Response to EDPB Guidelines 02/2026 on Anonymisation

Public consultation submission | Submitted in a personal capacity by an individual based in Japan | 29 October 2026

Purpose and scope

I welcome the European Data Protection Board (EDPB)'s work to provide a practical, context-sensitive framework for assessing anonymity. In particular, I support the proposed distinction between whether information is anonymous under the GDPR and whether personal data is protected by security measures. My comments focus on how the guidance might explain the contribution, and the limitations, of modern distributed data-protection architectures.

1. Clarify the role of technical and organisational safeguards (paragraphs 88-91)

Paragraph 90 appropriately states that technical, organisational and contractual measures may restrict access, but cannot by themselves render data anonymous. Paragraph 91 makes a similarly important distinction for encryption. I suggest adding an expressly technology-neutral example explaining that other protective measures - including secret sharing, all-or-nothing transforms (AONT), distributed storage, separation of recovery information, and independently administered trust domains - may also restrict practical access to intelligible information without automatically making that information anonymous.

In particular, a fragment that is unintelligible in isolation does not necessarily mean that the underlying information has ceased to be personal data in all relevant contexts. Reconstruction capabilities, collusion, related metadata, residual copies, authorisation structures and access available through third parties must still be assessed. Secret sharing and AONT should not be treated as equivalent technologies or as automatically achieving anonymisation.

2. Consider data-breach scenarios when assessing the contextual approach (paragraphs 88-90 and Example 22)

The Guidelines already recognise that a data leak may change the means of identification available to a relevant entity (paragraph 88), and Example 22 explicitly considers leakage through human error or cyber intrusion. These are important and practical observations. I encourage the EDPB to include a short implementation example distinguishing two scenarios:

- A compromised system yields a complete, intelligible dataset that can readily be copied or linked to external information.
- A compromised system yields only non-reconstructable fragments or protected representations, while the independent material and privileges needed to reconstruct intelligible records remain unavailable to the attacker.

The second architecture may reduce the volume of intelligible information exposed by a single compromise, depending on its actual design and threat model. However, the assessment should explicitly consider whether attackers can compromise several domains, obtain reconstruction material, exploit exposed endpoints, or combine fragments with other accessible information. No architecture should be assumed secure merely because data is distributed.

3. Preserve the distinction between anonymity and risk-reducing protection

I respectfully recommend a concise decision aid distinguishing (a) an affirmative conclusion of anonymity after applying the Guidelines' applicable legal and technical tests, (b) personal data protected by pseudonymisation or other privacy-enhancing or security measures, and (c) personal data that remains accessible in intelligible form after a foreseeable single-system compromise. This would discourage both overclaiming that protected or fragmented data is anonymous and undervaluing additional measures that meaningfully limit exposure even where the GDPR continues to apply.

The proposed tests of No Record Isolation, No Linkage and No Inference should remain decisive for the anonymity assessment; supplementary controls should inform the factual assessment of access and relevant entities, not replace those tests.

4. Encourage practical, technology-neutral evaluation

For sensitive settings such as health research, financial services and AI-enabled data analysis, the EDPB could recommend that controllers document:

- What intelligible personal information could be obtained following compromise of one device, administrator account, service provider or storage location;
- Which separate permissions, fragments, keys or recovery materials would be needed to reconstruct information, and whether they share a common point of failure;
- The consequences of collusion, backups, endpoint compromise, data exports, metadata exposure and unauthorised linkage; and
- Whether protections remain operationally proportionate, testable, recoverable and compatible with the rights of data subjects.

As a non-exclusive illustration of an existing commercial approach, Japan's ZenmuTech offers distributed data-protection technology, including ZENMU Virtual Drive. Mention of this example is not a claim that any particular product renders data anonymous, meets a specific GDPR requirement, or is suitable for all use cases. Such approaches should be evaluated independently against the same criteria as alternatives.

5. Suggested addition to the Guidelines

“Where relevant to the contextual assessment, entities may consider the extent to which properly implemented technical and organisational safeguards restrict access to intelligible information, including in foreseeable incidents such as a data breach. Such safeguards may include encryption and, where appropriate, distributed-data or split-trust arrangements. These measures do not, in themselves, establish anonymity. The assessment must continue to examine the relevant entities, the means reasonably likely to be used, any feasible reconstruction or combination of information, and the criteria of No Record Isolation, No Linkage and No Inference.”

Conclusion

I encourage the EDPB to clarify how modern post-compromise data-protection measures can contribute to an accurate contextual assessment without weakening the legal threshold for anonymity. A technology-neutral explanation would help organisations select proportionate safeguards while maintaining full GDPR protections where the information remains personal data.

Reference: EDPB, Guidelines 02/2026 on Anonymisation, version 1.0 (7 July 2026), especially paragraphs 88-92 and Example 22.