AMERICAN BAR ASSOCIATION
Antitrust Law Section

321 North Clark Street
Chicago, IL 60654-7598
(312) 988-5550
antitrust@americanbar.org
www.ambar.org/antitrust

Attachment

October 30, 2026

Via: https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en#no-back

SUBJECT: Comments on the European Data Protection Board's Draft Guidelines Relating to Data Anonymization

Dear Sir/Madam:

On behalf of the American Bar Association Antitrust Law and International Law Sections, I respectfully submit this comment on the Joint Section Comment on the European Data Protection Board's Draft Guidelines Relating to Data Anonymization.

The views expressed herein are being presented on behalf of the Antitrust Law and International Law Sections. They have not been reviewed or approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the Association.

If you have any questions after reviewing this report, we would be happy to provide further comments.

Sincerely,



Melanie L. Aitken
Chair, Antitrust Law Section



Edward Mullins
Chair, International Law Section

COMMENTS OF THE AMERICAN BAR ASSOCIATION ANTITRUST LAW SECTION AND INTERNATIONAL LAW SECTION ON THE CONSULTATION OF THE EUROPEAN DATA PROTECTION BOARD'S DRAFT GUIDELINES 02/2026 ON ANONYMISATION

October 30, 2026

The views expressed herein are being presented on behalf of the Antitrust Law Section and the International Law Section. They have not been reviewed or approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the Association.

The Antitrust Law Section and International Law Section of the American Bar Association (the Sections) welcome the opportunity to comment on the European Data Protection Board's (EDPB) Guidelines 02/2026 on Anonymisation (the Draft Guidelines).[1] The Sections commend the EDPB for undertaking this consultation and are grateful for the opportunity to provide these comments.

The Antitrust Law Section is the world's largest professional organization for antitrust and competition law, trade regulation, consumer protection, and data privacy as well as related aspects of economics. Section members, numbering over 12,000, come from all over the world and include attorneys and non-lawyers from private law firms, in-house counsel, non-profit organizations, consulting firms, federal and state government agencies, as well as judges, professors, and law students. The Antitrust Law Section provides a broad variety of programs and publications on all facets of antitrust/competition, consumer protection, and privacy. Numerous members of the Antitrust Law Section have extensive experience and expertise regarding similar laws of non-U.S. jurisdictions. For more than thirty years, the Antitrust Law Section has provided input to enforcement agencies around the world conducting consultations on topics within the Antitrust Law Section's scope of expertise.[2]

The International Law Section focuses on international legal issues, the promotion of the rule of law, and the provision of legal education, policy, publishing and practical assistance related to cross-border activity. Its members total over 11,000, including private practitioners, in-house counsel, attorneys in governmental and inter-government entities, and legal academics, and represent over 100 countries. The International Law Section's more than fifty substantive committees cover competition law, trade law, and data privacy and data security law worldwide

[1] Eur. Data Prot. Bd., Guidelines 02/2026 on Anonymisation (July 7, 2026), *available at* https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en#no-back [hereinafter Draft Guidelines].

[2] *See Antitrust Comments, Reports & Amicus Briefs*, AM. BAR ASS'N, ANTITRUST L. SECTION, http://ambar.org/atcomments.

as well as areas of law, which often intersect with these areas, such as regulatory compliance, mergers and acquisitions, and joint ventures. Throughout its century of existence, the International Law Section has provided input on debates relating to international legal policy[3] and has provided input on antitrust and competition law and policy for decades to authorities around the world.[4]

These comments reflect the expertise and experience of the Sections' members with data protection laws and enforcement practices around the world. The Sections are available to provide additional comments, or otherwise to assist the EDPB as it may deem appropriate.

SPECIFIC COMMENTS AND RECOMMENDATIONS

I. Anonymization Is a Factual Question That Must Be Based on an Assessment of All Relevant Factors

The Sections applaud the EDPB's efforts to provide a practical framework that reflects the recent decisions of the Court of Justice of the European Union (CJEU) on the meaning of personal data and the concept of anonymization.[5] The fundamental question in assessing anonymization is whether the "information relat[es] to an identified or identifiable natural person," taking "account . . . of all the means reasonably likely to be used."[6] This is primarily a factual question, and one that should be assessed empirically. The legal framework helps guide that process but should not lead it. The Draft Guidelines largely follow this approach. In particular:

- *Use of examples:* The Sections welcome the use of examples in the Draft Guidelines, both to illustrate how the principles in the Draft Guidelines operate but also as a reminder that this is ultimately a practical assessment.

