October 2026

Public Consultation – European Data Protection Board (EDPB)

Guidelines 02/2026 on Anonymisation

Comments by Frank Ingenrieth

Frank Ingenrieth, LL.M., Registered Lawyer

0 About the Author

Frank Ingenrieth, LL.M. (**Author**) is an executive and registered lawyer with over 15 years of interdisciplinary, international experience in managing data protection and regulatory strategies for sustainable, innovation-oriented solutions. His practice focuses on media, internet, and data protection law, as well as related areas such as real estate law, and intersecting fields such as competition and antitrust law, and issues of good governance.[1]

Frank Ingenrieth, LL.M. gained his valuable experience throughout his professional career, including his training, at major international law firms, data protection supervisory authorities, multinational corporations, and non-profit organisations. He publishes regularly, whether in the form of legal literature, expert commentaries, or through round-tables and panel discussions.[2]

These Comments were prepared independently, without direction from any clients. The statement and comments are based on the author's long-standing practical experience in the design and enforcement of conformity assessment programs, including those that require regulatory approval due to their legal presumptive effects.

Legal and Contact Information

Richard-Sorge-Straße 69a
10249 BERLIN

Phone +49 30 985 387 95
Fax +49 30 521 036 88
Email office@ingenrieth-online.de

Tax-Number 14/358/01684,
FA Friedrichshain-Kreuzberg.

I opted according to **§ 19 UstG**
as small business.

IBAN DE22 5002 4024 7497 0388 01

Competent Bar/Bar of Registry
Rechtsanwaltskammer Berlin,
Littenstraße 9, 10179 Berlin

Awarded **professional job title** in Germany
Rechtsanwalt (Lawyer)

most relevant **Professional Regulations**

- Bundesrechtsanwaltsordnung
  (Federal Lawyers' Act)
- Berufsordnung
  (Professional Code of Conduct)
- Rechtsanwaltsvergütungsgesetz
  (Lawyers' Fees Act).

These and other applicable professional regulations can be accessed via the website of the Lawyers' Bar Berlin (Rechtsanwaltskammer Berlin).

1 More details about the author can be retrieved via the law firm's website: https://ingenrieth-online.de/en/about.

2 A related overview of publications by the author can be retrieved via the law firm's website: https://ingenrieth-online.de/en/publications.

Table of Contents

0 About the Author....2

Table of Contents....3

1 Executive Summary....4

2 Scope and Structure....5

3 General Observations....6

3.1 Conceptual Remarks....8

3.1.1 Critical Reflection and Individual Context of CJEU Decisions....9

3.1.1.1 CJEU Decisions and Their Effect of Precedent....9
3.1.1.2 “Relating to a Natural Person”....10
3.1.1.3 Sharing Information Along a “Processing Chain”....12

3.1.1.3.1 Example 1: Vehicle Information Numbers....12
3.1.1.3.2 Example 2: Transferring Pseudonymous Data....14

3.1.1.4 Conclusion and Recommendation Post Examples 1 and 2....17

3.1.2 In-Parallel Reflection of Interrelated Concepts; Terminology....18

3.1.2.1 Terminology....18
3.1.2.2 Lifecycle of Personal Data....18
3.1.2.3 Necessity to Clarify and Streamline Terminology Regarding “Identification”....19
3.1.2.4 Necessity to Clarify the Relation to Previous Publications....21
3.1.2.5 Establishing Modular, Interrelated Guidelines....22

3.2 Expected Impact....23

3.2.1 Practitioners’ Expectations, Relative Approach....23

3.2.2 Simplified Approach is Non-Approach....24

3.2.3 Non-Deterministic Concept of the “Contextual Approach”....26

3.2.4 Backfiring Incentives....27

3.3 Realistic Expectations....29

4 Specific Observations....33

4.1 Attribution of Capabilities Across the Processing Chain....33

4.2 Attribution of Capabilities by “Meaningful Connection”....34

4.3 Anonymisation as Processing Activity....35

4.4 Anonyms – Data vs Data Set vs Database....36

4.5 Anonymisation as “storage limitation”....36

4.6 Extending the “relativity” within one entity / corporation....37

1 Executive Summary

These Comments address the Guidelines 02/2026 on Anonymisation as published by the European Data Protection Board (EDPB) in version 1.0.

The Comments welcome two central features of the Guidelines 02/2026: the acknowledgement that each processing context requires individual assessment, and the constant reference to the EDPB's previous publications and to CJEU case law. Against this background, the Comments identify a number of points at which the Guidelines 02/2026 would benefit from further clarification, refinement, or correction.

1. **Critical reflection on the individual context of CJEU decisions:** The Comments recommend a critical reflection on the individual context of the CJEU decisions on which the Guidelines rely, in particular *Nowak*, *SRB*, *VIN* and *Breyer*. Where the Guidelines 02/2026 present fact-specific judicial applications as general, context-free methodologies – most notably the three-step test for "relating to a natural person" – the added analytical value is limited, and the risk arises that formulations devised in 2007 are received as settled law.

2. **Conceptual and terminological coherence:** The Comments address the conceptual and terminological coherence of the Guidelines 02/2026 with the EDPB's other publications, in particular Guidelines 01/2025 on pseudonymisation and WP29 Opinion 05/2014. A functional lifecycle of personal data is proposed as a structuring device, and a modular architecture of interrelated guidelines is recommended.

3. **Expected practical impact:** The Comments examine the expected practical impact of the Guidelines 02/2026. The "simplified approach" is not, in substance, a simplification of the anonymity assessment but a voluntary risk-allocation mechanism. Read together with the "contextual approach", it risks establishing an indirect presumption of culpability against processing entities acting in good faith, which would be difficult to reconcile with the principles of proportionality and the rule of law. The Comments therefore recommend the establishment of a continuously maintained assessment framework that positively determines the "means reasonably likely to be used" for distinct processing contexts.

4. **Specific provisions**: The Comments address specific provisions, including the attribution of capabilities across the processing chain and by "meaningful connection", anonymisation as a processing activity requiring a legal basis, the distinction between data, data sets and databases, anonymisation as a functional equivalent of erasure for the purposes of storage limitation, and the extension of the relativity of personal data within a single entity.

5. **Need to innovate the GDPR:** The Comments address the potential need to generally innvate the GDPR. As the Guidelines 02/2026 highlight, it was necessary to introduce distinct terminology because the existing terminology of the GDPR does not allow for properly reflecting th needs of today. This finding is interlinked with the suggestions in respect of considering a general lifecycle of data processing as such, and in particular in respect of different levels of "identification".

2 Scope and Structure

These comments (**Comments**) address the Guidelines 02/2026 as published by the European Data Protection Board (**EDPB**) in its version 1.0 ("**Guidelines 02/2026**").[3] As appropriate, these Comments will also refer to the related summarising document "At a Glance", as published by the EDPB subsequently ("**Guidelines At a Glance**").[4]

The Comments will first elaborate on general considerations and findings, such as consistency with other recent publications of the EDPB and decisions by the European Court of Justice (**CJEU**)[5].

Where appropriate the comments will also reflect on how the Guidelines 02/2026 appear remaining (un-)fit for purpose provided the European Commission's (**EC**) proposal(s) to amend the European Digital legal framework, i.e. especially the General Data Protection Regulation (**GDPR**)[6], will pass.[7]

Subsequently, the Comments will address particular remarks as appropriate. Such remarks may address ambiguities of the provided language of the Guidelines 02/2026, expectations regarding the practical effects of certain elements of the Guidelines 02/2026, and similar aspects.

The Comments do not reflect any particular, sector-specific interests, nor will they provide any pre-coordinated suggestions. However the Comments may indicate approaches on how certain elements might be resolved differently.

By doing so the Comments intend to maintain or, as the case may be, increase the effective level of data protection for data subjects as guaranteed by European fundamental rights, such as Art. 8 European Charter of Fundamental Rights (**EU CFR**)[8].

3 The Guidelines were published 7 July 2026, accessible via https://www.edpb.europa.eu/documents/guideline/guidelines-022026-on-anonymisation_en.

4 The *'At a Glance'* document was published in October 2026, accessible via https://www.edpb.europa.eu/documents/guideline/guidelines-022026-on-anonymisation_en.

5 The CJEU refers to the overarching institution, comprising the Court of Justice (**ECJ**) and the General Court (**Court**).

6 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

7 Most relevant, EC '*Proposal for a Digital Omnibus Initiative*', COM(2025) 837 final (**Digital Omnibus**), accessible via https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2025:837:FIN. The Council of the European Union (**CoEU**) has just published its suggested amendments based on the EC's proposal, CoEU, 14756/26 (**CoEU Amendments**), accessible via https://data.consilium.europa.eu/doc/document/ST-14756-2026-INIT/en/pdf.

8 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

3 General Observations

This section will address general aspects that do apply uniformly without specific context.

Such general matters relate, besides others, to terminology, applied interpretation of legislature and court rulings – in general -, structure of the Guidelines 02/2026, or potential effects.

By means of transparency: The author published on related subject matters continuously and recently. Additional publications or updates thereof are in progress. Therefore, the provided Comments might build upon the author's general (academic) positions and reflect a continuation thereof.[9]

Any legislative framework shall remain aligned with societal needs. Unless the very core of applicable fundamental rights, as provided by the EU CFR or any Member State equivalents, is concerned, conceptually and from a legal methodology point of view, there is often a remarkably high degree of flexibility. Accordingly, limitations appear rather politically driven while there might be several political, societal and economic reasons why the legal framework should not be adapted too frequently or radically.

At the same time, occasionally, there are significant leaps in development – be it societally, technologically, or alike – which materialise individually or interrelated so that any other disciplines, including the law, must adapt accordingly.

