BSA SUBMISSION ON THE EUROPEAN DATA PROTECTION BOARD'S GUIDELINES ON ANONYMISATION

Response to the Public Consultation

October 30, 2026

The Business Software Alliance (www.bsa.org) welcomes the opportunity to provide input on the European Data Protection Board's (EDPB) Draft Guidelines on Anonymisation.

BSA is the global trade association of the enterprise software industry, representing companies[1] that are leaders in artificial intelligence, cybersecurity, cloud computing, quantum, and other breakthrough technologies. We work in more than 20 markets in the US, Europe, and Asia, advocating for policies that build trust in technology so that every industry sector and the public can benefit from innovation. BSA's members provide privacy- and security-protective services to business customers across every sector of the economy.

BSA supports the EDPB's efforts to clarify the notion of anonymous data and provide a practical framework for determining if data has been successfully anonymised. At the same time, we have significant concerns with the Draft Guidelines, including their:

- impractical approach to processors, which disincentivises privacy-protective arrangements
- uncertain standard for assessing "means reasonably likely to be used" to reidentify data
- emphasis on a "simplified" analysis that goes well beyond legal requirements
- treatment of anonymous, de-identified, and de-personalised data as equivalent
- lack of practical guidance about how privacy enhancing technologies may support anonymisation

We detail these concerns below and would welcome the opportunity to discuss them.

---

[1] BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

1. The Draft Guidelines Must Be Revised to Reflect the Role of Processors.

The Draft Guidelines do not recognise the role of processors — and should be significantly revised to promote processors' ability to handle data in privacy-protective ways. Under Paragraph 15, whether information is personal data for a processor depends on whether that information is personal data for the relevant controller. Under this approach, if information is personal data for a controller, it is personal data for the processor.

The Draft Guidelines undermine the privacy-protective nature of GDPR by disincentivising privacy-protective arrangements between controllers and processors, and their approach is not supported by the SRB judgment. Although controllers may often share identifiable data with processors, with processing falling clearly within GDPR, there may be situations where a controller anonymises data before sharing it with a processor, to protect the privacy and security of individuals and to minimise potential harms in the event of unintentional access or breach. Under the Draft Guidelines, there is no incentive to take these privacy-protective steps, since the processor would be required to treat the information as personal data whether the controller has removed identifying information or not. The Draft Guidelines discourage privacy-enhancing contractual arrangements and create incentives to share data in less privacy-protective ways.

Example 3 of the Draft Guidelines illustrates these poor incentives. That example contemplates an arrangement between an e-commerce retailer and a third-party agency hired to review its customer records. The example states that because the customer records are personal data for the retailer, they are personal data to entities processing the records on behalf of the retailer. This scenario is a day-to-day reality for many small online businesses — and the Draft Guidelines provide few incentives for those small businesses to apply privacy protections to customer records. A more privacy-protective approach would encourage the retailer to share a minimised data set with its processors and contractually and technically prohibit those processors from reidentifying that information.

The Final Guidelines should take a different approach — and encourage controllers to apply privacy protections to data they share with processors. For example, a controller may share a limited data set with a processor that does not include the means "reasonably likely" to enable identification of data subjects (in accordance with the criteria laid out in the ECJ's decision in EDPS v. SRB (C-413/23 P)). The controller may also adopt contractual and technical safeguards to prevent the processor from accessing identifying information or attempting reidentification. In this scenario, the analysis should focus on whether the information is anonymous for the processor. Instead, the Draft Guidelines discourage these privacy-protective steps, because the information remains personal data when handled by the processor whether the controller adopts such measures or not.

This result cannot be squared with the Draft Guidelines' contextual approach to anonymisation and must be revised. Rather than asking only whether information is personal data for a controller, the Draft Guidelines should also ask whether information is personal data for a processor. The contrary approach, adopted in the Draft Guidelines, fails to reflect the practical circumstances in which processors receive and handle data — and is at odds with the GDPR's risk-based, privacy-protective objectives.

BSA recommends that the EDPB:

- **Revise the Draft Guidelines to assess whether information is anonymous from the perspective of a processor, rather than only asking if data is anonymous to the relevant controller.**
- **Recognise that processors may handle data anonymously, based on a controller's instructions, limited data shared with the processor, and applicable technical and organisational measures.**

2. More Certainty is Needed on Means "Reasonably Likely to be Used."

Under the Draft Guidelines, data is not anonymous if an individual can be distinguished from others "using means reasonably likely to be used" and in a way that makes it possible to treat them differently. Whether means are reasonably likely "will depend on the relevant entity's perspective and should be assessed in light of all objective factors." The Draft Guidelines set out a range of factors to consider in this analysis, including five factors about whether an entity is likely to use certain means (in Paragraph 29), nine types of entities that may be relevant entities (in Paragraph 30), and four factors that may be relevant to rebutting the presumption that people will generally follow the law (in Paragraph 33). The Draft Guidelines also use phrases like "insignificant" and "disproportionate effort" without explaining what they mean.

