning of Article 6(4) GDPR. This applies not only where anonymisation is part of the same processing activity, but also where it is carried out at a later stage and outside the original processing activity, in particular in order to enable further use of the resulting anonymous information."*

   This addition to paragraph 38, which we propose, aims to strengthen incentives for data controllers to convert personal data into anonymous information as early as possible, which reflects the core essence of the principles of data minimisation (Art. 5(1)(c) GDPR) and data protection by design (Art. 25 GDPR). By recognising anonymisation as an instrumental means of achieving these protection goals, the necessary legal certainty is created to anonymise data even in later processing stages, without a renewed—and often cumbersome—assessment of purpose compatibility under Article 6(4) of the GDPR hindering effective risk reduction. This promotes a proactive approach that maximizes the protection of data subjects through the permanent removal of personal identifiers while simultaneously enabling the value-adding use of data in accordance with the spirit of the GDPR.

3) **Proposed wording for paragraph 90**: *"[…] In particular, controllers may deploy multi-layered governance architectures, such as data clean rooms, secure processing environments and data trustee models, including data intermediation services under Regulation (EU) 2022/868 (Data Governance Act). Where such an architecture effectively ensures that the recipient has neither logical nor physical access to the additional information needed for re-identification, possesses no lawful or practical means to obtain it, and cannot re-identify individuals through linkage or inference with means reasonably likely to be used, the data may be considered anonymous from the perspective of that recipient."*

   This addition to paragraph 90 closes a significant gap between the theoretical anonymity assessment and the modern technical reality of data ecosystems. By explicitly taking into account multi-layered governance architectures—in particular, data clean rooms and the intermediary services established by the Data Governance Act (EU 2022/868)—it is recognised that anonymity can be achieved not only by modifying the dataset itself but also through strict control of the processing environment. By incorporating the physical and logical exclusion of access to additional information as an objective factor in the proportionality assessment, a practical framework is created that combines the highest security standards with the necessary usability of data without compromising the level of protection for data subjects.

III. Greater Alignment with the Case Law of the ECJ

Furthermore, the CJEU's standard for anonymisation must also serve as the standard for the EDPB guidelines; only this is covered by the relevant authority to establish guidelines.

According to Article 4(1) in conjunction with Recital 26 of the GDPR, the decisive factor in assessing whether personal data has been anonymised is whether a natural person is identifiable, taking into account all means that the controller or any other person might reasonably use to identify that person. This standard has been clarified by the case law of the CJEU and simultaneously constitutes the legal framework that the EDPB must

adhere to when drafting its guidelines pursuant to Article 70(1)(e) GDPR. The authority to promote the uniform application of the GDPR does not include the authority to establish additional substantive requirements for anonymisation that go beyond the EU legal standard for identifiability.

In its *Breyer* judgment, the CJEU had already clarified that not every theoretically conceivable link to additional information is sufficient to establish a person's identifiability. Rather, it must be assessed whether the means necessary for identification can reasonably be employed.[9] This is particularly not the case when identification is prohibited by law or impracticable, for example because it would require a disproportionate expenditure of time, costs, and manpower, such that the risk of identification appears de facto negligible.[10] The decisive factor is thus not the abstract possibility, but the probability of identification, which must be assessed on the basis of the specific circumstances.

The CJEU expressly confirmed this standard in its *EDPS v. SRB* judgment and further developed it with regard to pseudonymised data. According to this standard, the mere existence of additional identifying information does not mean that pseudonymised data constitutes personal data for every individual.[11] Rather, effective measures can ensure that the recipient cannot identify the data subject—or can no longer do so—even though the original controller may still be able to match the data to the individual.[12] In this regard, the CJEU requires a relative and context-dependent assessment of identifiability, in which all objective circumstances—in particular, the available means of identification, the likelihood of their use, costs, time required, and technological possibilities—must be taken into account.[13] Accordingly, the complete elimination of even a purely hypothetical re-identification risk is not required.