In times of such significant developments that might also be referred to as "groundbreaking" or "resulting in tectonic shifts", it might be the time to critically assess the legal frameworks' very foundations, too.

Such critical reflections need not lead to abandoning well-established, long-lasting principles of social coexistence, nor must they. Reflections are neutral at first place, conclusions should be drawn as they appear necessary and suitable. Artificially preserving detailed reflections of such rules of social coexistence might lead to unnecessary challenges and conflicts.

9 Contribution as author to legal commentary, Nink, StichwortKommentar Digitale Sicherheit (2026), regarding the terms / chapters '*Anonymisierung*' (Anonymisation) and '*Pseudonymisierung*' (Pseudonymisation); '*Opportunities to Reduce Bureaucracy under GDPR after CJEU in EDPS v. SRB (C-413/23 P)*', Computer Law Review international, https://doi.org/10.9785/cri-2026-270103; '*GDPR Model Draft: Towards a 21st Century Regulatory Framework*' (2026), v.1.1, https://doi.org/10.13140/RG.2.2.30130.77762; '*Wenn die Reform dreimal klingelt*' (2026) 1 InTeR 26; '*Data Protection, Innovation and Competitiveness Ain't Just a Matter of Structure And Competence*' (2026), https://doi.org/10.2139/ssrn.6996200; an overview can also be retrieved via the author's list of publications at https://ingenrieth-online.de/en/publications.

In other words: at times where several developments happen simultaneously and where each of such developments prove remarkably impactful on societal life, the law can become an active (design) element to guide and navigate developments, provided the competent institutions and bodies seize their opportunities.

Currently, there are indeed times of significant changes. The era of digitalisation, currently erupting and evolving into an era of artificial intelligence (**AI**), has been referred to by Member State ministers as more impactful than the era of industrialisation[10]. Consequently, this might be the time to critically and structurally assess the legal framework – and as the case may be – adjust the framework accordingly.[11]

This finding must acknowledge the given competences of those stakeholders involved.[12] The EDPB has no power to decide upon any modification of the underlying law, i.e. the GDPR. However, the EDPB retains the power to advise the legislator in the subject matter, Art. 57.1 lit. c) GDPR.

These Comments address guidelines as published by the EDPB: Guidelines are supposed to communicate the authorities' general understanding and interpretation of the law. In other words: while it cannot change the wording of the law and while it must remain within the boundaries of such wording, Guidelines may subtly (or radically) influence the application of the law, see Arts. 70.1 lit d) et seqq. GDPR.

While current times may require open-minded assessments and courage to critically reflect on the existing framework, its intents and its readiness and fitness in modern times, this must not be confused with unreasonable deregulation and lowering the appropriate levels of protection. Neither should efficiency by means of equalising multiple scenarios be mistaken with innovation-friendly environments.

Innovation reflects the continuous challenge of the existing – both in theory and practice. Therefore, innovation derives from the possibilities inherently carried by uncertainties, ambiguities and unknowns. Innovation builds on the power of differentiation and on the examination and refinement of individual cases. Such specific case knowledge will be transferred into abstract rules – if and to the extent common denominators are determined.

10 Federal Minister for Digital Affairs Wildberger (Germany), '*KI ist größer als industrielle Revolution'*, Deutschlandfunk, 24 December 2025, https://www.deutschlandfunk.de/ki-ist-groesser-als-industrielle-revolution-100.html.

11 In this respect, also refer to the structural assessments and related recommendations: Ingenrieth, *GDPR Model Draft* (n 9); Ingenrieth, '*Stop patchworking, rethink conceptually - Does Data Protection need an updated architecture*' (2026), https://ingenrieth-online.de/did-2026-q2-001.

12 The German Initiative of the "Stuttgarter Impulse" is a positive reflection on how data protection supervisory authorities can contribute the debate; Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (**DSK**), '*Stuttgarter Impulse zur Modernisierung des Datenschutzes!*' (2026), https://stuttgarter-impulse.de; see also Ingenrieth, *Data Protection, Innovation and Competitiveness* (n 9).

3.1 Conceptual Remarks

It is welcome that the Guidelines 02/2026 decline to equate any potential scenario but acknowledge the individuality of each processing context.

Likewise is it well received that the Guidelines 02/2026 provide constant reference to either EDPB's previous opinions, guidelines or other types of documents, as well as CJEU decisions. Such references facilitate recognising the line of argumentation drawn by the EDPB.

However, it seems the Guidelines 02/2026 would benefit from

- acknowledgement of the individual context of CJEU decisions, including conceptual deviations where CJEU decisions may be incompatible for generalisation[13]
- stronger alignment and interplay of affected concepts under the GDPR, including the parallelisation of related documents previously published by the EDPB.

It is understood that EDPB guidelines shall – principally – foster the correct application of the GDPR. Hence, it should provide practical guidance facilitating day-to-day operations.

It is therefore understood that guidelines shall rather have (low-level) practical impact than re-iterating complex (high-level) legal theories. While technically the audience of EDPB guidelines might be considered data protection and/or legal experts, it should be critically reflected whether this is a given. It should be questioned whether

- assumptions on the expertise of the audience are accurate;
- where such an assumption proves accurate, whether it might be a self-fulfilling prophecy due to the conception, language, and design of guidelines in the past;
- where such an assumption proves inaccurate, whether the guidelines already maximise their positive effects or whether different approaches in concept, style and language might be beneficial.

Against the background of such questions, it is well received that the EDPB has already started to adapt its means of presentation recently. Considering the Guidelines 02/2026 this is reflected by the "At a Glance"[14] document published alongside the guidelines.

13 Such incompatibility for generalisation might be a consequence of the original case and its specificities, or a consequence of subsequent developments, be it modified legal frameworks, changes in societal standards, innovations or progess in (scientific) knowledge.

14 See (n 4).

At the same time, guidelines should go beyond simply repeating the existing CJEU decisions. In interdependent and constantly evolving areas, the structural collation of existing court rulings may certainly be of help; because it facilitates navigating otherwise potentially overwhelming databases.

On the other hand, if guidelines limit themselves to repeating the decisions and / or the law, their added value is unnecessarily limited. Transferring those decisions into real life use cases, at best those commonly debated[15], will provide most added value.

3.1.1 Critical Reflection and Individual Context of CJEU Decisions

As the Guidelines 02/2026 claim, each processing will *prima facie* require individual assessment. While the applicable law remains the same, the primary legal source, i.e. the GDPR and its subsequent secondary (Member State) law, include terminology that is subject to interpretation. After almost 50 years of European data protection law, one might expect most terms were contoured over time. Yet, even where related (CJEU) decisions exist, such decisions only provide arguments to interpret the literal wording of the law.

3.1.1.1 CJEU Decisions and Their Effect of Precedent

Even though CJEU decisions are referred to as "case law", CJEU decisions do not qualify as legislation. This holds true despite any *erga omnes* effects[16] established and despite the binding nature of CJEU decisions with respect to stabilising and harmonising the interpretation of EU law, as stipulated by the Treaty on the Functioning of the European Union (TFEU)[17].

That is to say, CJEU decisions must not be ignored, and where previous decisions provide sufficiently clear precedent, it is a matter of harmonised European law, legal certainty and foreseeability, and efficiency to refer to existing decisions, respectively the arguments therein.

However, where the precedent results from highly specific contexts of the case, where the precedent dates back to modified applicable laws[18], or where (recent) developments in real life might impact the courts' conclusions, deviating lines of argumentation should be duly considered.

15 Transferring existing CJEU decisions on real life use cases where there are no ambiguities in how to apply GDPR is considered of very limited added value.

16 See ECJ, Judgment of 27 March 1963 (*Da Costa*), Joined Cases 28-30/62, ECLI:EU:C:1963:6; further contoured by ECJ, Judgment 6 October 1982 (*CILFIT*), C-283/81, ECLI:EU:C:1982:335.

17 See e.g. Art. 267 TFEU.

18 Technically, already minor modifications should suffice to conceptually assess whether (1) previous conclusions can be reasonably upheld or (2) deviating matters can be reasonably argued leading to request another – distinct or updated – decision.

The Guidelines 02/2026 might benefit from a critical reflection whether the findings of the CJEU are still fit for purpose at several occasions where the Guidelines 02/2026 refer to CJEU decisions.

Such reflections and verbalisation thereof, including probably existing gradients of legitimate interpretations of the GDPR, might beneficially affect the implementation of EDPB guidelines in general, and thus, contribute to protection of data subjects.

3.1.1.2 "Relating to a Natural Person"

The Guidelines 02/2026 integrate an entire section on how to determine "Relating to a Natural Person"[19]. In this respect, the Guidelines 02/2026 refer to existing ECJ judgments, i.e. *Nowak*[20] and *SRB*[21].

First, it remains unclear why the Guidelines refer to only two judgments, while there are even more CJEU decisions addressing this aspect.

Second, while it is accurate that the CJEU has referred to these three elements to determine the aspect of "relation", the three-step test, as presented in the Guidelines 02/2026, does not provide added analytical value in its current, context-free form. Considering the developments since its first invention, the elements might even in dedicated contexts provide no added value anymore. It shall be noted: The three-element structure origins from WP29 Opinion 04/2007[22] which was adopted by the ECJ in Nowak as part of its reasoning in a specific context.

This is why, the EDPB's current formulation risks presenting and consolidating a fact-specific ECJ application (Nowak) as a general, non-contextual methodology.

Reiterating the three-step test by referencing the ECJ case (*Nowak*)[23] as a general test in Guidelines 02/2026[24], without any additional contextual qualification, risks being perceived as circular reasoning. The ECJ decision (*Nowak*) drew the three-element structure from WP29 Opinion 04/2007; the Guidelines now rely on *Nowak* to re-establish that same structure. This is not strictly circular reasoning, but it does present a 2007 formulation, applied in a specific context, as a general test without added analytical value.