- *The three criteria (Section 3.4):* The Sections welcome the EDPB's factual application of the three criteria. For example, the "No Record Isolation" criterion does not, in itself, resolve the question of whether the data is anonymized. Example 24 contains a clear demonstration of the fact a record can be unique but still not identify an individual. Similarly, the Sections welcome the approach to "No Linkage" which, as set out in Example 25, is also not determinative of whether an individual is identified.

In contrast, the Sections think that some sections of the Draft Guidelines could be better grounded in the actual risk of reidentification. One example is the potential exclusion, or downgrading, of relevant factors when assessing "means reasonably likely to be used"

---

[3] *See About Section Policy*, AM. BAR ASS'N, INT'L L. SECTION, https://www.americanbar.org/groups/international_law/policy/about/.

[4] *See Blanket Authorities Initiatives*, AM. BAR ASS'N, INT'L L. SECTION, https://www.americanbar.org/groups/international_law/resources/policy/blanket-authorities/.

[5] Draft Guidelines, *supra* note 1, ¶¶ 18-22.

[6] 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 (General Data Protection Regulation) [GDPR], art. 4(1) & recital 26, 2016 O.J. (L 119) 1.

(MRLTBU).[7] As recognized in the Draft Guidelines,[8] "account *should* be taken of *all* objective factors."[9] The Sections suggest the EDPB reconsider and consolidate its summary of the key factors in assessing MRLTBU[10] to reflect this broad view, including:

- *Lawfulness restrictions in the GDPR:* The Draft Guidelines identify that means may not need to be considered if the likelihood of their use is insignificant because they are prohibited by law.[11] The Sections note this factor is expressly referred to at paragraph 29, which identifies the GDPR as an example. Processing conducted with the aim of reidentification would, if successful, involve personal data and be subject to the GDPR. If that reidentification exercise is expressly prohibited or otherwise unauthorized, it is very difficult to see how that processing would be fair and lawful[12] or satisfy a legal basis.[13] Therefore, where a relevant actor is subject to the GDPR or an equivalent regime, the assessment of MRLTBU should reflect the fact the GDPR itself creates a lawfulness barrier to reidentification.

- *Motivation*: The Draft Guidelines currently suggest that "lack of motivation" should be treated with caution,[14] as it can be difficult to assess, demonstrate objectively, and may change over time. The Sections agree that a subjective assessment of an actor's state of mind may be difficult and may change. However, the Sections submit that when considering MRLTBU, an assessment of motivation is not only possible but necessary (see above). That should address all relevant factors, such as the objectively assessed purposes and aims of the actor, value of the data in achieving those purposes and aims, and the impact of any contractual, legal or reputational constraints.

- *"Value" of the data:* The summary at paragraph 29 could also reflect and expand on the analysis of the value of the data at the end of paragraph 31. Any assessment of "all objective factors" should include an assessment of the "value" of the data to the relevant actor. Assessing costs and time without factoring in the resulting value fails to take into account all objective factors and may give false comfort about potential anonymization. For example, significant costs may not be a deterrent to reidentification if it could deliver significant value and vice versa. Paragraph 31 also takes too narrow a view of the assessment of value. It is insufficient to consider value as just a potential "offset" against the cost and time of reidentification. For example, a very significant reputational enhancement, *e.g.*, in demonstrating the success of a new technology say, may do little or nothing to offset costs, but may still justify material activity to re-

---

7 *Id.*, recital 26.

8 Draft Guidelines, *supra* note 1, ¶ 29.

9 GDPR, recital 26 (emphasis added).

10 Draft Guidelines, *supra* note 1, ¶ 29.

11 *Id.* ¶ 32.

12 GDPR, art. 5(1)(a).

13 *Id.*, art. 6.

14 Draft Guidelines, *supra* note 1, ¶ 31.

identify a dataset. This is also an area in which further examples would be useful. For example, under Article 40(12) of the Digital Services Act, Very Large Online Platforms (VLOPs) must give researchers access to data that is publicly accessible on their platforms.[15] While the output of any subsequent research will likely be anonymized, any attempts to reverse that re-identification are likely to be very limited given the underlying (and directly identifying) information is accessible and in the public domain.