It is inconsistent with this case law for the EDPB to cite hypothetical risks, unlawful conduct by third parties, or the state of the art as examples of the probability standard and thereby establish them as the standard. Mere hypothetical (and factually improbable) attack and access scenarios, abstractly conceivable but concretely improbable unlawful conduct by third parties, or technically conceivable but—by general

[9] CJEU, Judgment of 19 October 2016, C-582/14, paras. 42–46.
[10] CJEU, Judgment of 19 October 2016, C-582/14, para. 46.
[11] CJEU, Judgment of 4 September 2025, C-413/23 P, paras. 82, 86.
[12] CJEU, Judgment of 4 September 2025, C-413/23 P, paras. 75–77, 86.
[13] CJEU, Judgment of 4 September 2025, C-413/23 P, paras. 79, 82–87.

standards—unlikely-to-be-used methods must not be equated with actual identifiability.[14] They do not, in fact, represent a concrete probability within the context of a specific processing scenario. However, this is the only standard used by the CJEU to assess the likelihood of re-identification, especially since, in the case of unlawful conduct by third parties, the associated criminal law risks and, where applicable, the consequences under tort law must be taken into account. These factors also make unlawful conduct by third parties unlikely, which effectively rules out the risk of re-identification through unlawful conduct. Furthermore, if this standard is applied, there is ultimately always a possibility of re-identification, because there is always the possibility of unlawful conduct by third parties—namely, cyberattacks—that could enable re-identification. While this is not an excluded risk, it is, at first glance, a hypothetical re-identification risk that is, so to speak, inherent in every processing operation and would make anonymisation impossible. Even when state-of-the-art measures are in place, re-identification through such an attack cannot be ruled out. This standard goes far beyond the findings of the CJEU in the aforementioned decisions and thus beyond the scope of Article 70(1)(e) GDPR, which requires an assessment based on the specific context of the processing and the parties involved in the processing.

In the *SRB decision*, the CJEU, referring to the judgment of 9 November 2023 C-319/22 (*Gesamtverband Autoteile-Handel*, paragraphs 46 and 49 regarding the personal nature of the vehicle identification number (VIN) when transmitted by a vehicle manufacturer), ruled that such data should be considered indirectly personal for the entity for which the data is initially non-personal and which transmits the data (such as the vehicle manufacturer) if a subsequent recipient is able to identify the individual.[15] To clear up certain misunderstandings in practice, the EDPB should clarify the **temporal dimension of personal identification** in the guidelines. The possibilities for re-identification may need to be assessed in phases—including from a temporal perspective. A re-identification possibility that arises only later does not generally mean that the earlier processing of the (at that time) anonymous data is subject to the GDPR.

IV. Contractual and organizational restrictions should be taken into account

[14] CJEU, *Breyer*, Judgment of 19 October 2016, C-582/14, paras. 45–46; CJEU, *EDPS v. SRB*, Judgment of 4 September 2025, C-413/23 P, paras. 79, 82–83.
[15] CJEU, Judgment of 4 September 2025, C-413/23 P, *SRB*, para. 84.

The standard applied in the CJEU's judgments also highlights the independent legal significance of contractual and organizational restrictions.

Although the CJEU has not expressly ruled on the conditions under which contractual safeguards, such as access restrictions, establish anonymity on their own, its case law in does not limit the identifiability assessment to purely technical measures. Rather, it depends on *all* circumstances that objectively influence whether means of identification are likely to be used according to general judgment.

In particular, the following measures can influence the likelihood of re-identification and therefore effectively ensure anonymisation:

- contractual access and usage restrictions,
- prohibitions on linking to other data,
- restrictions on disclosure,
- binding confidentiality obligations, and
- monitoring and audit rights.

If these obligations are backed by effective termination rights and, in particular, substantial contractual penalties, the economic and legal consequences resulting from an identification carried out in violation of such contractual prohibitions may be so significant that the likelihood of such an identification being attempted is, as with a statutory prohibition, virtually ruled out. Therefore, when objectively assessing the likelihood of re-identification, such contractual restrictions must be considered on their own merits and not merely as a subordinate factor to technical measures and statutory prohibitions. What is decisive is their actual effectiveness in the specific case, not merely their contractual agreement.