19 Guidelines 02/2026, Recs 16 et seqq.

20 ECJ, Judgment 20 December 2017, C-434/16, '*Nowak*', ECLI:EU:C:2017:994.

21 ECJ, Judgment 4 September 2025, C-413/23 P, '*SRB*', ECLI:EU:C:2025:645.

22 WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007.

23 See (n 20).

24 Transparency note: the Guidelines 02/2026 also refer to the original Opinion 04/2007.

This might be misperceived and misinterpreted as EDPB's reluctance to critically re-examine the validity of tests that were reasonable when established in 2007, in light of recent technical and societal developments. Likewise, the practical consequence for practitioners might be that a formulation devised in 2007 may be received as settled law, entrenching an outdated approach.

Yet in other words: the methodology of "relating to" remains subject to the conceptual drafts of 2007. Most probably, the conceptual ideas and challenges to be addressed by the 2007 wording dates back even further, expecting the WP29's Opinion was based on – established and well-known – discussions and needs of their time.[25]

Given the wording of the GDPR, none of those elements appear ultimately necessary to determine a "relation". Quite the contrary: the establishment of those additional elements – content, purpose and effect – dilutes the straightforward logic of Art. 4.1 GDPR. Art. 4.1 GDPR stipulates that any information related to a natural person is personal data.[26]

Even though the Guidelines 02/2026 re-iterate the unnecessary complications on how to determine "relating to", EDPB guidelines also use a much clearer language, already. In Guidelines 02/2026 it is "linked to", in Guidelines 01/2025 it is "attributed to".

De facto, the relation refers to the technical or organisational interlink of an information relating to a natural person. If at all, at the level of "relation" one might think of establishing thresholds of gradients of relativity, e.g.

- when is a device or internet access point used individually enough to establish a reasonably likely link to a natural person, yet,
- when is a device shared amongst too many individuals resulting in any such "link" to vanish.

Almost twenty years post the original opinion the debate has progressed which should be reflected in the newly drafted guidelines. The "original" elements of the WP29 Opinion 04/2007[27] rather define elements of identifiers and identifiability. Those should not be confused with the subject matter "relation".

25 Considering the approach of WP29's Opinion 04/2007 to focus on the interlink of (mobile) devices to natural persons, that is to say, that apparently there are possibilities and risks that (mobile) devices are pre-dominantly used by a distinct individual resulting in any device-related activities to be attributable to the distinct individual, fits the innovations of that time. 2000s and 2010s were the time, in which smartphone became popular, first in business (BlackBerry) then in general private use; e.g. the first iPhone was introduced in 2007.

26 E.g. this is also aligned with early German judgments, such as of the Federal Constitutional Court (BVerfG), BVerfG, Judgment of 15 December 1983 - 1 BvR 209/83 (Census Judgment).

27 See (n 22)

3.1.1.3 Sharing Information Along a "Processing Chain"

The Guidelines 02/2026 refer to ECJ judgments that dealt with the sharing of information across entities.

It is positively received that the EDPB confirms (again) within its Guidelines 02/2026 that identifiability is no absolute concept, but must be determined relatively, considering the available means reasonably likely to be used.[28] This approach reflects the common understanding[29].

Yet, different consequences appear possible to be drawn from the referenced ECJ judgments.

3.1.1.3.1 Example 1: Vehicle Information Numbers

The Guidelines 02/2026 appear to establish respectively confirm the interpretation of the ECJ case regarding vehicle identification numbers[30] that originally anonymous data become personal data retroactively, if a controller of such anonymous data transfers information thereof to another third party who might correlate such information with personal data.[31] The Guidelines 02/2026 explicitly state: "[...] this transfer means that the transferred information would also indirectly become personal for the transferring entity, even if that entity would not otherwise have means reasonably likely to be used to identify the individuals in question."[32]

This is not the only possible interpretation of the underlying ECJ judgment (*VIN*).[33] The ECJ did not conclude deterministically in its judgment. Indeed the ECJ argued that such a retroactive qualification might be a possibility, remaining subject to the referring court to be determined. Yet, even if the referring court determined the existence of personal data, such processing would be found lawful.

It is to say, the ECJ in *VIN,* therefore, addressed two questions:

- whether the transfer renders the data personal for the transferring entity (matter of threshold),
- whether the transfer is nevertheless lawful.

The Guidelines 02/2026 apparently conflate these, presenting the threshold as settled, whereas the ECJ left it to the referring court. The lawfulness element does not resolve the threshold question.

28 Guidelines 02/2026, Recs 8 et seq, Recs 18 et seqq.

29 See Ingenrieth in Nink (n 9), Anonymisation, Recs 16, 22; Ingenrieth in Nink (n 9), Pseudonymisation, Recs 23 et seqq.

30 ECJ, Judgment 9. November 2023, C-319/22 (*VIN*).

31 Guidelines 02/2026, Recs 9, 20 et seq.

32 Guidelines 02/2026, Rec 21.

33 See ECJ *VIN* (n 30).

In other words: The ECJ's reasoning can be read as a conditional holding: if the referring court determines that the data is personal for the transferring entity, the transfer may nevertheless be lawful. The Guidelines 02/2026, however, present the threshold question as settled, thereby converting a conditional, fact-dependent holding into an automatic legal consequence."

De facto, it remains necessary to determine individually the effective means between the parties, whether or not such attribution shall be deemed to exist.[34]

It is therefore recommended to prevent any impression of such automatism where the transfer of undoubtedly and demonstrably anonymous data shall become personal data – retroactively – if and so far there is any frequent or orderly relation between the parties.[35]

Instead, the relativity of personal data should be further outlined with distinct gradients and thresholds.

To the extent information will be exchanged bidirectionally, and the expected reflux of information will enable the original controller of anonymous data to enrich its original data set ultimately transforming such anonymous data to personal data, this should require further analysis with a high probability that such reflux will result in personal data even for the original controller.

To the extent anonymous data is being transferred to a receiving third party which holds the capabilities to either enrich such anonymous data to transform the anonymous data to personal data or where the receiving party may link the anonymous to personal data, this should require further analysis with a high probability that the receiving party must treat the originally anonymous data as personal data.

To the extent there is no reflux of information, there seems no necessity to qualify anonymous data retroactively as personal data with regard to the original controller.

Such an analytical and structural approach seems to also enhance consistency with the mirror-image situation, where the original controller holds personal data, but the receiving third party will not hold any means to relate the information to any natural person, i.e. the originally personal data prove "anonymous" for the receiving party, see also example 2, 3.1.1.3.2.

34 See also Ingenrieth in Nink (n 9), *Pseudonymisation*, Rec 26.

35 This refers to the Guidelines 02/2026 elements of "meaningfully connected", e.g. in Rec 9.

3.1.1.3.2 Example 2: Transferring Pseudonymous Data

The ECJ confirmed in its judgment (*SRB*)[36] the relative concept of personal data. The Guidelines 02/2026 refer to the ECJ's judgment accordingly.[37]

The Guidelines 02/2026 state, e.g. "*In many cases, the second question will receive a qualified response ("The individual might be identifiable, but only if…"). […] This question therefore needs to be viewed as one of likelihood: rather than asking if the individual is identified or identifiable in an absolute sense, it should ask how likely it is that the individual will be identified or identifiable by some entity.*"[38]

This appears an accurate summary of the ECJ judgment (*SRB*)[39]. However, even the ECJ judgment (*SRB*) provides for concerns whether its unreflected application will ultimately increase data protection.

This is the consequence, if the relativity is only measured with respect to the entities involved and the likelihood of identification.

The latter is a consequence of current GDPR, as it defines personal data as both any information related to an identified and identifiable natural person. In this respect, "personal data" is a non-determined, endless concept, rather than a conclusive threshold.[40]

The EDPB is bound by the letter (*littera legis*) of the GDPR, as is the ECJ. Therefore, unless the European Digital Omnibus[41] addresses this matter, Guidelines should strive to resolve incoherent results as best as possible.

More flexibility provides the GDPR with respect to the aspects regarding its concept of "relativity", while the relativity with respect to parties involved (the Guidelines 02/2026 use "entity"), other aspects might be certainly of relevance, too.

The Guidelines 02/2026 – partially – refer to such aspects, even though in other contexts. Another relevant factor seems the timeline. The Guidelines 02/2026 recognise that an entity's capabilities will change over time.[42] The Guidelines 02/2026 also mention that it may be legally required to assess a situation as per distinct moments in time.[43]

36 See (n 21).

37 Guidelines 02/2026, Recs 37, 6, 8.

38 Guidelines 02/2026, Rec 8.

39 ECJ, *SRB* (n 21).

40 Art. 4.1 GDPR.

41 See (n 7)

42 Guidelines 02/2026, Rec 88, in the same vein also Rec 35.

43 Guidelines 02/2026, Rec 14 (Example 2).

Such in-moment assessments are well-established across the provisions of the GDPR. Pursuant to Arts. 13.1 and 13.2 GDPR, the transparency obligations are to be fulfilled "at the time when personal data are obtained". Art. 14.3 lit. b) GDPR refers to the "time of the first communication", as well as Art. 21.4 GDPR.

Art. 25.1 GDPR stipulates in a confusing manner a continuum to effectively and efficiently balance risks with available technical and organisational measures.[44]

Against this background the status of qualification of information should consider – besides other aspects – their lifecycle.[45]

Applied in the context of the ECJ judgment (*SRB*)[46] the aforementioned might have significant impact on the determination of anonymity. It shall be recalled that the underlying case was subject to a highly specific and densely regulated legal framework. It appears, data protection became a last resort of claimants to materialise their claims originating entirely outside primary data protection concerns.[47]

Undoubtedly, at the time of collection, the controller collected personal data: although it separated direct identifiers from indirect[48] identifiable information, the latter remained linked to the former by means of a pseudonym.

