Verbraucherzentrale
Bundesverband

Anonymisation is relative – Accountability must not be

vzbv comments on the European Data Protection Board's "Guidelines 2/2026 on Anonymisation"

28. Oktober 2026

Content

I. Relevance for consumers 3

II. Executive summary 3

III. Introduction 4

IV. Detailed comments 5

1. Applicable Perspectives, Disclosures and Continuity of Accountability 5
2. Means Reasonably Likely to Be Used 7
3. Accountability and Reassessment 8

Imprint 11

I. Relevance for consumers

Whether information is treated as personal or anonymous has direct consequences for consumers. Once information is genuinely anonymous for an organisation, the General Data Protection Regulation (GDPR) no longer governs that organisation's processing of it. Rights to information, access, rectification, erasure and objection, together with the safeguards provided by accountability requirements and independent supervision, are then no longer applicable. Any conclusion that information is anonymous must therefore rest on a reliable assessment.

This is increasingly relevant in digital services, personalised advertising, data brokerage and AI-supported processing. Individuals are often identified without their name through persistent identifiers, device characteristics, behavioural patterns or the combination of information from different sources. Data may also pass between several organisations, each of which holds only part of the information or technical capability needed for identification.

A clear and consistently applicable framework is essential to reflect these realities and to ensure that GDPR's protective provisions apply wherever individuals can still be recognised, singled out or treated differently. The legal status of data should depend on actual identifiability within the relevant processing context, not merely on the formal separation of identifiers, datasets or functions. Such a framework can strengthen trust in data use and provide legal certainty for organisations across the Union.

II. Executive summary

The Guidelines address an important need for legal clarity on anonymisation within the existing GDPR framework. Their contextual approach recognises that the same information may be personal for one entity and anonymous for another, depending on the means reasonably likely to be available to each. It also reflects that identification does not require knowledge of a person's civil identity and that relevant information and capabilities may be held by other entities or distributed across a chain. Precisely because the assessment is relative to each entity and context, the final Guidelines must ensure that individuals' rights and accountability do not become fragmented while individuals remain identifiable within the relevant processing environment. The EDPB should:

- **Clarify the general application of paragraph 21.** The Guidelines should make explicit that, where a recipient can identify an individual using means reasonably likely to be used, the disclosure must be treated as processing of personal data, even if the disclosing entity does not itself have the means to identify the individual. This principle should apply to actual, intended and reasonably foreseeable disclosures, including public disclosures, targeted disclosures and multi-stage processing chains. The assessment should take account of the parties' roles and recipient capabilities, while data provenance, transparency and data subject rights must remain effective throughout those chains. A practical example involving adtech or data brokers would help illustrate its application **(para. 21)**.

- **Provide clearer criteria for assessing means reasonably likely to be used.** The Guidelines should clarify that "sufficient evidence of a concrete risk" does not require proof that a named actor is planning a specific unlawful identification attempt. They should also provide practical criteria for adequate safety margins and make clear that appropriate security controls do not automatically exclude unauthorised actors from the assessment **(paras 33 and 88–89)**.
- **Strengthen accountability, documentation and reassessment.** The Guidelines should clarify when an entity can no longer rely on a previous anonymity assessment, identify typical reassessment triggers and explain when and with what consequences previously anonymous data become personal data for the relevant entity. They should also provide minimum requirements for documenting claims of anonymity and enabling effective supervisory verification, including where anonymity depends on continuing conditions at independent recipients **(paras 35 and 41–42)**.

III. Introduction

The European Data Protection Board's (EDPB) "Guidelines 2/2026 on Anonymisation" update the Article 29 Working Party's Opinion 05/2014 in light of legal, technological and practical developments.[1] Clear, robust and consistently applicable criteria are essential because the classification of information as anonymous determines whether the protections of the GDPR apply. Such criteria must safeguard individuals while also providing legal certainty for organisations across the Union.

The central challenge is to ensure that a contextual assessment of anonymity preserves protection and accountability throughout relevant processing steps and disclosures. Neither individuals' rights nor organisational responsibility should be weakened merely because data, additional information or identification capabilities are distributed between different entities. This submission therefore focuses on a limited number of legal issues that are particularly important for maintaining accountability and enabling individuals to exercise their rights effectively. It also addresses those parts of the technical framework that directly shape the application of the legal standard.

Against the background of the debate on the proposed changes to the definition of personal data in the Digital Omnibus, the final Guidelines can provide the necessary legal clarity within the existing GDPR framework by developing the implications of the CJEU's case law while preserving the existing scope of protection.[2] The Federation of German Consumer Organisations (vzbv) welcomes the public consultation and thanks the EDPB for the opportunity to comment.