It is incompatible with this outcome-based standard to assign contractual restrictions – regardless of their effectiveness – from the outset merely a subordinate, supplementary role vis-à-vis technical measures or statutory prohibitions.

However, this is precisely what paragraphs 34 and 90 of the EDPB Guidelines, in their current form, suggest. While it is true that contractual prohibitions cannot automatically be equated with statutory prohibitions, it does not follow from this that their effect on the likelihood of re-identification is, as a matter of principle, secondary, nor that additional technical measures are always required. Such a general priority of technical measures

cannot be inferred from either the *Breyer* judgment (paras. 45–46) or the *EDPS v. SRB* judgment (paras. 79, 82–87).

With its guidelines, particularly in paragraphs 34 and 90, the EDPB therefore also goes beyond the framework established by the case law of the CJEU and thereby exceeds the competences to issue guidelines granted under Article 70(1)(e) GDPR. Rather, the EDPB should recognize that effective contractual and organizational restrictions can also play a decisive role in ensuring that, based on general judgment, re-identification is unlikely in a specific processing context. The actual possibility of identification through other reasonably available means must be factored into the assessment of probability. This should be explicitly clarified in the guidelines.

This interpretation is also consistent with the position already set forth in the DAV Position Paper No. 21/2026 regarding the European Commission's proposal for a Digital Omnibus Regulation (COM (2025) 837 final). In its Position Paper, the DAV, referring to the *EDPS v. SRB* decision, explicitly highlighted the relative personal reference and the potential anonymizing effect of pseudonymisation.[16]

The present Position Paper pursues the same goal: The EDSA should create incentives for the use of effective anonymization technologies and privacy-friendly procedures, rather than hindering their use through requirements that go beyond the statutory standard and lingering legal uncertainty.

The guidelines should therefore make full use of the legal options for anonymisation recognized by the CJEU and give appropriate weight to standardised, effective protective measures. The probability standard must therefore be guided by the

[16] See DAV Position Paper No. 21/2026 on the European Commission's proposal for a Digital Omnibus Regulation (COM (2025) 837 final), pp. 19–23. The proposals to add a definition of anonymisation in Article 4(5a) of the GDPR (draft) and to clarify the proposal contained therein for an article 41a of the GDPR (draft)—which includes a rebuttable presumption of non-re-identifiability when specified technical and organizational measures are applied—are intended to improve legal certainty regarding anonymisation. The introduction of a definition of the term "anonymisation" in Art. 4(5a) of the proposed GDPR builds on the case law of the European Court of Justice and assesses the issue of re-identifiability with respect to the actors involved in processing within the specific processing context, without requiring that specific measures – whether technical, organizational, contractual, or a combination thereof—be given priority. The only relevant factors are the means of re-identification available to the parties involved in the processing within that specific context.
By clarifying the rebuttable presumption in Article 41a of the proposed GDPR—according to which, when the means and criteria set forth in a Commission implementing act are used, there is a rebuttable presumption that the data will not lead to re-identification and that the identification of the data subject is ruled out—legal certainty is established without abandoning the probability criterion. The principles of the Court of Justice of the European Union are taken into account.

principles of the CJEU. Hypothetical risks, unlawful conduct by third parties, and the state of the art alone should be removed as examples and replaced with those that are based on an assessment of probability within the specific processing context. In addition, contractual and organisational safeguards must be given independent weight when determining the means likely to be used for re-identification, and the probability standard in the specific processing context must be applied to these just as it is to technical measures.

V. Legally and Politically Undesirable Negative Effects of the "Simplified Approach"

The guidelines recommend a "simplified approach" that, upon closer examination, is anything but "simplified." Rather, it is an approach that—as the EDPB itself even acknowledges—is not based on the objective legal situation.

Measured against the standards of the GDPR and, in particular, the recent case law of the CJEU, the "simplified approach" is based on a one-sided interpretation of the term "reasonably likely," which seeks to take into account even those risks that are not, in fact, reasonably likely (as discussed above). Even purely hypothetical and improbable risks are to be considered.