Accordingly, the controller was required to provide its transparency statement pursuant Art. 13 GDPR at the time of collection.

The identifying and the identifiable information were strictly separated

- one data set – identified – clearly qualifying as personal data to any party that might process such data set.
- another data set, that rose concerns whether it qualifies as "identifiable" for any party that might process such data set.

44 Literally, Art. 25.1 GDPR establishes the obligations for such evaluation "both at the time of the determination of the means for processing and at the time of the processing itself". Effectively, these two points in time result in a continuous evaluation across the entire lifecycle of a processing activity, beginning at its theoretical conception and continuing until its *de facto* cessation.

45 Regarding the lifecycle of personal data, see also 3.1.2.2.

46 ECJ, *SRB* (n 21).

47 See also Ingenrieth, '*SRB v EDPS - facts, context, high-level impacts & remaining questions*', 2025-Q3-001, https://ingenrieth-online.de/did-2025-q3-001; Ingenrieth, *Opportunities to Reduce Bureaucracy* (n 9).

48 Note: by the terminology of the Guidelines 02/2026 the pseudonymisation by the controller would still result in "direct identifiability" because all capabilities to identify the individual natural person laid within the controller. By means of the Guidelines 01/2025, however, it would be a matter of indirect identifiability, because the individual natural person would not unfold by itself but only subject to the combination of different data sets ("additional information"); see also 3.1.2.3 and 3.1.2.5.

The ECJ concluded from the perspective as of the controller. It never assessed the quality of personal data solely from the perspective of the receiving party; if at all the ECJ applied an overarching joint-perspective.

The ECJ did not elaborate on how its – relevant – conclusion shall be practically implemented where it states "pseudonymised data must not be regarded [...] in all cases and for every person, personal data [...] in so far as pseudonymisation may [...] effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable."[49]

As the ECJ uses the term "pseudonymised data", the ECJ did not expect the controller to delete its "additional information", probably resulting in "anonymous data" already at the level of the controller.

The ECJ emphasised this finding with the reasoning that the EDPS was in err assuming that such an approach would unduly undermine the high European standard of data protection.[50]

While this certainly establishes the relativity based on the entities involved, it also carries a time-related element. Because, apparently, the assessment must be made not only at different entities but also at different point in time. Relevant points in time are probably

1. time of data collection
2. time of establishing effective pseudonymisation
3. time of transfer by the transferring party
4. time of retrieval by the receiving party (which also equals time of collection by the receiving party)
5. time of enriching the retrieved information with additional information by the receiving party

The rudimentary timeline already indicates why data subjects, the moment information qualifies as personal data at the receiving party, will always be subject to adequate protection. Because if information, that qualifies as pseudonymous or anonymous data for the original controller, will subsequently qualify as personal data because of the capabilities held by the receiving party, the receiving party will be subject to the GDPR. The time of retrieval starts the "lifecycle of personal data" at the receiving party.[51]

49 ECJ, *SRB* (n 21), Rec 86.

50 ECJ, *SRB* (n 21), Rec 85; ""[...] the EDPS is incorrect [...] that the fact that pseudonymised data are not [...] personal [...] for persons to whom the controller transfers the pseudonymised data makes it unduly possible to remove those data from the scope of EU law on the protection of personal data."

If ECJ's judgment (*SRB*)[52] in conjunction with ECJ's judgment (*VIN*)[53] would result in an automatism that any transfer of information, where such information will qualify as personal data at one moment in time, will qualify such information as "personal data" for any party involved, the ECJ would have established a legal concept of relativity which proves impossible.

Therefore, the findings of the ECJ in *SRB*[54] must be related to the specificities of the case, i.e. the claim of an incorrect transparency statement. It might also have been considered by the ECJ – even though the judgment does not provide any evidence in this regard – that there has been a "meaningful connection"[55] between the parties concerned. In this scenario, the "meaningful connection" might result from the fact that the relation between the controller and the receiving party remained.

Technically, as a matter of legal doctrine, given the independence of the analysis of the receiving party, the receiving party may not (fully) qualify as a processor – while in this case any of the discussions would not exist at first place. Yet, the receiving party did not fully qualify as a controller without ties to the original controller, either. Information was transferred to the receiving party and subsequently, there was a reflux back to the original controller.

It is recommended to critically reflect on the ECJ's decisions, to effectuate the opportunities they created. The Guidelines 02/2026 should not – unintentionally – re-establish impracticalities that were just rejected by the ECJ (*SRB*)[56].

3.1.1.4 Conclusion and Recommendation Post Examples 1 and 2

Based on the elaborations on the potential inconsistencies provided by the ECJ judgments, it is recommended to extend the Guidelines 02/2026 with practical foresight.

It would be highly appreciated if the EDPB, as the principal body within the EU to harmonise the application of the GDPR, would analytically address such concerns openly. Especially, the Guidelines 02/2026 should not create the impression of already generally concluded and determined concepts, where the underlying decisions may reflect highly individual scenarios or may have outlived their suitability for practical transfer due to significant developments in legal and societal contexts.

51 The ECJ highlighted in its judgment (*SRB)* (n 21) that any concerns with respect to limited transparency are a result of a deliberate design by the legislator, because the applicable transparency obligation provide for such exceptions; see ECJ, *SRB* (n 21), Rec 89; also Ingenrieth, *Opportunities to Reduce Bureaucracy* (n 9).

52 ECJ, *SRB* (n 21).

53 ECJ, *VIN* (n 30).

54 ECJ, *SRB* (n 21).

55 Using the wording of the Guidelines 02/2026.

56 ECJ, *SRB* (n 21).

3.1.2 In-Parallel Reflection of Interrelated Concepts; Terminology

The Guidelines 02/2026 address anonymisation distinctively. While it is acknowledged that reference is made to other EDPB guidelines, such as those on pseudonymisation (**Guidelines 01/2025**)[57], both guidelines would benefit from a coherent approach.

3.1.2.1 Terminology

This also reflects GDPR's terminology and very concept of "personal data" as such. Taking account of recent ECJ judgments[58], in which the contextual perspectives of pseudonymised and anonymised data were distinguished, the concept of personal data must – at last – be understood as (perspectively) relative, with graded conclusions.

The Guidelines 02/2026 recognise the challenges in existing terminology. Accordingly, the Guidelines 02/2026 integrate their own glossary. The suggested terminology appears consistent and logical, provided it needed to remain aligned with the existing legal frameworks, i.e. the GDPR.[59] In this respect the suggested terminology seems aligned with commonly used terminology.[60]

Limitations in terminology appear just a symptom for the GDPR reaching its limits to properly address challenges related to current reflections of processing activities. It is therefore recommended, to critically reflect on the consequences of previous publications and CJEU decisions, see also 3.1.1.1.

3.1.2.2 Lifecycle of Personal Data

Such reflections should start with analytically presenting the lifecycle of personal data. While the current definitions of the GDPR are intertwined, they may still be compatible with a significant share of the (technical) lifecycle. A functional lifecycle for personal data, for purposes of the present Comments, might comprise the following stages (not necessarily sequential):

1. start: non-personal data (not related to natural persons)
2. non-identifiable data related to a natural person (anonymous data)
3. identifiable data (pseudonymous data)

57 EDPB, Guidelines 01/2025, v1, January 2025; still "draft" status while the public consultation closed March 2025.

58 ECJ, *SRB* (n 21).

59 The current definitions of GDPR respectively the interplay of terms and concepts such as "data subject", "natural person", "identified", "identifiable", "individual", "pseudonymous" or "anonymous" reach their limits. Therefore, see also proposals for generally updating the conceptual foundations, Ingenrieth, *GDPR Model Draft* (n 9) with further references; Ingenrieth, *Stop patchworking, rethink conceptually* (n 11).

60 See e.g. Ingenrieth in Nink (n 9), *Anonymisation / Pseudonymisation*, each Recs 1 et seqq.

- data originally comprising / being enriched by indirect identifiers[61]

4. identified data (personal data in its narrow sense)
    - data originally comprising / being enriched by direct identifiers
5. data where direct identifiers were removed (reflecting pseudonymous data)[62]
6. data where direct and indirect identifiers were removed (reflecting anonymous data)
7. end: anonymised data (equivalent to 2)

The lifecycle is not strictly linear. Data may move between stages as a result of enrichment, de-identification, re-identification, or the passage of time (change in available means). The legal status at each stage must be assessed at the relevant point in time and from the perspective of the entity in question.

Addressing the lifecycle of personal data analytically might facilitate identifying current inconsistencies or imbalances in applying the data protection regime. Even if such inconsistencies or imbalances will not be of any direct effect, those may limit future evolutions of data protection law or make it unnecessarily burdensome to apply data protection law effectively to challenges of tomorrow. Upcoming challenges will require clear concepts of identification and identifiability, as this will become the distinction which legal frameworks will apply.

3.1.2.3 Necessity to Clarify and Streamline Terminology Regarding "Identification"

The GDPR uses "personal data" as anchor, Art. 4.1 GDPR. Inherently, the GDPR introduces several concepts, such as "identified" and "identifiable", which subsequently builds upon "identifiers", which can be "direct and indirect".

It is recommended that EDPB's guidelines will assist streamlining those (individual) concepts establishing an overarching methodology fit for purpose. It is acknowledged that such an endeavour will prove extremely ambitious, given the current phrasing of the GDPR. However, the logic within the current GDPR should – at a minimum – be applied consistently and – at best – unambiguously.

