CONSULTATIVE REMARKS

ON THE DRAFT EDPB GUIDELINES 02/2026 ON ANONYMISATION

DR. ZSOLT G. BALOGH

LUDOVIKA UNIVERSITY OF BUDAPEST

INSTITUTE OF THE INFORMATION SOCIETY

UNESCO CHAIR

29 OCTOBER 2026

CONTEXTUAL ANONYMITY AND CONTINUING ACCOUNTABILITY

1 INTRODUCTION

The European Data Protection Board's Guidelines 02/2026 offer a welcome reassessment of anonymisation following the Article 29 Working Party's Opinion 05/2014. Their principal achievement is to connect legal identifiability with a technical assessment that accommodates different recipients, capabilities and processing environments. Nevertheless, the flexibility of this framework creates corresponding demands for evidence, transparency and supervision. This Guidelines supports the contextual approach, while recommending clearer safeguards against selective assessments, stronger treatment of evolving identification capabilities, and explicit coordination with the Union's wider digital legislation. Anonymous data should facilitate socially valuable reuse; its classification should not become a discretionary means derogating fundamental rights.

2 ASSESSING ANONYMITY UNDER THE GDPR

2.1 LEGAL PERSPECTIVES AND ORGANISATIONAL RESPONSIBILITIES

The legal analysis correctly treats anonymity as dependent on whether information relates to an identified or identifiable natural person. Following *Breyer v Bundesrepublik Deutschland*[1] and *EDPS v SRB*[2], identifiability cannot simply be equated with a theoretical possibility of identification. Conversely, removing names does not establish anonymity. The Guidelines appropriately recognise that information may be anonymous for an independent recipient while remains personal for its originating controller. This distinction must remain obligation-specific: the recipient's inability to identify individuals does not extinguish the originating controller's

[1] *Breyer v Bundesrepublik Deutschland*, paras. 43–49;

[2] *European Data Protection Supervisor v Single Resolution Board*, paras. 78–85 and 102–111

transparency obligations. Moreover, *EDPS v SRB* concerned Regulation 2018/1725[3]; its relevance to the GDPR rests on the corresponding definitions and protective rationale, rather than identical statutory provisions[4].

For controllers and processors, the central practical difficulty is establishing the relevant assessment perimeter. Asking for whom data is intended to be anonymous is a useful starting point, but subjective intention cannot determine whose capabilities count. The Guidelines already recognise *unauthorised and malicious actors*[5] and chains of access. They should additionally require a documented explanation of excluded perspectives, foreseeable onward disclosure, auxiliary datasets and organisational relationships. Paragraph 15's treatment of processors is particularly valuable: outsourcing does not sever the controller's identification capabilities from processing performed on its behalf. The final text should distinguish this interpretation from the factual assessment of genuinely independent recipients, with examples covering cloud analytics, research collaborations and shared corporate infrastructure.

2.2 TECHNICAL CRITERIA AND THE LIMITS OF INFERENCE

The technical framework improves on a rigid reading of the 2014 Opinion. No Record Isolation, No Linkage and No Inference provide sufficient assurance when satisfied, while failure prompts further analysis rather than automatically establishing personal-data status. This refinement avoids conflating isolation of a record with identification of a person. Nevertheless, the further-analysis pathway requires reproducible evidential standards. Controllers should record tested attacks, relevant auxiliary information, success measures, assumptions and unresolved limitations. Alexin's empirical analysis[6] and Kondor and colleagues' mobility research[7] demonstrate why generalisation and identifier removal cannot be evaluated independently of population characteristics and cross-dataset matching. Neither an average success rate nor a single privacy metric adequately describes risks to unusually identifiable individuals.