---

[1] European Data Protection Board: Guidelines 02/2026 on Anonymisation, 2026, https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en, accessed on 28 October 2026.

[2] European Data Protection Board and European Data Protection Supervisor: Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 2026, paras 15–19 and 21, https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf, accessed on 28 October 2026.

IV. Detailed comments

1. Applicable Perspectives, Disclosures and Continuity of Accountability

The Guidelines rightly recognise that anonymity cannot be assessed in isolation. **Paragraphs 11 to 15** ask for whom the data are intended to be anonymous and focus on the actual processing context. Relevant factors include access to and control over the data, transfers between parties, their relationships and whether an entity processes data on behalf of another organisation.[3] As modern processing often involves service providers, intermediaries, platforms and data brokers, the relevant perspectives should follow the actual use and movement of the data rather than formal descriptions or organisational boundaries.

Public disclosure illustrates how the relevant perspective must reflect the foreseeable audience. In Example 1, which draws on *OC v Commission*, the Guidelines recognise that this audience may include investigative journalists with research capabilities beyond those of an average reader. The assessment cannot therefore be limited to the perspective of the average public where foreseeable members of that audience have greater means to identify the person concerned.[4]

The applicable perspective also depends on the parties' roles. **Paragraph 15** prevents outsourcing from changing the assessment: a processor cannot treat data as anonymous merely because it does not itself hold the information needed to identify the people concerned. The controller's perspective remains decisive. However, the Guidelines should also clarify how the perspective is determined where joint controllership has already been established and identification means are distributed between the parties.[5]

The need to consider the recipient's perspective also applies to targeted disclosures. Where an organisation intends to make data available to a particular recipient or category of recipients, it cannot assess anonymity solely by reference to its own technical capabilities. The recipient's realistic access to, or legal means to obtain, supplementary information, matching services or other identification tools forms part of the disclosure context. **Paragraph 21** is central in this respect. Where a transfer to a third party is reasonably likely and the recipient may identify the individual using means reasonably likely to be used, the data must be treated as personal data for the transfer and the recipient's subsequent processing. Paragraph 21 further states that the transferred information also becomes indirectly personal for the transferring entity, even where it

---

[3] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 11–15. The Guidelines identify access, control, transfers, relationships between parties and processing on behalf of another entity as relevant factors.

[4] Court of Justice of the European Union, judgment of 7 March 2024, *OC v European Commission*, C-479/22 P, paras 52–64, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0479, accessed on 28 October 2026; EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 12 and Example 1.

[5] EDPB and EDPS, Joint Opinion 2/2026 on the Digital Omnibus, cited in fn 2, para 19 and fn 29. The Joint Opinion refers to two related questions raised following EDPS v SRB: whether data may remain personal for a processor that does not itself have the means to identify the individuals and whether an entity may be a joint controller where it helps determine the purposes of processing but lacks such means. Paragraph 15 of the Guidelines addresses the first question by making the controller's perspective decisive for processing carried out on its behalf but does not provide an equally explicit answer to the second. See also EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 9 and fn 7.

could not otherwise identify the individuals itself.[6] By disclosing data to a recipient that can identify the individual, the disclosing entity itself creates the additional data protection risk that justifies taking the recipient's capabilities into account.

These principles are particularly important in chains involving more than two actors. Company A may collect personal data and remove direct identifiers before transferring them to an intermediary, company B. B cannot identify the individuals using its own information but makes the data available to company C, which can match them with customer records, device identifiers or other data and use the resulting profiles to treat people differently. C does not return any identifying information to company B.

The anonymity assessment for B, however, cannot be limited to B's own identification capabilities where disclosure to C is intended, reasonably foreseeable or forms part of B's business model or technical architecture. C's capabilities are particularly relevant where B selects or structures the data for C, provides an access interface or otherwise prepares the data for combination with other information. An intermediary should not turn a connected processing chain into steps supposedly outside the GDPR.

The assessment should focus on actual, intended and reasonably foreseeable disclosures. Relevant factors include the purposes of the processing, the business model, the technical design, contractual relationships and established disclosure practices. Paragraphs 9, 13, 20, 21 and 28 already provide the basis for such an assessment. Further practical guidance would help organisations and supervisory authorities apply these provisions consistently to targeted transfers, platform access, data broker chains and other multi-stage processing operations.

Furthermore, the contextual nature of anonymity must not undermine transparency or the effective exercise of data subject rights. Drawing on *EDPS v SRB*, Example 2 explains that the obligation to inform data subjects about recipients must be assessed from the controller's perspective at the time of collection. Where the information was personal data for the collecting controller, its later transfer qualifies as a transfer of personal data for that obligation, irrespective of whether the recipient can identify the individuals.[7] People should not lose information about where their data have been sent because an intermediary or recipient considers the information anonymous from its own perspective.