II. The Guidelines' Treatment of Processors Should Align Fully with EDPS v. SRB

The Sections would also welcome further explanation of the approach taken to processors, as set out in the Draft Guidelines: "if an entity processes information on behalf of a controller . . . that information should also be considered personal data for the processing entity. That entity should, therefore, be considered a processor under the GDPR and be subject to the obligations applicable to processors."[16] This is said to be based on a teleological application of the GDPR but is difficult to reconcile with the CJEU's judgment in *European Data Protection Supervisor v. Single Resolution Board*.[17] That decision related to the Single Resolution Board's (SRB) engagement of Deloitte to review a set of pseudonymized comments. The CJEU's decision was that the pseudonymized data continued to be personal data in SRB's hands because it had the means to reidentify the individuals. However, the data was not necessarily personal data in the hands of Deloitte. It states: "pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data . . . in so far as pseudonymisation may, depending on the circumstances of the case, 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."[18]

The CJEU's treatment of personal data is also notable. As the Court explained, "that concept is not unlimited since that provision requires, inter alia, that the data subject be identified or identifiable."[19] Moreover, "clarifications relating to the assessment of whether or not the data subject is identifiable would be deprived of any practical effect if pseudonymised data were to be regarded as constituting, in all cases and for every person, personal data for [those] purposes."[20] The decision does not directly address a controller-processor relationship, but any teleological analysis should be underpinned by the CJEU's reasoning. The Sections respectfully suggest the approach should therefore vary depending on the specific obligation placed on the processor. For example:

---

15 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), art. 40(12), 2022 O.J. (L 277) 1.

16 Draft Guidelines, *supra* note 1, ¶ 15.

17 Case C-413/23 P, Eur. Data Prot. Supervisor v. Single Resol. Bd., ECLI:EU:C:2025:645 (Sept. 4, 2025).

18 *Id.* ¶ 86.

19 *Id.* ¶ 88.

20 *Id.* ¶ 80.

- *Technical and organizational measures:* There is a justification for the obligations under Article 32 GDPR to apply. Even if there is no confidentiality risk (because the technical measures mean the processor cannot reidentify any individual) there might still be availability or integrity risks, such as where the data is corrupted or maliciously encrypted.

- *Transfers:* In contrast, there is no logical justification for Article 44 GDPR and the related transfer provisions in Chapter V to apply. If the processor cannot re-identify any individual, it is not clear why these provisions should apply. It would also lead to a situation in which the transfer of anonymized/pseudonymized data will be subject to Chapter V if the recipient is a processor, but not if they are a controller. It would be helpful for the EDPB to explain its reasoning and this discontinuity in light of *SRB*.

III. The Board Should Assess Contractual Assurances in the Context of Surrounding Technical and Administrative Controls

The Sections appreciate the EDPB's reluctance to treat contractual assurances against reidentification, on their own, as a sufficient guarantee of anonymization and agrees that such assurances should be "reliable, verifiable and enforceable."[21] Although it is possible that parties will change or even breach their commitments, due diligence processes, contractual accountability mechanisms, and technical controls—in addition to the regulatory standards that anonymization processes must meet—reinforce contract terms. We recommend that the EDPB recognize the role that these mechanisms play. Recent experience with U.S. state privacy regulations, such as the California Consumer Privacy Act (CCPA), the Utah Consumer Protection Act, and the Iowa Consumer Protection Act, are instructive on this point. The EDPB may wish to study the alternative approaches toward anonymization reflected in these laws.

The CCPA employs a more prescriptive regulatory approach. In addition to providing a definition of "deidentified" data that includes a contractual prohibition against attempting reidentification,[22] the CCPA's implementing regulations mandate due diligence and oversight processes in agreements between controllers and third parties. California regulators will consider "[w]hether a business conducts due diligence of the third party" in their assessment of "whether the business has reason to believe that the third party is using personal information in violation of the CCPA" and therefore may be held liable for the third party's violations.[23] Such agreements also must include terms granting the controller the right to "take reasonable and appropriate steps to ensure that the third party uses" personal data in a manner consistent with the purposes permitted in the agreement and to "stop and remediate unauthorized use of personal information."[24] Organizations are translating these regulatory requirements into practice through pre-contractual technical assessments and mechanisms to assess ongoing compliance with data use restrictions.

---

21 Draft Guidelines, *supra* note 1, ¶ 34.

22 *See* Cal. Civ. Code § 1798.140(m).

23 *See* Cal. Code Regs. Tit. 11, § 7053(b).

24 *See id.* §§ 7053(a)(4)-(a)(5).

Other state privacy laws take a different approach. Utah's Consumer Privacy Act,[25] for example, relies more heavily on role-base responsibility, ordinary contractual allocation of risk, and security practices calibrated to the volume and nature of the data at issue. It does not impose a general requirement that controllers conduct data-protection assessments or obtain recurring technical audits of every processor. It also excludes deidentified data from the definition of personal data, does not require deidentification, and protects a controller that lawfully discloses data without actual knowledge that the recipient intends to violate the law.

Iowa's Consumer Data Protection Act[26] similarly omits a general data-protection assessment requirement, limits enforcement to the attorney general, provides a substantial cure period, and recognizes that deidentified data need not be maintained in identifiable form. These approaches do not eliminate contractual safeguards or reasonable security obligations. They instead permit parties to tailor those safeguards to the sensitivity of the information and the risks of the transaction.