---

[3] Regulation (EU) 2018/1725, Arts. 3(1), 3(6), 15(1)(d)

[4] GDPR, Art. 4(1), Recital 26

[5] EDPB (2026), para. 30

[6] Alexin (2014)

[7] Kondor et al. (2018) p. 2

Unstructured data require fuller attention. Free text, images and recordings reveal identities through contextual combinations that tabular techniques may overlook. Weitzenboeck and colleagues show why legal and technical approaches[8] to these materials must be developed together. The Guidelines should therefore include worked examples involving clinical narratives, legal documents and multimodal datasets. They should also explain that *differential privacy* supplies a formal guarantee[9] under specified parameters and assumptions, rather than automatically establishing GDPR anonymity. Repeated releases, cumulative queries and overlapping datasets may alter the assessment. Vokinger and colleagues' classification usefully exposes variation in technical protection[10], although intermediate technical categories must not be mistaken for additional legal categories between personal and anonymous data.

The treatment of inference presents a deeper conceptual difficulty. Paragraph 71 and Examples 13–14 distinguish specific, meaningful inferences from general population predictions. This distinction appropriately prevents every useful statistic from becoming personal data. However, removing one person's records without changing a prediction does not, by itself, resolve whether the remaining information relates to that person through content, purpose or effect. Information concerning relatives or small groups may remain revealing, while redundant records may obscure individual contribution. The final Guidelines should clarify that this comparison is an analytical aid, not an exhaustive legal test. They should also emphasise that applying anonymous population information to an identifiable person can generate new personal data and associated obligations.[11]

3 DATA SUBJECT RIGHTS AND LAWFUL ANONYMISATION

For data subjects, anonymisation offers protection while potentially ending the applicability of GDPR rights to the resulting information. Paragraph 40's transparency requirement is therefore essential. Notices should explain the anonymisation purpose, the categories of intended recipients, whether source data remain identifiable, and whether anonymity depends on restricted access. This does not require a general right to veto anonymisation, nor disclosure of

[8] Weitzenboeck et al. (2022) p. 203

[9] Holzel, J. (2019) p. 194

[10] Vokinger et al. (2020) p. 229

[11] *Nowak v Data Protection Commissioner.* paras. 35-36. The criticism concerns the sufficiency of the proposed inference comparison; it does not claim that all population statistics are personal data.

security-sensitive details. It does require understandable information about the transition being claimed. Where the original personal data remain, applicable access, objection and erasure rights continue in relation to those data. The Guidelines should expressly distinguish successful anonymisation of an output from fulfilment of a separate duty to erase its source.[12]

Accountability must also cover the anonymisation operation itself. Subsequent anonymity cannot retrospectively legitimise unlawful collection or incompatible processing. The presumption in paragraph 38 that the preceding legal basis and Article 9 condition continue where anonymisation forms part of the same activity and pursues the same purposes should be illustrated carefully. A new commercial reuse objective may require a different assessment. Controllers should document purpose compatibility, necessity and any applicable special-category condition before transformation. Data protection by design and impact assessment can support this analysis where their statutory requirements apply; they should not be presented as universally mandatory procedures for every anonymisation exercise.[13]

4 ANONYMISATION WITHIN THE EU DIGITAL FRAMEWORK

4.1 ARTIFICIAL INTELLIGENCE

The AI Act by its Article 10 data-governance requirements for relevant high-risk systems address quality and bias, while Article 4a, introduced by Digital Omnibus on AI Regulation, permits exceptional processing of special-category data for bias detection[14] and correction under strict conditions, including inability to achieve the objective effectively using other data. Its reach extends beyond providers of high-risk systems, making coordinated guidance particularly important. Anonymisation that disproportionately removes minority observations may undermine representativeness. Conversely, a synthetic dataset or trained model may retain exploitable information.

The Guidelines should coordinate their inference analysis with EDPB Opinion 28/2024 and provide examples of membership inference and extraction testing. AI Act compliance does not

[12] GDPR, Arts. 5(1)(a), 12–15, 17 and 21, subject to their respective conditions and exceptions.

[13] GDPR, Arts. 5(1)(b), 5(2), 6, 9, 25 and 35. Legislative proposals discussed in Mateiciuc (2026) must be distinguished from applicable law; the argument here does not assume enactment of the Digital Omnibus proposal.