So, where C acts as a controller and can identify or individually treat people, it must have a lawful basis and comply with the GDPR for its own processing. This does not answer, however, whether B was allowed to disclose the data. Where paragraph 21 applies, B's disclosure is itself subject to the GDPR, with the applicable obligations depending on the roles of the parties. Responsibility must not disappear merely because B treats the data as anonymous and the individual becomes identifiable only after C links the data with additional information. By then, the original source, earlier purposes and intermediate recipients may no longer be visible to the person concerned.

---

[6] Court of Justice of the European Union, judgment of 9 November 2023, *Gesamtverband Autoteile-Handel v Scania*, C-319/22, paras 45–49, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0319, accessed on 28 October 2026; Court of Justice of the European Union, judgment of 4 September 2025, *European Data Protection Supervisor v Single Resolution Board*, C-413/23 P, paras 84–85, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0413, accessed on 28 October 2026; EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 20–21; EDPB and EDPS, Joint Opinion 2/2026 on the Digital Omnibus, cited in fn 2, para 16.

[7] Court of Justice of the European Union, *European Data Protection Supervisor v Single Resolution Board*, cited in fn 6, paras 102–103 and 108–111; EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 14 and Example 2.

This can substantially weaken data subject rights in practice. A person may know the original service but not intermediary B or company C using the resulting profile. A downstream recipient may hold a profile or identifier but lack complete information about the original source. Rectification, erasure or restriction may not reach other recipients if disclosures and recipient records have not been maintained. The same problem can impair the effective exercise of the right to object.

The Guidelines should therefore address the interaction with Articles 13 to 19 and 21 GDPR. They should clarify what information about sources, disclosures and recipients organisations need to preserve to support transparency and the effective exercise of access, rectification, erasure, restriction and objection. This does not require organisations to retain additional identification keys where these are not necessary. It requires data-minimising records of provenance and recipients so that rights do not end at a supposedly anonymous intermediate stage.

> The EDPB should clarify **paragraph 21** as a general principle for actual, intended and reasonably foreseeable disclosures, including public disclosures, targeted disclosures and multi-stage processing chains, and explain how transparency, data provenance and the effective exercise of data subject rights remain protected throughout those chains. In doing so, the assessment should reflect established processing roles and take into account the recipient's capabilities as well as any selection, structuring, enrichment or technical preparation carried out for the disclosure. A practical example involving an intermediary in an adtech or data-broker chain could illustrate that C's own GDPR obligations do not replace the assessment of B's disclosure

2. Means Reasonably Likely to Be Used

The Guidelines are right to interpret "means" broadly. Relevant capabilities or additional information may be held by another organisation, and **paragraph 28** requires consideration of whether a "chain of means" can bring the necessary elements together. This is essential in processing environments where identification capabilities are distributed between several actors. The EDPB should maintain this position.[8]

Paragraph 34 also rightly makes clear that a contractual prohibition on re-identification is not equivalent to a prohibition by law. Contracts may reduce the likelihood that certain means will be used, but only as a complement to effective technical restrictions. They should not allow organisations to treat data as anonymous where access to identifying information or technical means remains reasonably likely in practice. The EDPB should not weaken this position.[9]

The effect of legal prohibitions requires careful contextual assessment. **Paragraphs 32 and 33** identify relevant factors such as monitoring and enforcement, the deterrent effect of sanctions, incentives to infringe the law, previous breaches and practical protection against unlawful access. However, the requirement for "sufficient evidence of a concrete risk" needs further clarification.[10] It

---

[8] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 28 and Example 7.

[9] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 34.

[10] Court of Justice of the European Union, judgment of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, para 46, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582, accessed on 28 October 2026; Court of Justice of

should not require proof that a named actor is already planning a specific unlawful identification attempt. Persistent enforcement deficits, repeated infringements in the relevant sector, known methods of circumvention and strong economic incentives may together demonstrate a concrete risk. The assessment must also consider whether relevant actors fall outside the effective scope of the prohibition.

The Guidelines are also right to take technological developments into account. **Paragraph 88** recommends adequate safety margins, while paragraphs 92 and 93 recognise that identification techniques may become cheaper and more accessible and that AI may reduce the time and cost needed to combine information from different sources.[11] The concept of an "adequate safety margin" nevertheless requires more practical guidance. Relevant factors should include the expected duration of the processing or availability of the data, their resolution and dimensionality, the likely emergence of additional information, the number and types of actors with access, foreseeable technological developments, the value of successful identification and the expected robustness of the safeguards over time. The margin should ensure that the anonymity assessment remains reliable throughout the period in which the data are expected to be used or accessible.

