Comments of

The Center for AI and Digital Policy

to the

European Data Protection Board

in response to

Guidelines 02/2026 on Anonymisation

The Center for AI and Digital Policy (CAIDP) welcomes the opportunity to respond to the European Data Protection Board's (EDPB) request for comments on the Guidelines 02/2026 on Anonymisation (Guidelines).[1] CAIDP commends the work being done to update and refine the Article 29 Working Party Opinion 05/2014 on anonymisation techniques.[2]

Given the critical role of anonymisation in protecting privacy in the context of AI, where powerful inference capabilities can potentially reveal sensitive information even from seemingly non-identifiable data, CAIDP offers the following measures to further strengthen the Guidelines.

CAIDP Recommendations

1. Adopt genuine Privacy-Enhancing Technologies (PETs)
2. Require robust anonymisation assessments for AI training and deployment
3. Strengthen safeguards against re-identification and inference
4. Ensure transparency and accountability in claims of anonymisation
5. Mandate ongoing testing and documentation of anonymisation practices

About CAIDP

CAIDP is the largest independent nonprofit AI policy research and education organization, with a global footprint across 130 countries and a network of more than 2,000 experts.[3] CAIDP has previously submitted a statement to the EDPB on the use of facial recognition in law enforcement, recommending a ban on mass surveillance.[4] CAIDP has also advised the Dutch Data Protection Authority on Generative AI, calling for verifiable

[1] European Data Protection Board, *Guidelines 02/2026 on Anonymisation* (07 Jul. 2026), https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en#no-back.

[2] European Commission, Article 29 Working Party Opinion 05/2014 on anonymisation techniques (10 Apr. 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[3] CAIDP, https://www.caidp.org/

[4] CAIDP, *Statement to European Data Protection Board on the Use of Facial Recognition Technology in the Area of Law Enforcement* (18 Jul. 2022), https://www.caidp.org/app/download/8405683363/CAIDP-Statement-EDPB-FRT-01082022.pdf

anonymisation,[5] and on automated decision-making, urging mandatory fundamental rights impact assessments.[6] More broadly, CAIDP has consistently engaged with the European Union, European Commission, and other EU bodies on the drafting and implementation of the EU AI Act.[7]

CAIDP publishes the ***CAIDP AI Index***, which is the most comprehensive global assessment of national AI policies and practices against human rights and democratic values.[8] The ***CAIDP AI Index*** highlights the work of the EDPB, including its central role in clarifying how EU data protection law applies to AI.[9]

1. Adopt genuine Privacy-Enhancing Technologies (PETs)

CAIDP urges the EDPB to adopt Privacy-Enhancing Technologies precisely as it was originally conceived—techniques to "minimize or eliminate the collection of personal data."[10] PETs include utilizing low-data artificial intelligence, deleting unnecessary data, and creating techniques for robust anonymity.[11] The aim of PETs is not to enable further transfers of personal data, but to limit the collection of personal data in the first instance.

The EDPB's recent statement on smart glasses encourages data controllers to mitigate risks by incorporating "other privacy-friendly settings and protective measures by default, in line with the principle of data protection by design and by default".[12] Extending this approach to the anonymisation of data more generally is therefore an effective next step to uphold this core principle.

---

[5] CAIDP, *CAIDP Advises Dutch Privacy Agency on Generative AI* (29 Jun. 2025), https://lnkd.in/p/gSn8VbMh

[6] CAIDP, *Dutch Data Protection Authority: Automated Decisions Require Real Transparency, Meaningful Contestability* (25 May 2026), https://lnkd.in/p/gAKdwxVP;

[7] CAIDP, *EU AI Act, https://www.caidp.org/resources/eu-ai-act/*

[8] CAIDP, *CAIDP AI Index 2026*, https://www.caidp.org/reports/caidp-index-2026/.

[9] Ibid, p.40.

[10] *Madrid Privacy Declaration of 2009,* https://www.edps.europa.eu/sites/default/files/publication/09-11-03_madrid_privacy_declaration_en.pdf; Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision in Technology and Privacy: the New Landscape* 143–67 (eds., Philip E. Agre & Marc Rotenberg 1997)

[11] CAIDP, *Comments to the US OSTP on Advancing Privacy Enhancing Technologies* (9 Jun. 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Center-for-AI-and-Digital-Policy-PET-RFI-Response-2022.pdf

[12] European Data Protection Board, *Statement 1/2026 of the EDPB on Smart Glasses* (13 Oct. 2026), https://www.edpb.europa.eu/documents/statement/statement-of-the-edpb-on-smart-glasses_en, para. 33.

2. Require robust anonymisation assessments for AI training and deployment

CAIDP urges the EDPB to require assessors, controllers, and entities to conduct robust, ex-ante anonymisation assessments before anonymised datasets are relied upon for AI training or deployment, followed by reassessment throughout the lifecycle where relevant circumstances change. This includes recommending the simplified approach to identifying personal data to be the standard approach during AI training and deployment. This approach appropriately shifts the risk toward false positives—where data may be treated as personal even when they are anonymous—rather than false negatives, where data are treated as anonymous despite remaining identifiable. [13] Furthermore, this approach is vital given the large-scale use of data within AI training, the scale and variety of data processed by AI systems during deployment, and the potential harms which can arise as a result.[14] These characteristics make reliance on a contextual approach particularly risky in the AI context and support a precautionary approach where there is uncertainty as to whether individuals remain identifiable.