However, this approach is *not* "simplified." It leads to a legal misalignment in which data protection law is applied where it does not belong.

From the DAV's perspective, the "simplified approach" appears primarily to be an attempt by the EDPB to preserve its earlier legal interpretation of the concept of "personal data," an interpretation that was rejected by the CJEU (at the latest) in the SRB decision. Instead of deriving a sensible and practicable guideline from the GDPR and the case law of the CJEU, the EDPB now devotes a large portion of the guidelines to a "recommendation" that the EDPB presents as legally certain and supposedly easier to implement, but which fails to meet this standard.

From the DAV's perspective, describing this approach as "simplified" is inaccurate. Generally speaking, from a legal perspective, it is advisable only in a few, select situations to apply data protection law "as a precaution" even where it is not actually required. While this *may* be sensible in certain situations to mitigate legal uncertainties, it remains only a "second-best solution" even in such cases. In the majority of cases,

however, this approach is not recommended: The application of data protection law almost always leads to *greater* complexity and effort, triggers further legal uncertainties, and hinders or prevents data processing. This hindering effect is justified only if it serves to protect fundamental rights and data subjects. However, where these interests do not need to be protected—because the data lacks a personal reference—data protection law lacks justification, both politically and constitutionally.[17]

In addition, there are two further points that argue against an "overly broad" application of data protection law:

1) Various other EU legal acts apply only when data protection law does *not* apply. For example, Articles 3(13) and (14) as well as Article 32 of the Data Act specifically address "non-personal data." Access to data under the Data Act *must* be granted if the GDPR does not preclude it. The Data Act does not provide for the application of the GDPR "as a precaution." While other EU legal acts do not explicitly state this, they take a back seat to the GDPR where the latter applies.[18]

2) Even provisions of the GDPR itself do not permit leaving the question of personal relevance open or assuming personal relevance merely "as a precaution." For example, it would constitute a violation of Article 13(1) or Article 15(1) of the GDPR if a controller gave data subjects the impression that it was processing their personal data, even though the data in question is actually anonymised.

This means that in many situations, data-processing organisations have no leeway to assume "just to be on the safe side" that data is personal. The question of whether a specific data set is personal is like a legal crossroads that triggers certain legal obligations in *both* directions. Organisations have no leeway here; rather, they need legal certainty.

Overall, the DAV therefore recommends removing all references to the legally unfounded "simplified approach" from the guidelines and instead presenting only the actual legal situation. This is also in line with the role of the EDPB and the data

[17] Like any interference with fundamental rights, the application of the GDPR must also be justified by objectives recognized by the European Union that serve the public interest or by the requirements of protecting the rights and freedoms of others (Art. 52(1) of the Charter of Fundamental Rights of the European Union). This justification is lacking if the underlying data no longer relates to an individual, i.e., no longer falls within the scope of protection under data protection law.

[18] See, for example, regarding the applicability of the DSA's provider privileges where data protection law also applies, ECJ ECLI:EU:C:2025:935, para. 127 et seq. – *Russmedia*.

protection authorities, as they have no mandate to shape policy but are only intended to promote the application of existing law (as interpreted by the courts) (see Section I above).

The problem is further exacerbated by the fact that the guidelines do not clearly distinguish between the "simplified approach" and the actual legal situation. In some parts of the guidelines, the "simplified approach" is even applied *exclusively*[19] which means that in these areas, the guidelines do not reflect the legal situation at all, but merely present "recommendations" from the data protection authorities or the EDPB. As a result, (above all) these sections of the guidelines are only useful for organisations that—contrary to the actual legal situation—follow the "simplified approach."

The EDPB itself clarifies in paragraph 48 that the "simplified approach" does not constitute an alternative legal standard. A negative result from this simplified assessment must therefore not be treated as evidence of personal data by supervisory authorities, auditors, or contractual partners. For this purpose, an assessment based on the specific relevant perspectives and the means of identification that can reasonably be expected remains necessary.