61 Including quasi-identifiers.

62 Indeed it is to argue whether indirectly identified data always qualify pseudonymous data in the meaning of Art. 4.5 GDPR. It is also to be discussed and to be assessed individually whether the removal of direct identifiers retains indirect identifiers, which will act as pseudonym; with indirect identifiers the removal of direct identifiers might automatically lead to anonymised data, see 6). Yet, such inconsistencies in current terminology should be resolved by analytically assessing the lifecycle and establishing a coherent conceptual approach.

Exemplarily, the Guidelines 02/2026 refer to “direct identifiers”, providing a non-exhaustive list of examples, i.e. name, ID number or reference code.[63] From a terminology point of view, this refers to the “attribute” itself. While it could be well understood that a “name” qualifies as “direct identifier”, this becomes surprising for any “ID numbers or reference codes”. The latter term, literally, contains the concept of “reference”.

References – in common understanding – are indirect identifiers. If a natural person can only be identified by means of “identification numbers” or “reference codes”, the identification will subsequently require a look-up to further information. This logic has been commonly understood as “pseudonymous/pseudonymised” data, while the “reference code” there is understood as “pseudonym” as reflected by EDPB Guidelines 01/2025.[64]

It should be highlighted, that the Guidelines 01/2025 defined “direct identifier” differently from the Guidelines 02/2026. In Guidelines 01/2025, a simple “name” was not considered a (direct) identifier[65]. Instead, a “set of attributes” was deemed necessary, e.g. “first name, last name and date of birth”.[66]

While the aforementioned addressed the terminology on the attribute level, the Guidelines 02/2026 proceed with direct and indirect identification.[67] It remains unclear whether the Guidelines 02/2026 are changing their target of focus deliberately or whether the Guidelines 02/2026 consider their line of argumentation (and target of focus) in continuity.

The Guidelines 02/2026 determine that “direct identification” – which is process level, not attribute level – requires the capabilities to identify the natural person within the very same entity. While – in contrast – “indirect identification” shall require capabilities of at least one other party.[68]

This understanding appears artificially narrow and unnecessarily confusing. While indirect identification may require additional, third-party information, such “externality” is not a given. The Guidelines 02/2026 seems to apply a different understanding of direct and indirect just a few paragraphs later, i.e. in recitals 23 et seqq, 25.

63 Guidelines 02/2026, Rec 19.

64 See Guidelines 01/2025, Glossary.

65 Guidelines 01/2025, Glossary; which seems in accordance with Art. 4.1 GDPR, which might be understood as listing “name” as indirect identifier, while remaining ambiguous, admittedly.

66 This understanding appeared reasonable, because there especially regarding very common names there might be several natural persons with the exact same name. It might even be necessary to add yet another attribute, such as postal codes, to prevent confusion of several individuals, as there might even be multiple “J Doe” born on “1.1.1970”.

67 Guidelines 02/2026, Rec 20.

68 Guidelines 02/2026, Rec 20.

There, the Guidelines 02/2026 stipulate that attributes do not necessarily have to be about the individual concerned but can relate to other individuals and matters. By means of (cross-)data analytics such attributes may still be referred to the individual concerned.

Against this background, the terminology respectively the conceptual framework underlying the terminology remains unclear at best, conflicting at worst. Considering this terminology forms the very core of data protection law as it ultimately affects whether the legal data protection framework applies at all, this is highly unsatisfying if not even concerning.

3.1.2.4 Necessity to Clarify the Relation to Previous Publications

The Guidelines 02/2026 explicitly refer to previous publications regarding anonymisation, namely WP29 Opinion 05/2014[69].

With respect to level of details regarding technical measures and implementation, the Guidelines 02/2026 stay behind WP29's Opinion 05/2014.

This might either indicate that – from the perspective of the EDPB – there has not been any significant, technical development within a decade impacting the concept of anonymity.[70]

This might also indicate that the Guidelines and the Opinion follow different approaches and intents. While the Opinion focuses on the technical and scientific perspective of data analysis and anonymisation techniques, the Guidelines 02/2026 rather focus on the legal perspective by sorting, clustering and elaborating on recent legal developments[71] impacting the qualification of information as personal data.

The Guidelines 02/2026 – unfortunately – remain ambiguous on their relation to WP29's Opinion 05/2014. On the one hand, the Guidelines 02/2026 state they are updating the previous Opinion 05/2014.[72]

By means of common legal methodology, *lex posterior derogat legi priori*, the Opinion becomes respectively became obsolete the moment the Guidelines 02/2026 were published. While this principle technically applies to statutory laws, the EDPB has continuously applied this principle to its own publications in the past, accordingly.

69 WP29, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.

70 Quite the opposite seems the case, the Guidelines 02/2026 clearly claim significant developments since 2014; Guidelines 02/2026, Rec 2.

71 Such might be court decisions, other publications of the EDPB, or legislative initiatives.

72 Guidelines 02/2026, Rec 2.

At the same time, the Guidelines 02/2026 claim to refine the criteria as established by the WP29's Opinion 05/2014.[73] A refinement does not necessarily overrule the existing but might take effect alongside the existing.

That both the WP29's Opinion 05/2014 and the Guidelines 02/2026 shall take effect, might be concluded from the Guidelines statements that any conclusions drawn under the aegis of the Opinion 05/2014 shall remain valid.[74]

3.1.2.5 Establishing Modular, Interrelated Guidelines

Acknowledging the interdependent phenomena of today, it seems reasonable to strengthen modular approaches within legal frameworks in general, within EDPB guidelines in particular.

Exemplary, the modularity could address

- the concepts of "personal data" and "identification" as the very foundation.[75]
  - In accordance with the "lifecycle" approach, see 3.1.2.2, this might already include the fundamentals of pseudonymous and anonymous data.
- establishing on-top elements in distinct guidelines, e.g. for pseudonymisation and anonymisation.
  - e.g. to what extent it will make a difference if data is originally collected pseudonymous / anonymous or whether data will be pseudonymised / anonymised later in time[76]
  - further outlining – and constantly updating – relevant thresholds, e.g. in respect of "means reasonably likely to be used"
    - either a sophisticated and solid methodology
    - or continuously updated examples, that go beyond the already existing decisions of the CJEU, yet transfer such decisions into real life scenarios which are commonly subject to uncertainty
  - further outlining – and constantly updating – any advantages or disadvantages if processing entities (do not) apply certain measures

73 Guidelines 02/2026, Rec 2.

74 Guidelines 02/2026, Rec 2 Footnote 3; "[…] a controller that has assessed a dataset as anonymous in accordance with Opinion 05/2014 before the publication of these new guidelines is not expected to conduct a new assessment".

75 Regardless of whether the content might still be fit for purpose, such an approach might be seen in the early WP29's opinion 4/2007 on the concept of personal data (n 22).

76 E.g. the Guidelines 02/2026 clarify the process of anonymisation will require a justification, Recs 37 et seqq.

Such an approach is also good practice in other fields, e.g. conformity assessment. Some standards respectively families of standards first start with a standard establishing a common terminology, while subsequent standards elaborate on more practical means of implementation.

Such an approach ensures a consistent structure and continuous improvement by the very methodology which is being applied. At the same time it allows for a high degree of flexibility and speed in case of need. Because instead of ensuring consistency across several documents, alongside with the related (majority) decisions to be taken, overarching element will just require the modification at central provisions.

3.2 Expected Impact

Anonymisation is a key element in today's data processing landscape.

Anonymous data is not subject to data protection requirements, neither materially nor formally.

Anonymous data, however, might still create added value as still highly specific and contextual conclusions might be drawn, patterns might be recognised, (conditional) dynamics both in analog and virtual environments can be implemented.

3.2.1 Practitioners' Expectations, Relative Approach

The Guidelines 02/2026 have been long-awaited by practitioners. Practitioners were hoping for clear guidance on how to determine, whether a set of data qualifies as personal or anonymous data.

It is well received that the EDPB aligns with recent ECJ judgments and long-lasting literature opinions that anonymity under GDPR is no absolute concept. Anonymity under GDPR is a legal concept.[77]

As a legal concept, thresholds must be defined. The Guidelines 02/2026 ground the threshold of 'means reasonably likely to be used' primarily in CJEU case law[78]. The EDPB could have anchored the threshold additionally in its primary legal source, Recital 26 GDPR, thereby clarifying that the concept is already enshrined in the GDPR itself. This would have made clear that the threshold is a matter of the Regulation, not merely a variable outcome of judicial interpretation.

77 Guidelines 02/2026, Recs 7 et seq, 26, 29; also Ingenrieth in Nink (n 9), *Anonymisation*, Recs 16, 22, 61, 74; ibid *Pseudonymisation*, Recs 22 et seqq.

78 E.g. ECJ, *SRB* (n 21).

3.2.2 Simplified Approach is Non-Approach

The Guidelines 02/2026 establish a three-step test (see also 3.2.3) for the "contextual approach", unless the "simplified approach" will be applied instead. Apparently, the contextual approach is deemed overly complicated or insufficiently deterministic, which is why the "simplified approach" seems to be introduced.

However, it must be acknowledged that the simplified approach is not anything "simpler" with respect to the exact thresholds. The Guidelines 02/2026 itself call out " this approach is a way to voluntarily shift the risk from false positives to false negatives"[79]

In other words: instead of simplifying the procedure for determining anonymity, the simplified approach is – de facto – rather a shortcut. This approach results in treating data – as a precaution – as "personal data" even where, on the facts, it may not qualify as such.

Strictly speaking, therefore, the simplified approach does not perform a substantive assessment of anonymity. It rather operates as a – business – strategic approach to avoid deterministic decisions and reduce potential liability risks.

While as processing entity – and legal practitioner – such a strategy always exists, it is recommended that EDPB guidelines will address exactly such areas of uncertainty and ambiguity.