The Sections also suggest that the EDPB ensure that its guidance is consistent with EU regulations that assign a central role to contracts in data governance. For instance, the Digital Markets Act (DMA) establishes that certain contract terms—including protections against reidentification—are a necessary element of providing third parties with access to gatekeepers' aggregated datasets.[27] The DMA does not envision contracts as the sole means of providing and governing access, but it does incorporate them into the broader regulatory scheme. We suggest that contracts should play a similar role in deidentification.

IV. The Board Should Engage with Privacy-Enhancing Technologies

As the Draft Guidelines recognize in Section 3.5.2, certain technologies can play a vital role in facilitating organizational compliance whether the data at issue is personal data under Article 4(1) or anonymous data outside the scope of the GDPR. Specifically, privacy-enhancing technologies (PETs)[28] are tools and methods that protect personal data "by design and by default"[29] while enabling organizations to collect, use, analyze, or share data for lawful purposes. PETs include pseudonymization, homomorphic encryption, differential privacy, k-anonymity, federated

---

[25] *See* Utah Code Ann. § 13-11-1 *et seq*.

[26] *See* Iowa Code §§ 715D.1 to 715D.11.

[27] *See* Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), recital 61, 2022 O.J. (L 265) 1.

[28] Privacy-enhancing technologies are understood as "a broad set of tools and methods aimed at providing ways to build products and functionality while protecting the privacy of users' data." *See* Simon Fondrie-Teitler, *Keeping Your Privacy Enhancing Technology (PET) Promises*, FED. TRADE COMM'N (Feb. 1, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/keeping-your-privacy-enhancing-technology-pet-promises.

[29] GDPR, art. 25.

learning, and secure multiparty computation.[30] The Sections recommend that the EDPB consider providing additional guidance on PETs, if not in the Draft Guidelines, then in supplemental policy statements or other forms of guidance.

The increasing prevalence of re-identification techniques makes it particularly important that PETs are accessible to organizations of all sizes. However, several factors may limit the widespread adoption of PETs, such (1) limited awareness among data subjects and data controllers of the technologies and their safeguards; (2) lack of technical expertise; (3) complex pricing, if bundled with other products or services; (4) uncertainty as to how PETs enhance regulatory compliance;[31] and (5) the privacy-utility tradeoff with real compute costs and loss in model performance.[32] Sophisticated organizations may already have the technical expertise and resources to deploy PETs, but these tools may be cost prohibitive for small- and medium-sized enterprises or organizations with limited resources. This asymmetry potentially creates an imbalance where methods of re-identification become increasingly inexpensive and widely available, especially with the rapid evolution of AI, while effective technologies to mitigate the risk of unauthorized re-identification requires substantial resources and specialized expertise.

The EDPB could bridge this gap in awareness and capabilities by providing guidance on appropriate PETs and their applications in different contexts, developing or endorsing standardized methodologies, providing illustrative use cases and cost-benefit awareness tools for both firms and consumers,[33] and encouraging the development of tools accessible to organizations that do not have extensive in-house resources. The Sections further encourage the EDPB to promote greater transparency regarding the capabilities, limitations, and costs of PETs offered by third-party technology providers. Additional transparency may be particularly valuable to small- and medium-sized enterprises that may lack the technical expertise or resources to independently evaluate these technologies. Information about protections that PETs provide would enable these organizations to make more informed cost-benefit assessments and have the potential to assist with better evaluation of whether their technology providers are delivering the promised privacy protections.

* * *

[30] *See* Elizabeth Renieris, *Why Pets (Privacy-Enhancing Technologies) May Not Always Be Our Friends*, THE ADA LOVELACE INST. (Apr. 29, 2021), https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends.

[31] *See* U.K. Info. Comm'r Office, *Tackling Barriers to Privacy-Enhancing Technologies Adoption — A PETs Project Report* (Sept. 2025), https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tackling-barriers-to-privacy-enhancing-technologies-adoption.

[32] *See* U.S. Gov't Accountability Off., GAO-26-109063, *Science & Tech Spotlight: Privacy Enhancing Technologies* (May 19, 2026), https://www.gao.gov/products/gao-26-109063.

[33] *See* U.K. Dep't for Sci., Innovation & Tech. and Information Comm'r Off. *Privacy Enhancing Technologies: Cost-Benefit Awareness Tool*, (Nov. 7, 2024), https://www.gov.uk/government/publications/privacy-enhancing-technologies-cost-benefit-awareness-tool.

The Sections appreciate the opportunity to comment and remain available to respond to any questions about these comments or provide additional assistance to the EDPB in connection with its consultation.