VI. Unbalanced Interpretation of the Term "Reasonably Likely"

Due to the conflation of the "simplified approach" with the actual legal situation described above, it is difficult in many parts of the guidelines to determine whether the EDPB is describing its legal opinion or merely offering a recommendation. This applies in particular to the interpretation of the term "reasonably likely," as used, among other places in paragraph 26, and relied upon in the interpretation of Article 4(1) of the GDPR.

Recent case law from the CJEU on the personal nature of data would have offered an opportunity in this regard to promote a more pragmatic and legally certain interpretation of the term "reasonably likely," thereby providing greater incentives for anonymisation. However, the current draft of the guidelines clearly misses this opportunity. Instead, the

[19] This is particularly the case in sections 3.4.1–3.4.3; see footnote 53*: „For the sake of explanation, the descriptions of these criteria in sub-sections 3.4.1–3.4.3 use the simplified approach, which allows this sub-section to focus on the methods themselves. The contextual matters will then be reintroduced sub-section 3.5."*

risks of re-identification of data subjects are overstated, which, as described above, effectively discourages companies from anonymising data.

In its case law described above (under II.), the CJEU has clarified that “reasonably likeliness” must always be assessed in the context of the specific case and from the perspective of the actual data processing. Hypothetical risks need not be taken into account any more than methods for establishing a personal connection to which none of the parties involved has “ reasonably likely“ access. Nor must methods for establishing a personal connection that are prohibited by law be taken into account.[20]

However, many of the statements used in the guidelines—particularly many of the use cases—are not compatible with this standard. The DAV recommends a fundamental revision of the guidelines to bring them into line with the legal framework and case law of the CJEU, while at the same time avoiding the impression that anonymization is deliberately unattractive and risky.

In particular, the following statements should be corrected:

1) **Paragraph 21:** Although the phrase “cannot be ruled out” echoes the wording of the CJEU, it overlooks the fact that the CJEU supplements this with “reasonably” attainable means (see *EDPS v. SRB* judgment, para. 85: *„Accordingly, in so far as it **cannot be ruled out** that those third parties have means **reasonably** allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.“*).

   In light of this, the guidelines should clarify, in accordance with the case law of the CJEU, that they do not establish a “zero-risk” standard: only identification using means that are “reasonably likely” to be used must be ruled out; theoretical, abstract possibilities of re-identification are not sufficient.

2) **Paragraph 24:** In situations where a person can be identified only on the basis of a general description *(„the one with the northern accent“, „the one who lives*

[20] Established case law; see ECJ ECLI:EU:C:2016:779, paras. 4 –46 – *Breyer*; ECLI:EU:C:2024:215, paras. 50–51 – *OC v. Commission*; ECLI:EU:C:2025:645, paras. 81–84 – *SRB*.

underground" or *„the person in a black suit who is also walking a dog")* contrary to the legal interpretation in the guidelines, there is generally no personal reference. In such cases, there is often no way to identify that person. The situation is different only if the description makes it possible to determine the person's identity using probable (!) methods (for example, by checking identification), or if, despite the lack of assigned identifiers, it is possible to "single out" this person.

The concept of "singling out," in particular, remains underemphasised in the guidelines.[21] In particular, the guidelines fail to take into account that this concept implies, by extension, that individuals who cannot be identified by direct identifiers (e.g., name, ID number) are "identifiable" only if "singling out" is possible—that is, for example, if the data allows for effects to be retroactively applied to that person in the real world.

3) **Paragraph 28:** The risk described here—that a business partner could "easily" hire a third party to de-anonymise a data record—is generally not "reasonably likely." In practice, no one usually has an interest in de-anonymising anonymised data, especially not data recipients. After all, the data is valuable to such business partners precisely because it lacks any personal reference, meaning it can be processed without the restrictions of data protection law. Furthermore, de-anonymisation would constitute a clear and serious violation of the GDPR and would expose both the business partner itself and the data provider to serious liability risks. It is therefore generally prohibited by contract for the business partner. Furthermore, in reputable business dealings, no one would provide anonymised data to a business partner known for deliberately reversing the anonymisation of such data or even attempting to do so. It is <u>not</u> "reasonably likely" in reputable business dealings that business partners would engage in such unlawful conduct; rather, it is entirely remote. In any case, unlawful conduct should not be taken into account in the probability test.[22] Unlawful identification methods may not, in any event, be considered solely on the basis of their abstract possibility; rather, concrete, objectively verifiable circumstances are

[21] See, in this regard, only Section 3.4.1 as part of the "no record isolation" criterion and in para. 98.
[22] See the case law cited in footnote 20 .

required that make their application appear reasonably likely in the specific case at hand.