Especially, regarding Guidelines 02/2026 it would have been appreciated, if the EDPB would have provided sufficient details in assessing the "means reasonably likely to be used" so that processing entities could be appropriately sure about their assessments.

A more incentivising approach might have been, if the EDPB further elaborated on its (future) assessments on liabilities. Infringements of the GDPR shall be prevented by any processing entity. Where the GDPR is infringed there might be both authoritative remedies and sanctions[80], as well as compensation / damages claimed by data subjects[81].

It is a fundamental principle in law that liabilities generally exist to the extent where there has been a wrong-doing by means of a culpable misconduct.[82] Consequently, the mere fact that – in future – processing entities may wrongfully conclude on the effectiveness and existence of "means reasonably likely to be used" would not necessarily and inherently result in infringing the GDPR through culpable conduct.

79 Guidelines 02/2026, Rec 48.

80 See Arts. 58.2 lit i), 83 GDPR.

81 See Art. 82 GDPR.

82 Exceptionally, the law may provide for strict liability irrespective of culpability.

The Guidelines 02/2026 rather create the impression that the scenarios in mind were of high demanding nature. For those, acting in good faith, at best underpinned with due documentation of their assessment, it appears challenging to prove negligent misconduct, not to mention intentional misconduct.

It is duly noted that the EDPB – given its core purpose is facilitating and promoting the protection of personal data – cannot suggest any actions deliberately undermining the protection of data subjects. On the other hand, the EDPB is not required to set aside principles of best efforts.

On the contrary, the EDPB may accept that – even with best efforts – good faith actions may prove wrong in future. This reflects the fundamental principles of proportionality[83], which is – in the context of GDPR – also referred to as risk-based approach.

One might argue that the simplified approach will (or shall) establish a negative assumption regarding any processing entity that opted-in for the contextual approach. In comparison to entities opting for the simplified approach, such entities, who opted for the contextual approach, shall be deemed as those who deliberately chose false negatives, who deliberately bring data subject at risk. Consequently, whenever their assessment might prove factually wrong in future, the non-use of the "simplified approach" might give reason to establish culpable (negligent) misconduct.

It is recommended to re-evaluate if such line of argumentation has been indeed the intent of the EDPB. Where this line of argumentation should be the intent of the EDPB this approach is strongly opposed. Such an approach flips fundamental principles of liability and good faith.

It is acknowledged that the GDPR does not establish a "good faith" defence as such. However, Art. 83.2 lit. c) and d) GDPR expressly permit the supervisory authority to take into account the technical and organisational measures implemented pursuant to Arts. 25 and 32 GDPR, as well as any actions taken to mitigate the negative consequences of the infringement, and pursuant to Art. 83.2 lit. b) „the intentional or negligent character". The concern is not that a good-faith error should be immune from sanction, but that EDPB guidelines should not create a presumption of negligence merely because a different (more conservative) approach existed. The absence of such a presumption is a matter of the rule of law and the principle of proportionality.

The impact of the Guidelines 02/2026 might remain behind their potentials. First, because the simplified approach and its collateral consequence might backfire, see also 3.2.4.

83 Arts. 58.2 lit i), 83 and 82 GDPR reflect such principle by means of recourse to the element of "culpability". The GDPR refers to the concept of proportionality also across several other articles; explicitly using "proportionate" e.g. Arts. 14.5 lit b), 19, 34.3 lit c), 35.2 lit b) GDPR; using equivalently indicative terms, such as appropriate, e.g. Arts. 5.1 lit e) and f), 12.1, 24.1, 24.2, 28.1, 32.1, 32.2, 46 GDPR.

3.2.3 Non-Deterministic Concept of the "Contextual Approach"

The contextual approach comprises three main elements. Those elements are generally in accordance with elements already acknowledged in practice.[84]

Unfortunately, the Guidelines 02/2026 conceptually establish a negative test. It is understood that it will prove challenging to determine positive thresholds.

On the other hand, a negative test as such appears conflicting with the general findings of the Guidelines and references court rulings.

It is well received that the EDPB recognises recent technical developments. Indeed, these days provide technical capabilities to analyse vast data set in almost no time. This is both a consequence of mere hardware power and algorithmic processes; AI might even provide yet another boost.

This is accompanied with a constant increase in available information. Ultimately, this combination of both increased availability and capability will reshape entire risk frameworks and the conceptual understanding of personal data.

Against this background it was even more important to re-iterate the fact that the GDPR stipulates a relative understanding of identifiability. Therefore, identifiability is a legal concept, with legally defined thresholds. Identifiability is not a binary property of a dataset but a relational, context-dependent assessment that fluctuates with changes in the available means, the identity of the data controller, and the passage of time.

Despite all the objectified consistency, identifiability remains, in this respect, a theoretical (philosophical) concept within the social sciences, and is certainly not a natural science principle.

At some (close) point in time, any of the negative tests might – practically – be impossible to be met. Because, technically, developments and innovation rendered the simple impossibilities test inadequate.

The pressing elements of today lay within the positive determination of "means reasonably likely to be used". The establishment of a continuously maintained assessment framework, with clear guidance with respect to distinct processing contexts and common risk scenarios[85], will most probably provide the expected guidance.

84 Ingenrieth in Nink (n 9), *Anonymisation*, Rec 51.

85 Based on different elements, such as data categories involved, exposure of the processing entity or the data subjects concerned, potentials for (abusive) re-use of (identified) data, or just the economic value of the (identified) data.

It is therefore recommended to establish such framework, which (at best) positively determines the means reasonably likely to be used related to the respective processing contexts.

Such an approach starts at the determination of "related to a natural person". Electronic devices are used significantly different today, as compared to the early days of data protection law or even at the time of the publication of the WP29's Opinion 04/2007[86].

While in the early days of the internet it was rather common that both the "Internet Access Point" and the device used for such access were shared media, there is "mobile-first habitus" today. Such a "mobile-first habit" correlates with a higher degree of individually used devices and internet access points.

However, shared media still exist. The simple possibility of respectively claim of a "shared medium" suffices in other criminal and civil law to break the chain of causation or attribution to an individual.[87]

It would be beneficial in practice to determine a distinct gradient or at least the relevant factors of concern to conclude on identifiability (with respect to relation to a natural person), where primarily technical identifiers are being processed.

This concept can be transposed to any other aspect of the three relevant tests.

The Guidelines 02/2026 apparently acknowledge the challenges created by the negative test and the potential impossibility. The Guidelines 02/2026 stipulate that even if one (or more) of the test will fail, this will not automatically result in the impossibility of the assumption of anonymous data. It is rather that in those cases, where one (or more) tests fail the processing entity that seeks to maintain the claim of anonymity must then evaluate the possibility of additional (mitigating) measures and implement those accordingly.[88]

As a result, the Guidelines 02/2026 might create more ambiguity than they resolve.

3.2.4 Backfiring Incentives

De facto, the Guidelines 02/2026 appear to leave practitioners without any distinct guidance. More concerningly, the Guidelines 02/2026 risk establishing an indirect presumption that operates to the detriment of processing entities acting in good faith.

The EDPB could have established incentives for processing entities to anonymise data as much as possible. The "benefit" regarding formalities come along with practical "disadvantages", i.e. material costs in losing information quality.

86 See (n 22).

87 Exemplarily it shall be made reference to "file sharing" activities.

88 Guidelines 02/2026, Rec 52.

Likewise, if a processing entity was about to anonymise data to the best of their knowledge and in good faith prior transfer to a receiving party, this would always be to the benefit of the data subject.

- First, the data at the transferring party was subject to the high level of protection under the GDPR anyway.
- Second, if the data is fully anonymised, the data – under the logic of the existing legal framework – result in minor risks to the data subjects; so minor that no additional layer of protection as established by the GDPR was deemed necessary by the legislator.[89]
- Third, if the data – originally fully anonymised – is legitimately or illegitimately enriched so that the data qualifies as personal data, such data will be subject to the GDPR.

Excessively complicating the process of anonymisation does not fill any gaps protection that otherwise would occur.[90] But an overly protectionist approach, i.e. adding a second layer of "GDPR application" without legal necessity, might backfire.

If a processing entity would fall under the regime of the GDPR anyway, such processing entity would not have any benefit compensating the material loss of data quality. Apparently, the processing entity did have a justification[91] to process the personal data. It is therefore likely, that the processing entity will have a justification for the processing activity which otherwise was performed with anonymised data.

Indeed, there might be business models that abusively claim anonymous data to monetise personal data illegitimately. It is worth mentioning that such illegitimate processing activity would already be infringing the GDPR. And if the data was not properly anonymised, the GDPR would still remain applicable. This even will hold true in case of international data transfers, because the territorial scope of the GDPR is hardly limited.[92]

If it remains a matter of enforcement: Where a compliance obligation is imposed on entities acting in good faith while the same obligation is not effectively enforced against entities acting in bad faith, a concern arises under Art. 20 EU CFR[93] and the principle of proportionality. The EDPB should address this asymmetry, either by clarifying the conditions under which a good-

89 It is worth noting that, even if the GDPR is not applicable, data subjects are still protected. It is just that data subjects would have to make up their cases more thoroughly, might have to prove any harms, et al.

90 In this respect, also ECJ, *SRB*, 85; also Ingenrieth, *Opportunities to Reduce Bureaucracy* (n 9).

91 Legal bases, e.g. as provided by Art. 6 GDPR.

92 Art. 3 GDPR, here most importantly Art. 3.1 GDPR.

93 Re-confirming from a German constitutional perspective, BVerfG, Decision 4 November 2024, 1 BvR 1177/22, Rec 20.

faith anonymisation assessment is protected from subsequent reclassification, or by acknowledging that the simplified approach, as a voluntary risk-allocation mechanism, should not generate adverse effects regarding the good faith of entities that chose the contextual approach.