The treatment of unauthorised actors also requires clarification. Paragraph 30 expressly recognises that relevant actors may include rogue employees, unethical companies, foreign intelligence agencies and cybercriminals. **Paragraph 89** could nevertheless be read as excluding unauthorised actors from the risk assessment whenever appropriate security controls are in place. Appropriate security controls reduce the likelihood of unauthorised access, but they should not automatically remove such actors from the assessment. Paragraph 90 and Example 22 already recognise that even strong security measures may not prevent leaks caused by human error or external attacks over time.[12] The assessment should therefore consider the expected duration of storage or access, the attack surface, the value of successful identification, known attack methods, previous incidents, human error and remaining technical weaknesses. Treating security measures as a categorical exclusion could result in data being classified as anonymous while realistic routes to identification remain and GDPR safeguards no longer apply.

> The EDPB should clarify that "sufficient evidence of a concrete risk" does not require proof that a named actor is planning a specific unlawful identification attempt. It should also provide practical criteria for determining adequate safety margins in light of changing technology, additional information and access conditions, and make clear that appropriate security controls do not automatically exclude unauthorised actors from the assessment.

3. Accountability and Reassessment

Paragraph 35 rightly recognises that anonymous data may later become personal because re-identification technologies and techniques have advanced or additional information has become

---

the European Union, *OC v European Commission*, cited in fn 4, para 51; Court of Justice of the European Union, *European Data Protection Supervisor v Single Resolution Board*, cited in fn 6, para 82; EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 32–33 and Example 8.

[11] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 88 and 92–93

[12] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 30 and 89–90 and Example 22.

more widely available, but describes periodic reassessment only as good practice.[13] The Guidelines should distinguish such precautionary review from situations in which an entity can no longer rely on its previous assessment. An entity should reassess anonymity before a planned material change that may affect identifiability and without undue delay where new information calls a central assumption of the original assessment into question.

The Guidelines should provide a non-exhaustive list of typical triggers. These should include new recipients, publication or other new forms of disclosure, newly available additional information or linkage possibilities, material technological developments, changes to the purpose or processing context that affect the relevant perspectives, means or access conditions, use beyond the period assumed in the original assessment, security incidents[14] and the removal or weakening of safeguards. Without timely reassessment, data may continue to be treated as anonymous even though individuals can again be identified and the safeguards of the GDPR apply.

The Guidelines should also clarify the timing and consequences where a reassessment shows that data are no longer anonymous. Data become personal for the relevant entity when the factual conditions of identifiability are met, not only when the entity formally reclassifies them.[15] If the original assessment was incorrect, the data were personal from the outset. If the assessment was initially sound but circumstances later changed, the GDPR applies to ongoing and subsequent processing from the point at which the data became personal for the relevant entity.

Effective reassessment also depends on reliable documentation. **Paragraphs 40 and 41** rightly call for transparent and non-misleading communication about anonymisation and adequate documentation of the anonymisation process. Claims that data are anonymous, de-identified or de-personalised should be supported by documentation that demonstrates both compliance with the GDPR during the anonymisation process and the effectiveness of its outcome.[16]

The Guidelines should, however, clarify the minimum content of the documentation required under paragraph 41. It should record the purpose and context of the anonymisation, the relevant perspectives and recipients, the additional information and identification methods considered, the tests performed and their results, the date and material assumptions of the assessment, the safeguards and safety margins relied upon and the expected period of use or availability. The documentation retained by the anonymising controller should be made available on request to the competent supervisory authority together with the information needed to verify the underlying methods and assumptions.[17] Where the assessment depends on continuing technical, organisational, legal or contractual conditions at an independent recipient, the anonymising controller should also document why those conditions are reliable, verifiable and enforceable and what arrangements are in place for relevant changes to be communicated or otherwise identified.[18]

---

[13] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 35.

[14] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 42.

[15] Regulation (EU) 2016/679, Articles 2(1) and 4(1) and Recital 26; EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 35 and 42.

[16] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 40–41.

[17] Regulation (EU) 2016/679, Articles 31 and 58(1)(a), (e) and (f); EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, para 41.

[18] EDPB, Guidelines 02/2026 on Anonymisation, cited in fn 1, paras 34 and 41.

> The EDPB should clarify when an entity can no longer rely on a previous anonymity assessment, identify typical reassessment triggers and explain when and with what consequences previously anonymous data become personal data for the relevant entity. It should also provide minimum requirements for documenting claims of anonymity and enabling their effective verification by competent supervisory authorities, including where those claims depend on continuing conditions at independent recipients.

Imprint

Published by:
Verbraucherzentrale Bundesverband e.V.
(Federation of German Consumer Organisations)
Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0
digitales@vzbv.de
vzbv.de

The Federation of German Consumer Organisations is registered in the German Lobby Register and the European Transparency Register. You can access the relevant entries here und here.