4) **Paragraph 30**: Similar considerations to those in paragraph 28 also apply to the examples cited in paragraph 30. Many of these are, in practice, precisely *not* sufficiently probable: In particular, this is not the case for the examples cited: "rogue employees," "an individual's partner, friends, colleagues," "investigative journalists," "law enforcement or intelligence agencies," "unethical companies," and "cybercriminals." All of these examples presuppose that individuals violate their confidentiality obligations or act deliberately with the intent to unlawfully re-identify the data.[23]

   In the practice of data processing, it is extremely rare for individuals with malicious or criminal intent to access anonymised data. The same applies (provided that proper data security measures are followed) to disclosures to unauthorised partners, friends, or colleagues. Furthermore, situations in which data is disclosed to law enforcement agencies or even intelligence services never occur in most data-processing organisations, or are at any rate the absolute exception. Merely citing such cases as examples of "probable" identification possibilities creates a distorted picture of the probability standard.

5) **Paragraph 31**: Contrary to what is claimed in the guidelines, a "lack of motivation" can and must indeed be included in the likelihood test. Neither the wording of the GDPR nor the CJEU permits this criterion to be disregarded in the probability assessment. Rather, *all* objective criteria must always be included in the probability test. This includes, for example, whether a data recipient has economic or other incentives to reverse the anonymisation, or whether doing so would instead constitute self-defeating behaviour.

   The question of whether a data recipient would establish a personal connection *accidentally* or *negligently* can also be objectively assessed in advance. Provided that an appropriate standard of data security is maintained, the accidental establishment of a personal connection is <u>not</u> "reasonably likely."

[23] At most, in the context of "investigative journalists," it might be conceivable that they have a legal basis for re-anonymizing anonymized data. However, this risk is relevant only to a negligible minority of practical scenarios. It is unclear why the EDPB cites such remote scenarios as examples.

6) **Paragraph 32:** The guidelines qualify the case law of the CJEU, according to which legally prohibited means of re-identifying an individual are not taken into account. The reasoning given is that, in the three CJEU decisions, the parties involved were "properly limited by the rule of law." The EDPB apparently seeks to infer from this that the CJEU's case law cannot be generalised. This is not legally justifiable: The three CJEU decisions *did not* hinge on whether all parties involved were "limited by the rule of law." Moreover, this is to be assumed in any case for *all* normal economic operators. Consequently, no controller is required to assume that third parties will act unlawfully.

7) **Paragraph 33:** This paragraph uses an example that assumes a company's data security measures are so poor that third parties could, through interception ("unlawfully intercepted") or a hacking attack, gain access to the supposedly anonymized data and then make it identifiable again. The example is poorly chosen for two reasons:

   - First, contrary to established case law of the CJEU, it assumes that unlawful conduct by third parties is "reasonably likely" (as discussed above).

   - Second, an organisation with inadequate data security measures should not be used as an example of the identifiability of data subjects. If an organisation has inadequate data security, the consequence should not be that it forgoes anonymisation, but rather that it improves its data security measures. Poor data security should not be allowed to serve as an "excuse" for failing to provide certain data to a public authority, particularly when doing so constitutes a legal obligation (see, e.g., Art. 18(4) of the Data Act).