The Guidelines 02/2026 should be designed so that processing entities acting in good faith and in accordance with the intent of the GDPR, especially in the sense of data minimisation, will not be exposed to liability, let alone trapped in it, for having misjudged the "means reasonably likely" to be used. It is a matter of proportionality to not unduly and in this respect excessively limit the possibilities as provided by the GDPR to those acting in good faith just because there are others who strategically undermine the GDPR.

Against this background it is also recommended to conceptually analyse whether EDPB's publications remain consistent and whether existing (legacy) approaches are still fit for purpose (see also 3.1.2, 3.1.2.2, 3.1.2.3, 3.1.2.4).

3.3 Realistic Expectations

The Guidelines 02/2026 should further outline and build upon realistic expectations, especially, in respect of how to determine "means reasonably likely to be used".

Currently, the Guidelines 02/2026 fall short on establishing contextual thresholds. The partially extensive interpretation of the law and its related ECJ decisions, might be misinterpreted in re-instating the logic of a *de facto* absolute approach.

If the burden of assessing means reasonably likely to be used in practice become disproportionate to the processing activity and if the Guidelines 02/2026 maintain their ambiguity regarding the establishment of a preliminary assumption of culpability[94], the opportunities granted by the relativity will dissolve.

It is therefore recommended to further evaluate which elements might affect the result of the applied methodology. Those elements might relate to[95]:

- rigour in respect of "expected" means regarding their level of sophistication, based on, e.g.
  - the categories of personal data involved
  - the potential of abuse of the personal data to (fraudulently) create economic value
- whether the processing of personal data defines the core business activity of the processing entity

94 See 3.2.2.

95 It is well noted that the Guidelines 02/2026 already refer to those elements, see Guidelines 02/2026, Rec 33.

- the size of the involved parties

It is important that none of those elements should establish automatisms lowering the level of data protection. Even small-sized companies may perform processing activities resulting in highest risks for personal data; *vice versa*: even large corporations may not process personal data in a way the related risks exceed the general risk of everyday life.

However, those elements might act as useful indicators for processing entities, how far their assessment of means reasonably likely to be used will reach.

While the Guidelines 02/2026 indicate that such elements might influence the extent of a processing entities assessment, the Guidelines 02/2026 lack of deterministic elements. Indeed, the Guidelines 02/2026 include examples. However, such examples either refer to obvious scenarios or remain too high-level that practical consequences could be drawn.

This also relates to the findings regarding expected breaches of law.[96] The ECJ noted in its decision (*Breyer*)[97] that the assessment of means reasonably likely to be used must take account of the lawfulness of the means. The Guidelines 02/2026 develop this into a general principle, first restating the ECJ by concluding such means must not be legally prohibited[98], then second, further qualifying this principle by reference to the effective enforcement of the legal prohibition.

This second, rather interpretive step by the EDPB should be expressly identified as such, with a clear statement of the conditions under which a contractual or statutory prohibition is to be disregarded in the assessment.

The EDPB generally creates the impression that processing entities still shall evaluate potential illegitimate, criminal actions of third parties. Positively, the EDPB highlights, such elements shall only become relevant, where there is sufficient evidence that in practice a legal prohibition is constantly ignored.[99]

Still, the conclusions of the EDPB remain surprising and confusing. The question remains unresolved why the legal prohibition is being constantly ignored. If such ignorance correlates with a lack of law enforcement one might focus on the effective law enforcement rather, first.

As the Guidelines 02/2026 refer to “the parties involved” only by means of an “in particular” statement, the Guidelines 02/2026 appear to de facto extend the assessment of expected breaches of law to be generic. This would totally negate the ECJ ruling that a legal prohibition shall make such means irrelevant for the assessment.

96 Guidelines 02/2026, Rec 33.

97 ECJ, Judgment 19 October 2016, C-582/14 (*Breyer*), ECLI:EU:C:2016:779.

98 ECJ, *Breyer* (n 97), Rec 46.

99 Guidelines 02/2026, Rec 33.

A transferring party should – when assessing the risks for re-identification – assess only legitimate means. The means reasonably likely to be used by a receiving party may evolve over time. Accordingly, the transferring party shall re-assess its conclusions.

Primarily, the transferring party should assess any means available to the receiving party of which the transferring party has positive knowledge. Secondly, it should assess additional means, which are supposedly likely to be or become available to the receiving party.[100] Thirdly, one might expect that, once the transferring party becomes aware of any other means available to the receiving party, the transferring party will re-assess its conclusions in due time.

Against this background, it should be clarified that, not in particular, but only if the transferring party evidently becomes aware of the receiving party using illegitimate means the transferring party shall take this into consideration.

Likewise, the interpretation of the EDPB, that prohibited by law relates to statutory laws only, and does not include contractual provisions, remains within the possible intent of the ECJ. However, it should be noted, that the underlying decision of the ECJ might also give leeway to consider contractual provisions as equivalently relevant. In this respect, the EDPB should clarify the Guidelines 02/2026.

The Guidelines 02/2026 may be read as giving contractual provisions little or no effect.[101] The EDPB refers to the powers of the parties to disregard contractual provisions at any time. While this is true, the EDPB seems to unnecessarily mix-up several status.

If the parties involved contractually agree upon several obligations and prohibitions in order to maintain the level of protection of data subjects, i.e. in this case ensure that any data being transferred remains qualified as anonymous, such contractual provisions must – *prima facie* – be sufficient.

The same factual assumption underlying the treatment of statutory prohibitions, that parties will comply with their legal obligations,[102] must apply equally to contractual safeguards.

100 At this point in time the assessment becomes highly assumptive and probabilistic. The conclusion is not based on the de facto processing but on mere potentials. For the time being, this seems a consequence of the GDPR and its broad definition of personal data which is not limited to "identified" natural persons but includes merely "identifiable" natural persons, too.

101 Guidelines 02/2026, Rec 34.

102 Guidelines 02/2026, Rec 33; there it is paraphrased by "people will follow the law".

It shall be agreed, though, that – for contractual safeguards – the mere paper must not be enough evidence for effective protective measures. The transferring party must provide reasonable means[103] to monitor contractual compliance.[104] But as long as there is no evidence of collusion or systematic breach of contract, contractual provisions should take similar effects as statutory laws.

To the extent the EDPB refers to the powers of the parties to deliberately disregard contractual provisions, this will require an "action" by both parties. In this respect, the assessment must be re-performed in the light of the then – amended – processing context.

In general, the Guidelines 02/2026 should establish more stringent coherence across the lifecycle of data, even across entities. Data subjects are not rendered without protection in most of the risk scenarios. It is rather that data subjects, in cases where anonymous data is being enriched, will have to reach out to this additional controller, instead of reaching out to the original controller.

The transfer of data is not limited to processor-relationships. It can at all times – even in case of the transfer of personal data – relate as well to controller-controller relationships, joint-controllerships. Therefore, data subjects are not less protected, conceptually, if the receiving party of "anonymous" data subsequently qualifies itself as controller.

Instead of extending the preventive nature of the GDPR, potentially creating overly burdensome scenarios, the EDPB might include distinct guidance in respect of the relevant transparency obligations in those scenarios. While Art. 14 GDPR provides exceptions regarding the obligation to pro-actively inform data subjects about their data being processed, the Guidelines 02/2026 might elaborate on the applicability of such exceptions. The Guidelines 02/2026 might even conclude that – in order to balance the various interests and mitigate the risks for data subjects – certain exceptions shall not apply – at a minimum in reasonably distinct contexts.

103 Which should be determined by future iterations of the Guidelines 02/2026.

104 In general it should suffice to maintain a reactive process in cases the receiving party becomes aware of distinct breaches. However, for high-risk context or in case of prior adverse experience, proactive means might be required, gradiently.

4 Specific Observations

The Guidelines 02/2026 provide some aspects that require further analysis. Such elements might be of specific concern because due to their ambiguity, or because they might be interpreted excessively, or because their positive effects might be increased if further elaborated on.

4.1 Attribution of Capabilities Across the Processing Chain

The EDPB should clarify its intent regarding Recital 15 of the Guidelines 02/2026.

This section might be understood as a clarification that within the context of a processor-relationship, no "transfer" of data in the sense of the Guidelines 02/2026 takes place anyway. Such a conclusion seems reasonable.

Likewise, this section might be (mis-)understood in a way that it extends the applicability of both the Guidelines 02/2026 and – potentially – the GDPR itself.

It is first to be highlighted that, indeed, a transfer of data between a controller and its processors (or a processor and its sub-processors) is not identical to the transfer of data in the sense of the Guidelines 02/2026. If data is transferred to a processor, the parties involved apparently assume a transfer of personal data. This is a requirement for the applicability of Art. 28 GDPR: First, only if personal data is processed, the GDPR might apply at the level of the controller. Second, Art. 28 GDPR refers to personal data, too, both implicitly[105] and explicitly[106].

Therefore, processors are of no relevance in receiving "anonymous" data. It would have been appreciated if the Guidelines 02/2026 clarified the consequences of "precautionary contractual safeguards". This refers to scenarios, where controllers transfer demonstrably anonymous data but establish precautionary contractual safeguards; it is the understanding of these Comments, that such precautionary contractual safeguards will not artificially and collaterally qualify the receiving party as a processor within the meaning of Art. 28 GDPR. This must be the case, whether the contract only provides the safeguards, as e.g. mentioned by the Guidelines 02/2026 in Recital 34, or whether the contractual safeguards – precautionary – foresee fallback mechanisms in cases where the supposedly anonymous data proves personal data at a later point in time.