The Draft Guidelines must be revised to provide more certainty about what means are considered "reasonably likely to be used" to reidentify relevant individuals. This standard is core to the Draft Guidelines but is not developed. For example, the Draft Guidelines do not indicate which factors may increase the realistic likelihood of identification and which may reduce that likelihood. In particular:

- *Unauthorised access should be more clearly addressed*. Paragraphs 26, 30, 31, and 33 indicate that an assessment of anonymity may consider means available to persons other than the controller or recipient — including unauthorised or accidental access like rogue employees, hackers/cybercriminals, investigative journalists, intelligence agencies or unethical companies. Treating these as "relevant entities" creates a standard that makes anonymisation unattainable. We recommend that the Final Guidelines focus an assessment of the likelihood of reidentification on the operational and contractual measures that an entity has adopted to avoid unlawful or ill-intended attempts to access data. This avoids treating all potential unlawful access as "relevant". The mere possibility of employees that may go rogue or hackers that may infiltrate systems should not establish reasonable likelihood of reidentification.

- *More weight should be afforded to effective and enforceable contractual measures*. The Draft Guidelines do not give contractual measures meaningful weight in preventing reidentification. This is difficult to reconcile with relevant case law and other aspects of the EU digital regulatory framework. This approach once again discourages companies from entering into privacy-protective contracts, undercutting incentives for strong privacy and security practices.

BSA recommends that the EDPB:

- **Clarify that unauthorised access is relevant to the "reasonably likely" analysis only when facts show a realistic likelihood of unauthorised access.**
- **Clarify that accidents and negligence, referenced in Paragraph 31, are relevant to the reasonably likely analysis only if they are reasonably foreseeable in the circumstances.**
- **Give more weight to effective and enforceable contractual mechanisms, including expressly recognising that the reasonably likely analysis should consider whether a contract is binding and supported by technical and organisational controls.**

3. The Simplified Approach Should Not Become an Extra-Legal Default.

The Draft Guidelines set out both a contextual approach to anonymisation that reflects the nuances of the legal standard and a simplified approach, which can go beyond the legal standard. Although the Draft Guidelines describe the simplified approach as a voluntary way for controllers to approach anonymisation, in practice it may become a default that goes well beyond the contextual approach of the GDPR.

BSA recommends that the EDPB:

- **Clearly state that the contextual approach represents the legal test under GDPR.**
- **Clearly state that the simplified approach is optional, and that controllers retain the determination of whether to switch from a simplified assessment to a contextual one.**

4. Anonymisation, De-Identification, and De-Personalisation Should Not Be Treated as Equivalent.

The Draft Guidelines caution controllers against using descriptions like anonymous, de-identified, or de-personalised if individuals "are actually still identifiable." This language in Paragraph 40 conflates these very different terms. The terms de-identified and de-personalised are widely used to indicate that de-identifying measures have been applied to data, but that the resulting information may not meet the standard for anonymity. Suggesting these concepts and terms are interchangeable will cause widespread confusion, as organisations rely on them to indicate distinct levels of identifiability and technical controls.

In addition, while we appreciate that the Draft Guidelines expressly recognise (in Paragraph 39) that anonymisation of data can be a positive factor in a legitimate interests balancing test, we recommend revising this language to recognise that de-identification and de-personalisation may also be positive factors.

BSA recommends that the EDPB:

- **Revise Paragraph 40 so that it cautions against describing data as "anonymous" or "anonymised" when individuals are still identifiable. References to "de-identified" and "de-personalised" should be removed.**

- **Revise Paragraph 39 to recognise that measures beyond anonymisation, including de-identification and de-personalisation, should also be weighed positively in a legitimate interests balancing test.**

5. The Draft Guidelines Lack Practical Guidance About Using Privacy Enhancing Technologies.

The Draft Guidelines extensively address the legal test for anonymisation but do not connect this analysis to practical tools that companies may use to de-identify data. For example, the Draft Guidelines do not explain how the criteria of No Record Isolation, No Linkage, and No Inference can be achieved through the use of privacy enhancing technologies. The Draft Guidelines also do not address the application of anonymisation principles to AI-related use cases, such as model training, model evaluation, or the generation of synthetic data. More guidance is needed to support greater legal certainty and consistent application across industries, encouraging the use of privacy-preserving technologies. For example, footnote 43 provides a test to compare outputs with and without an individual's records, but would be significantly strengthened with a worked example.

BSA recommends that the EDPB:

- **Provide practical guidance mapping common privacy enhancing technologies to the three criteria and explaining their legal effect.**
- **Provide practical examples of using privacy enhancing technologies, including in AI-related processing activities.**

6. The Draft Guidelines Should Provide More Practical Guidance and Examples.

Standard for identifiability. In addressing whether information is "identified or identifiable," Paragraph 21 focuses on whether it "cannot be ruled out" that a receiving entity has the means to identify the individual through means reasonably likely to be used. That standard — of "cannot be ruled out" — should be revised to align with the standard in the following paragraph, which states that the likelihood of reidentification does not need to be zero, but must be "insignificant in reality."

Contractual provisions. The Draft Guidelines require organisations to consider the "actual strength" of contractual measures, which "should be reliable, verifiable, and enforceable." We strongly recommend providing an example of contractual measures that meet this test. For example, a platform's terms are binding on application developers, backed by API access controls, review of applications on the platform and potential revocation of access if those terms are violated.

For further information, please contact Thomas Boué,

Vice President and Director General, Policy – EMEA, at thomas@bsa.org.