8) **Paragraph 43**: Contrary to what the guidelines assert, the assessment of "reasonably likely" de-identification measures does not depend on what is possible according to *the* "state of the art." In legal terminology, the term "state of the art" refers to the best possible technical method that is available *at all*. In practice, however, such a state-of-the-art technical method for de-anonymization is not available to most data controllers and is also not "reasonably likely." In our experience, most organizations do not even come close to having such

capabilities. They also have no incentive whatsoever to acquire such capabilities, since they are interested in the legally compliant processing of *anonymized* data. Furthermore, according to Recital 26, technical feasibility is only one of several factors to be taken into account.[24]

9) **Paragraph 62:** The example of the board game shop should be removed. It suggests that re-identification is "reasonably likely" because the owner of this game shop could match his own customer profiles with user profiles from a popular website and thereby identify the data subjects. This is obviously a highly specialized game store with a very small group of regular customers, a large portion of whom also overlap with an online community. Such stores may exist in practice, but they are certainly not an example of "normal" data processing in the retail sector. Furthermore, even in the example provided, it is highly questionable whether it would be "reasonably likely" that the store owner would match his own customer profiles with the user profiles of the online community. Such data processing would likely be unlawful for several reasons[25] and should therefore not be considered "reasonably likely."

10) **Paragraph 94**: Contrary to what the guidelines imply, under normal circumstances the risk of an unintentional data loss (referred to as a "leak" in the guidelines) is precisely not "reasonably likely." This is certainly not the case for *"individuals who might hack into the system and steal and distribute the data*," who are cited as a possible cause of a leak. If an organisation has reasonable data security measures in place, the risk of a leak or a hacker attack cannot be ruled out, but that does not make it "reasonably likely." Furthermore, this example also assumes that third parties are acting unlawfully, which, according to the case law of the European Court of Justice, should not be included in the probability test.

VII. Recognition of Legal and Contractual Barriers

[24] See also Recital 26, sentence 4, according to which "the technology available at the time of processing and technological developments" must be *taken into account*—and thus this is only one of several relevant factors.
[25] E.g., due to a violation of Art. 6(1), Art. 6(4), or Arts. 13 and 14 GDPR.

The guidelines tend to prioritize mathematical and technical methods. In Section 3, the EDPB focuses on three criteria for technical analysis (No Record Isolation, No Linkage, No Inference).[26] Although it also takes access restrictions and security controls into account within the framework of the contextual approach (para. 89), However, it assigns only a supplementary role to contractual and organisational safeguards.[27]

According to the case law of the CJEU, means are not “reasonably likely to be used” if identification is prohibited by law or impracticable because it would require a disproportionate expenditure of time, cost, and manpower.[28] Legal and contractual barriers come into play precisely here: Enforceable contractual prohibitions, the violation of which triggers significant sanctions, increase the effort and risk for the entity performing re-identification and can make re-identification practically unreasonable. The guidelines should therefore assign independent weight to contractual and organisational safeguards when assessing the means likely to be used.

In addition to contractual prohibitions on re-identification, such safeguards may include, for example, data clean rooms or data trustee models. Data clean rooms provide isolated computing environments in which analyses are performed without recipients having access to raw data or identifying attributes, or being able to export raw data. Data trustee models—such as data intermediary services under Chapter III of Regulation (EU) 2022/868 (Data Governance Act), which are subject to statutory obligations of neutrality and purpose limitation – can be structured in such a way that the additional information required for re-identification remains exclusively with an independent body.

The fact that such combined protection concepts are feasible in practice is also demonstrated by the European Commission’s decision of 16 July 2026[29], regarding the provision of anonymised search data by Alphabet pursuant to Article 6(11) DMA. The measures set forth therein combine technical anonymisation with contractual prohibitions on re-identification and linking, organisational access restrictions, and independent controls, thereby illustrating the practical contribution such safeguards make to limiting the risk of re-identification

[26] EDPB, Guidelines 02/2026 on Anonymization, V1, July 7, 2026, para. 52 et seq.
[27] EDPB, Guidelines 02/2026 on Anonymization, V1, July 7, 2026, para. 34, 90.
[28] See CJEU, Judgment of 19 October 2016, C-582/14, *Breyer*, para. 46 et seq.; CJEU, Judgment of 4 September 2025, C-413/23 P, *EDPS v. SRB*, para. 82 et seq.
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026DMA100209&utm_source=chatgpt.com

Such hybrid architectures combine technical access controls with binding contractual prohibitions. By assigning contractual prohibitions merely a supplementary role and—unlike statutory prohibitions (para. 32 et seq.)—failing to recognize them as an independent factor, the EDSA risks creating legal uncertainty for data-protection-friendly European research projects, data spaces, and AI developments that rely precisely on such architectures.