105 Implicitly, because Art. 28 GDPR might only apply, if the GDPR applies in general, second, Art. 28 GDPR refers to the concept of processing, which is defined by Art. 4.2 GDPR as any operation on personal data.

106 Explicitly, as Art. 28.3 refers to personal data, e.g. by stating "the type of personal data and categories of data subjects", or in lit a), b) or g) by stating "personal data".

In the processor relationship under Art. 28 GDPR, the personal data of data subjects are protected primarily through the controller's obligations. Processors are, in effect, simple "extended arms" or "implementers" of the controllers but do not qualify as an individual "processing entity"[107].

In other words – which is equally reasonable – the transfer of data to a processor is never sufficient to argue for an efficient anonymisation. The Guidelines 02/2026 might clarify on this.

On the other hand it seems inappropriate to automatically and unconditionally attribute capabilities of processors to their controllers. Where the controller contracts a processor with the intent to use such capabilities, there must be an attribution. This should also be the case if such capabilities form part of the generally provided service regardless of whether the controller de facto intends to use them.

A different stand should be taken where such capabilities of the processor are not part of the provided external services, nor otherwise made available in the course of the processing of received data in its capacity as a processor. Because if such services are not intended to be available to the controller, any attribution would confuse the roles of the parties involved.

For the sake of clarity: if the controller transfers data to a processor (a) in its capacity of a processor and additionally (b) in its capacity of an individual or joint controller, in cases of the latter the capabilities certainly might be attributed.

It is recommended that the Guidelines 02/2026 further elaborate on the different relationships and distinct roles of the parties involved.

On another note this section might be misinterpreted to extend the general application of the GDPR. E.g. where the transferring party does not fall within the scope of the GDPR – e.g. due to the household exemption or due to a lack of automatic means of processing -, yet the receiving party would not qualify for any or all exceptions, an unconditional attribution of capabilities (and obligations) might unreasonably extend the GDPR scope. The Guidelines 02/2026 should clarify that this has not been the intent of this section.

4.2 Attribution of Capabilities by "Meaningful Connection"

As already elaborated in 3.1.1.3 underlying ECJ decisions might also be interpreted differently.

But even if the approach of the EDPB would be applied, the Guidelines 02/2026 appear inconsistent. On the one hand, the Guidelines 02/2026 seem to establish an unconditional attribution amongst all entities who may have access to the data along the processing chain.[108]

107 This does not prevent the GDPR from establishing joint liabilities of controllers and processors.

On the other hand, reading Recital 15, Example 4, the relevant perspective shall be limited to the one of the research institute, „[s]ince it is acting independently" and „[t]he data will never be returned to the hospital".

Against this background, the EDPB seems to establish rather a gradient of attribution, considering the technical and organisational measures in place. Such a gradient also reflects the general proportionality principle under the GDPR. Therefore, the EDPB should further elaborate on the elements necessary to affect the attribution positively with regard to resulting in anonymous data.

For the time being, the Guidelines 02/2026 rather focus on potentials from a negative point of view. In other words: the Guidelines 02/2026 do not assist in determining the measures relevant to establish anonymous data; the Guidelines 02/2026 rather list elements by which identifiability will not be sufficiently reduced.

Those elements are neither presented in a deterministic fashion but in a probabilistic manner. Processing entities should take the presented elements into account and shall be aware of existing risks that will require mitigation. The Guidelines would significantly benefit from establishing good practices with concluding that – provided the measures as provided by the Guidelines 02/2026 are applied – data will be legally considered as anonymous data.

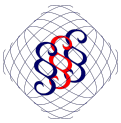
It is acknowledged that the Guidelines 02/2026 already integrate examples, which apparently are intended to indicate good practices. However, the provided examples are either too obvious cases, which in practice would not create any concerns, or might be read as partially inconsistent across the entire document, therefore resulting in more questions than providing answers, or lastly, or remain too high-level or too specific in nature, at least subtly indicating between the lines that such examples might not be transferred to other scenarios without performing an entire, individual assessment.

If the EDPB indeed considers a gradient applicable, the Guidelines 02/2026 should clarify and then – consistently – elaborate along such gradient potential risks, potential mitigations and good practices. In this respect, the Guidelines might also clarify on elements, such as contractual measures, and their potentials, see also 3.3.

4.3 Anonymisation as Processing Activity

The Guidelines 02/2026 take a clear stand on the debate whether anonymisation reflects a processing activity which will require a justification. Considering the GDPR in its current wording, the EDPB's conclusion seems reasonable and accurate.

108 Guidelines 02/2026, Rec 9 – "other entities (or chain of entities)"; Rec 28 – "chain of means", "The chain of means includes any transfer of the given data to (or access by) an entity that is involved in the respective identification process."



950 However, the Guidelines 02/2026 should further distinguish between the individual steps and
951 – subsequently – outline the legal bases suitable for each step.[109]

952 4.4 Anonyms – Data vs Data Set vs Database

953 The Guidelines 02/2026 clarify that the relevant target of evaluation shall always be the data
954 (set) attributed to an individual. In this respect, the perspective is distinct and narrow. Within a
955 broader database comprising a multitude of data (sets), some data (sets) may qualify as per-
956 sonal data while others remain unidentifiable and thus "anonymous".[110]

957 Additionally, the Guidelines 02/2026 appear to reasonably distinguish the perspective at the
958 time of transfer. Apparently, they conclude that if an entire "database" is to be transferred
959 which comprises a mixture of anonymous and identifiable data (sets) this transfer shall be con-
960 sidered a transfer of "personal data".

961 Probably, the EDPB intended this conclusion assuming that the transfer (and/or anonymisation
962 process) is not capable of distinguishing the different scenarios or where the processing or
963 transferring party is not willing to apply the efforts to distinguish such scenarios.

964 To maintain the legally required level of data protection, such a simplified and practical reflec-
965 tion is welcome. However, the Guidelines 02/2026 should further outline that, provided a dis-
966 tinction per data (set) remains possible and will be applied, the legal status of each data (set)
967 is to be assessed individually, thus the perspective remains per data (set) and conclusions will
968 be drawn accordingly.

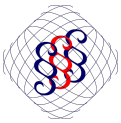
969 4.5 Anonymisation as "storage limitation"

970 It is an ongoing debate whether – effectively anonymised data – is a functional equivalent to
971 "deletion or otherwise render inaccessible" in respect of controllers' obligations to comply with
972 the requirements of "storage limitation".

973 It is highly welcome that the Guidelines indicate that anonymisation indeed might be a func-
974 tional equivalent. It is acknowledged that the Guidelines 02/2026, yet, do not take a final
975 stand which would be appreciated, though.

109 See also, Ingenrieth in Nink (n 9), Anonymisation, Recs 63 et seqq.

110 Guidelines 02/2026, Recs 36 et seqq.



However, they mention "This includes anonymisation that does not lead to a deletion of the original data and so does not contribute to storage limitation. These guidelines do not, therefore, provide guidance for the interpretation of existing specific legal provisions that may mandate erasure of the original data."[111] Therefore the Guidelines, subtly and *a contrario*, admit that anonymisation might contribute to storage limitation where the original data will be deleted.

This seems a reasonable approach. Where data has been effectively anonymised, it ceases to be "personal data". Consequently, the GDPR no longer applies. Accordingly, any storage limitation obligation as provided by the GDPR no longer applies to it either.

The data subject's protection is not diminished: Even though the anonymised data is outside the GDPR's scope, data subjects retain the protections afforded by applicable non-GDPR law (e.g. national civil law, sector-specific regulations).

It would be appreciated in practice, if the Guidelines would confirm this, subject to the caveat that the anonymisation must be effective and durable at the time of assessment.

It must also be noted that, had the data in question been collected in anonymised form from the outset, the same analysis would apply.[112] The level of protection for data subjects appears functionally identical.

4.6 Extending the "relativity" within one entity / corporation

While the Guidelines 02/2026 appreciate and confirm the relativity where several entities are meaningfully connected, the EDPB – *vice versa* – appears to continue the interpretation and approach that information will always be attributed across several departments within one entity.

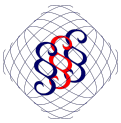
From a logical point of view this would apply, in cases where one entity has control over another entity – be it based on the corporate structure or the probable identity of personnel.

However, against the background of the Guidelines 02/2026 findings, that the relativity should be based on the effectiveness of the implemented technical and organisational measures, it seems worth considering the reversed approach as feasible, too.

This being said: If – within one entity – information will be shared across departments it seems worth evaluating the potential positive effects if anonymity could apply. If the concept of anonymity remains rejected by mere formal elements (corporate structure, being one entity), this might prevent processing entities from reducing the amount of personal data; knowing that the entire regime of the GDPR will apply anyway.

111 Guidelines 02/2026, Rec 10.

112 See also Ingenrieth in Nink (n 9), Anonymisation, Recs 80 et seqq.



However, it is already established that – even if is considered "controller" as entire entity – the entity must implement appropriate technical and organisational measures, including internal access controls (Art. 32 GDPR). In other words: the processing entity is – already under the regime of the GDPR – forced to implement strict access controls, separation of different (categories) of information, to ensure that only those departments and personnel may access the information as necessary for their task and purpose.

This requirement – as the case may be – even applies within one and the same department by means of: case handlers shall only have access to those cases they are assigned to, rather than to any cases of such department.

It is recommended to evaluate the consistency of those approaches across the requirements of the GDPR and – alongside – develop a coherent (metrical) framework within the Guidelines 02/2026 (or an overarching EDPB guideline, as suggested in 3.1.2.5).

Public Consultation – European Data Protection Board (EDPB)

Guidelines 02/2026 on Anonymisation

October 2026

Frank Ingenrieth, LL.M., Registered Lawyer