[14] Mateiciuc, E. (2026). p. 50

establish anonymity, and claimed anonymity does not remove AI Act obligations that apply independently of personal-data status.[15]

Must note and consider that the Article 4a replaces the former Article 10(5) and extends the conditional permission to additional providers and deployers.[16]

The competitive implications of anonymisation are particularly apparent in generative AI markets, where control over valuable datasets can reinforce the position of dominant firms. Casey (2026) argues that carefully tailored antitrust duties to deal could address emerging bottlenecks by requiring access to resources needed for competing AI services, including, in appropriate circumstances, data accumulated within an incumbent's ecosystem. Although he identifies anonymisation as a possible safeguard for such sharing, its effectiveness requires closer examination: the detail and contextual richness that make information useful for developing specialised AI applications may also create opportunities for identification. From this perspective, anonymisation is a practical condition affecting the feasibility and design of competition-enhancing data access. The EDPB's Guidelines can therefore help clarify when useful sharing can proceed on the basis of anonymous information and when access must instead remain subject to data protection requirements and appropriate safeguards.[17]

4.2 CYBERSECURITY

Cybersecurity is equally integral to contextual anonymity. Paragraphs 42 and 88–89 of the draft Guidelines recognise that confidentiality failures can change identifiability. However, the proposition that appropriate controls exclude unauthorised access from reasonably likely means needs to be read alongside the earlier treatment of malicious actors. Assessment should consider concrete vulnerabilities, insider access and foreseeable compromise rather than assume perfect security.

The European cybersecurity framework provide relevant risk-management and incident-reporting duties[18] for entities within scope. The Cyber Resilience Act adds product-security requirements[19] according to its phased application. Neither framework certifies anonymity. A

[15] AI Act, Arts. 2(7), 4a, 10(3)–(4), 15 and 113, as amended by Digital Omnibus on AI

[16] AI Act Explorer. https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4a

[17] Casey, A. (2026) pp. 149-151 and footnote 277

[18] NIS2, Articles 21 and 23

[19] CRA, Art. 71, Annex I.

security incident should trigger reassessment, while any GDPR breach-notification duty requires a separate analysis of the affected processing and statutory conditions. Note, that the CRA generally applies from 11 December 2027, with specified provisions applying earlier; no claim of full present application is made.

4.3 PLATFORMS AND DATA ACCESS

Platform regulation makes the balance between protection and useful access particularly visible. DMA Article 6(11) requires anonymisation of personal query, click and view data when search data are shared with qualifying competitors. The Guidelines should offer examples that preserve meaningful access while preventing reconstruction through rare queries and successive releases. Under DSA Article 40, researcher access requires appropriate protection of personal data; it is not universally conditional on producing anonymous datasets. Secure access may therefore support lawful research where public release would be inappropriate.

Anonymisation occupies a pivotal position in the data economy because it can enable the reuse of information whose value extends beyond the purposes for which it was originally collected. As Hacohen (2026) argues, the non-rivalrous character of data creates opportunities for research, innovation and competition that remain underexploited when access is concentrated in the hands of a limited number of organisations. Personal data are particularly consequential in this respect: information generated through individuals' activities can improve services and support commercially valuable predictions, while exclusive access to those data can reinforce market power. Yet broader access also creates risks to the individuals concerned, making openness a question of appropriate conditions rather than unrestricted disclosure. Against this background, the EDPB's anonymisation Guidelines have significance beyond the classification of information under the GDPR: a credible and practicable framework for assessing anonymity can facilitate socially beneficial data circulation while preserving effective protection against identification and misuse.[20]

The Data Act and Data Governance Act likewise require differentiated treatment. Data Act access rights encompass personal and non-personal data within their respective scope, but do not displace GDPR requirements or independently supply a general legal basis for personal-data processing. Under DGA Article 5, protected public-sector data may be made reusable

[20] Hacohen, U. Y. (2026). especially pp. 263–267, 279–282 and 300.

through anonymisation or suitable controlled arrangements, subject to the applicable conditions. These are legally distinct routes. The Guidelines should distinguish

- unrestricted publication,
- access by specified independent recipients and
- processing within secure environments.