Anonymisation should not be treated as a substitute for compliance with the GDPR requirements that apply to the collection and processing of personal data before anonymisation. Controllers must establish a lawful basis, comply with purpose limitation and data minimisation, and conduct a DPIA where required. Subsequent anonymisation does not retroactively render unlawful collection or processing lawful. The burden of demonstrating that data meet the standard for anonymisation should rest with the controller relying on that claim, not with data subjects to demonstrate that they remain identifiable.

3. Strengthen safeguards against re-identification and inference

CAIDP urges the EDPB to take into account AI's ability to potentially infer sensitive personal data from seemingly anonymous data, and require controllers, entities, and assessors to implement rigorous safeguards against re-identification and inference.[15] Such assessors, controllers, and entities should demonstrate that they have assessed the effectiveness of the

[13] European Data Protection Board, *Guidelines 02/2026 on Anonymisation* (07 Jul. 2026), https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en#no-back, paras. 45 and 47.

[14] European Union Agency for Fundamental Rights, *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights* (11 Jun. 2019), https://fra.europa.eu/en/publication/2019/data-quality-and-artificial-intelligence-mitigating-bias-and-error-protect

[15] CAIDP, *Statement on the ICO on Purpose limitation in the generative AI lifecycle* (12 Apr. 2024), https://www.caidp.org/app/download/8568853163/CAIDP-Statement-UK-ICO-GenAi-06102024.pdf

(re-)identification techniques identified in paragraph 85 of the Guidelines.[16] Where AI systems or agents are used to process anonymised data, testing for re-identification and meaningful inferences should be required. This is necessary to avoid potential error or exploitation by such agents, and to ensure that any flaws in the initial anonymisation are not amplified by such further AI usage. To prevent such situations, the EDPB should establish minimum documentation requirements for anonymisation tests and clearly state that tests must be repeated in cases where changes in AI capabilities or external information could significantly affect the previous assessment. This should include methods, results, and limitations that could lead to identification or inference of identity that might otherwise go unnoticed.

4. Ensure transparency and accountability in claims of anonymisation

CAIDP urges the EDPB to specify minimum disclosure requirements for controllers and entities claiming that data used in AI systems are anonymous. Such disclosures should identify from whose perspective anonymity is assessed, the purposes for which the data will be used, and any restrictions on access necessary to support the claim.[17] Building on the Guidelines' transparency and documentation requirements, controllers should provide an accessible explanation of the assessment methods, key assumptions, and limitations, and make supporting evidence available to supervisory authorities without publishing details that could enable re-identification.[18] These measures would help prevent context-specific findings of anonymity from becoming blanket claims that obscure the continued application of data protection safeguards.

5. Mandate ongoing testing and documentation of anonymisation practices

CAIDP urges the EDPB to strengthen paragraph 41 of the Guidelines by specifying that controllers should maintain up-to-date evidence of anonymisation effectiveness through ongoing testing and documented review.[19] Controllers should review anonymisation more frequently where identification risks are higher, and whenever changes in available data, access, or identification techniques could undermine earlier assessments. Controllers should also record the methods, results, limitations, and corrective actions from each review, rather than retain only the documentation produced when anonymisation was completed. Where

[16] European Data Protection Board, *Guidelines 02/2026 on Anonymisation* (07 Jul. 2026), https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en#no-back, para. 85.
[17] European Data Protection Board, *Guidelines 02/2026 on Anonymisation*, Version 1.0 (07 Jul. 2026), paras. 11–14 and 29, https://www.edpb.europa.eu/system/files/2026-09/edpb_guidelines_202602_anonymisation_v1_en_0.pdf.
[18] Ibid., paras. 40–41.
[19] Ibid., para. 41.

testing reveals that individuals are identifiable, controllers should cease relying on the anonymisation claim and ensure that subsequent processing complies with the General Data Protection Regulation (GDPR).[20]

For large-scale AI training or other processing presenting heightened risks of re-identification, anonymisation assessments should also be subject to appropriate independent scrutiny, including external audit where appropriate.

Closing Remarks

We thank you for considering our contributions. We welcome the opportunity to engage and discuss these recommendations in further detail.

Sincerely,

 **Merve Hickok** **CAIDP President and Policy Director**	 **Marc Rotenberg** **CAIDP Founder and Executive Director**	 **Ren Bin Lee Dixon** **CAIDP Policy Group Associate**
 **Emma Jones** **CAIDP Policy Group Member**	 **Saima Tariq Khan** **CAIDP Policy Group Member**	U.A **Uche Anyamele** **CAIDP Policy Group Member**
P.M. **Pritika Magima** **CAIDP Policy Lead**	 **Mert Özyiğit** **CAIDP Policy Lead**	

[20] European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (4 May. 2016), https://eurlex.europa.eu/eli/reg/2016/679/oj/eng; CAIDP, *Comments to NTIA on AI and Accountability* (12 Jun. 2023), summary recommendation 4, https://www.caidp.org/public-voice/ntia-ai-accountability-us-2023/