VIII. Case Studies on the Applicability of the GDPR in Cases of Subjective Anonymity

While the more technical explanations in the guidelines are relatively extensive, the section on legal analysis (especially paras. 37 – 42) is relatively brief and general. However, the relativity of personal reference poses various challenges regarding the applicability of, in particular, articles 12 et seq., 26, 28, and 30 of the GDPR. It would be desirable for the EDPB to clarify the applicability of the GDPR provisions in B2B scenarios using brief case studies—similar to what is found in many other guidelines—to assist practitioners, for example, in the following cases, which are outlined here merely as examples:

Use Case 1:

A B2B customer transmits data to a recipient (a SaaS provider) that is not personal data from the customer's perspective. However, the recipient possesses additional knowledge, as it also processes data relating to natural persons on behalf of other B2B customers. The individual B2B customer cannot reasonably assess this additional knowledge, and the recipient is contractually prohibited from combining data relating to different customers. Clarification from the EDPB would be welcome as to whether, in such circumstances, a data processing agreement and the information obligations under Articles 13 and 14 GDPR may be dispensed with.

Use Case 2:

A company (seller) receives data that has already been pseudonymised—data that the company cannot re-identify—and sells it to a third party (buyer) for the purpose of AI development. The buyer has additional knowledge enabling the singling out of natural persons but cannot identify the data subjects by name. A clarification that the buyer,

too, has no obligation to provide information under Article 14 GDPR would be helpful in practice.

The fact that the anonymity of data may be assessed differently depending on the number of parties involved in a given set of facts—including from a temporal perspective—leads to legal uncertainty when applying those GDPR provisions that are not designed to account for this relativity. Case studies in the EDPB guidelines could help reduce legal uncertainty.

Mailing List

Europe

European Commission
- Directorate-General for Communications Networks, Content and Technology (DG CNECT)
- Directorate-General for Justice and Consumers (DG JUST)

European Parliament
- Committee on Legal Affairs (JURI)
- Committee on Civil Liberties, Justice and Home Affairs (LIBE)

European Data Protection Board (EDPB)
European Data Protection Supervisor (EDPS)
Council of the European Union
Permanent Representation of the Federal Republic of Germany to the European Union
Legal Advisors of the Permanent Representations of the Länder to the European Union
Council of Bars and Law Societies of Europe (CCBE)
Bundesverband der Freien Berufe (BFB) – Brussels Office
Deutsche Industrie- und Handelskammer (DIHK) – Brussels Office
Bundesverband der deutschen Industrie e.V. (BDI) – Brussels Office
Bundesrechtsanwaltskammer (BRAK) – Brussels Office

Germany

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesministerium für Digitales und Staatsmodernisierung

Ausschuss für Inneres im Deutschen Bundestag
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Fraktionen im Deutschen Bundestag

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Justizministerien der Länder
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe e.V.
Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und
Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
Staatsanwälte e.V. (DRB)
Deutscher Notarverein
Deutscher Steuerberaterverband e.V. Berlin

Bundesverband der Deutschen Industrie e.V.
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.
Deutscher EDV-Gerichtstag e.V.
GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.
Bitkom e. V.
Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)
ver.di - Vereinte Dienstleistungsgewerkschaft
Gewerkschaft der Polizei
Deutsche Polizeigewerkschaft im DBB (DPolG)

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Press

Frankfurter Allgemeine Zeitung GmbH
Süddeutsche Zeitung GmbH
Redaktion NJW
JUVE Verlag für juristische Information GmbH
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt
juris GmbH
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
DER SPIEGEL GmbH & Co. KG
Computer und Recht