Anonymity established for a restricted recipient cannot simply be carried over to a public release, whose audience and available auxiliary information are materially different.[21]

5 SUPERVISION AND CONCLUDING RECOMMENDATIONS

National supervisory authorities need a common method for reviewing these assessments. The EDPB should develop a proportionate documentation template and worked sectoral examples, while avoiding universal numerical thresholds unsupported by context. Reassessment should be linked to material changes such as new auxiliary datasets, onward disclosure, security incidents or improved attacks. The statement in footnote 3 that earlier WP29-compliant assessments need not be repeated should expressly preserve the need to respond when their factual assumptions cease to hold. Otherwise, historical assessments could acquire unwarranted permanence. Authorities should coordinate with cybersecurity, AI and platform regulators while preserving their respective statutory competences.[22]

Finally, the glossary and Annex 1 should make the limits of every conclusion visible. An assessment should specify the data, applicable perspectives, access conditions, assumptions and review triggers. The flowchart should direct users back to the legal analysis where uncertainty remains, rather than suggest that technical testing alone determines GDPR scope. The proposed refinements would preserve the Guidelines' valuable flexibility while making their conclusions contestable and auditable. The appropriate policy objective is dependable, evidence-based anonymity within a coherent system of continuing accountability, enabling useful data circulation without concealing the conditions on which protection depends.

[21] Data Act, Art. 1(5), Arts. 4–6; Data Governance Act, Arts. 1(3), 5(3)–(5)

[22] GDPR, Arts. 57–58 and 70(1)(e)

REFERENCES

- Alexin, Z. (2014). Does fair anonymization exist? *International Review of Law, Computers & Technology, 28*(1), 21–44. https://doi.org/10.1080/13600869.2013.869909
- Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on anonymisation techniques* (WP216).
- Casey, A. (2026). Generative AI's duty to deal dilemma. *Albany Law Journal of Science & Technology, 36*(2), 83–155.
- European Data Protection Board. (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*.
- Hacohen, U. Y. (2026). Fostering open data. *Berkeley Technology Law Journal, 41*(1), 261–306. https://doi.org/10.15779/Z38M61BS11
- Holzel, J. (2019). Differential privacy and the GDPR. European Data Protection Law Review (EDPL), 5(2), 184-196.
- Information Commissioner's Office. (2012). *Anonymisation: Managing data protection risk code of practice*.
- Kondor, D., Hashemian, B., de Montjoye, Y.-A., & Ratti, C. (2018). *Towards matching user mobility traces in large-scale datasets* (arXiv:1709.05772, Version 4). https://arxiv.org/abs/1709.05772
- Mateiciuc, E. (2026). Redefining 'personal data' in the Digital Omnibus proposal: Implications for AI processing by EU institutions under Regulation (EU) 2018/1725. *Lex et Scientia International Journal, 33*(1), 44–53.
- Vokinger, K. N., Stekhoven, D. J., & Krauthammer, M. (2020). Lost in anonymization – A data anonymization reference classification merging legal and technical considerations. *The Journal of Law, Medicine & Ethics, 48*(1), 228–231.
- Weitzenboeck, E. M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: Is anonymization possible? *International Data Privacy Law, 12*(3), 184–206.

CASES

- *Breyer v Bundesrepublik Deutschland*, Case C-582/14, ECLI:EU:C:2016:779 (Court of Justice of the European Union, October 19, 2016).
- *European Data Protection Supervisor v Single Resolution Board*, Case C-413/23 P, ECLI:EU:C:2025:645 (Court of Justice of the European Union, September 4, 2025).
- *Nowak v Data Protection Commissioner*, Case C-434/16, ECLI:EU:C:2017:994 (Court of Justice of the European Union, December 20, 2017).

LEGISLATION

- GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 (protection of personal data by Union institutions, bodies, offices and agencies)
- Data Governance Act. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022
- DMA. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 (Digital Markets Act)
- DSA. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act)
- NIS2 Directive. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive)
- Data Act. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (Data Act)
- AI Act. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act)
- CRA. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (Cyber Resilience Act)
- Digital Omnibus on AI. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)