Comments on EDPB Guidelines 02/2026 on Anonymisation

The MPC Alliance welcomes the European Data Protection Board's work to clarify when information can be considered anonymous under the GDPR. Our comments focus on the treatment of privacy-enhancing technologies, particularly secure multiparty computation (MPC). MPC allows several parties to compute an agreed result from their respective inputs without having to disclose those inputs to one another.

This can be useful where organizations need to produce joint statistics or conduct analysis without creating a central collection of individual-level records. The technique does not, however, make every output anonymous. The result, the information revealed during the protocol and any other information available to the parties must still be assessed.

From our perspective, the industry needs clearer guidance on how cryptographic safeguards should be considered in the contextual assessment and examples showing how privacy-preserving computation can be combined with controls on what the result discloses.

Sincerely,

Giannis Rousopoulos
Executive Director
MPC Alliance

Consider the actual information available to each party

Relevant provisions: paragraphs 9, 13, 20, 28-30 and 88-91.

The guidelines correctly require an assessment of the means reasonably likely to be used by the relevant entities. In MPC systems, that assessment depends on the precise information a party can see: its own input, any messages or intermediate values made available by the protocol, the agreed output and any additional information it can obtain. It is not enough to assume that every participant can access all inputs simply because the participants take part in the same computation.

Equally, it would be wrong to assume that separation of inputs always prevents identification. Depending on the protocol and deployment, several participants may be able to cooperate, or a party may acquire information outside the protocol. An assessment should therefore identify the relevant collusion threshold, the parties controlling the infrastructure and keys, and the likelihood that additional information can be combined with the output.

We recommend that section 3.5.2 state expressly that verifiable technical restrictions on the information accessible to each party may be considered when applying the contextual approach. Their significance should depend on the protection they provide in the deployment being assessed, including the possibility of collusion or compromise, rather than on a general description of the technology.

Distinguish input confidentiality from output anonymity

Relevant provisions: paragraphs 50-52, 66-82 and 91.

The most important clarification is that a secure computation and an anonymous result are two different things. MPC can protect inputs while a calculation is carried out. It does not by itself prevent the authorized result from disclosing information about an individual. A computation returning a single person's salary, for example, does not become anonymous because MPC was used to produce it.

Conversely, an MPC deployment might compute a sufficiently protected aggregate without sharing the underlying individual records between participants. In that case, the anonymity assessment should focus on the actual output and on any other information accessible through means reasonably likely to be used. The mere fact that identifiable inputs were processed does not establish that the resulting statistic is personal data in the hands of every recipient. The processing of those original inputs remains subject to the GDPR where applicable.

We suggest including a short example in section 3.4.3: several hospitals use MPC to calculate a joint health statistic without exchanging patient-level records. The final figure may be anonymous if it cannot reasonably be used, alone or with accessible information, to single out patients or draw specific, meaningful inferences about them. A small subgroup result or repeated overlapping queries may fail that test. The example should examine both outcomes.

Address repeated queries and cumulative disclosure

Relevant provisions: paragraphs 76-82 and 87.

We welcome the discussion of how aggregate statistics and query systems may allow inferences about individuals. This deserves more practical attention, particularly where a service returns multiple outputs over time. Individual results may appear harmless when viewed separately but may disclose sensitive information when compared, combined or subtracted from one another.

For systems using MPC, as for other systems, the evaluation should cover the complete disclosure surface, not only a single output. Relevant controls can include minimum group sizes, restrictions on overly precise or overlapping queries, query limits, disclosure review and, where appropriate, formal privacy mechanisms such as differential privacy. The safeguards chosen should follow the type of result and the identified attack, rather than being prescribed for every deployment.

We recommend that paragraph 77 or 82 explicitly refer to cumulative disclosures and that the practical guidance invites assessors to test sequences of outputs and realistic auxiliary information, including knowledge held by a participating organization about its own input data.

Explain how cryptographic safeguards should be evidenced

Relevant provisions: paragraphs 29, 34, 41 and 88-91.

The draft correctly rejects the idea that encryption or contractual restrictions automatically make data anonymous. It would nevertheless help controllers and supervisory authorities if the guidelines identified the evidence that can support reliance on an appropriately deployed cryptographic control.

For MPC, an assessment could document the purpose and output of the computation; the information accessible to each participant; the security assumptions of the protocol; the number or combination of parties required to reveal protected information; the management of keys and secret shares; access controls; any known leakage; and the consequences of participant collusion or system compromise. Independent technical review or testing may be appropriate for higher-risk deployments.

This should not become a compulsory checklist or a certification requirement. A short, non-exhaustive description of relevant evidence in section 3.5.2 would make the contextual approach easier to apply consistently, while leaving room for new protocols and different use cases.

Give greater weight to the separation of data and capabilities

Relevant provisions: paragraphs 20-21, 28-30 and 89-90.

Paragraph 20 explains that identification may depend on means distributed across different parties. That is an important point. The corresponding question should be whether those means can realistically be brought together. Cryptographic separation is intended precisely to prevent one party from acting alone. If the technical design requires cooperation by several independent parties before protected information can be revealed, the feasibility and likelihood of that cooperation should form part of the analysis.

We recognize that arrangements described as distributed are not necessarily independent in practice. Common ownership, shared administrators, key custody, subcontracting and incentives to cooperate may undermine the separation. We recommend the guidelines to encourage assessment of the system as deployed, rather than treating either distributed architecture or a single-party breach scenario as conclusive.

Provide practical guidance on review over time

Relevant provisions: paragraphs 35, 41-42 and 88, 92-93.

We agree that anonymity may need to be reassessed as technology and available information change. It would be more useful to link reassessment to identifiable changes in risk. Examples include material changes to the output or permitted queries; a new source of auxiliary information; a change in participants or their control relationships; a protocol vulnerability; compromise of keys or shares; or a meaningful advance in attacks against the cryptographic assumptions used.

A risk-based approach with documented review triggers would be more workable than an expectation of continuous technical re-evaluation. It would also give organizations a clearer way to demonstrate that the initial assessment remains valid.

Recommended changes to the final guidelines

A few targeted additions could help provide further clarity on the application of the guidelines to cryptographic systems. The MPC Alliance would welcome the opportunity to contribute technical examples to support the EDPB's work. In particular, we invite the EDPB to consider the following:

• Including an example of MPC-based joint statistical analysis in section 3, illustrating both an anonymous output and an output that permits inference about an individual.

• Clarifying in section 3.5.2 how the contextual approach can take account of tested cryptographic controls that limit what each relevant entity can access, including the realistic possibility of collusion or compromise.

• Explaining that protection of inputs during computation does not, on its own, establish anonymity of the output, which would still need to be assessed against No Record Isolation, No Linkage and No Inference.

• Expanding the discussion of query systems to address repeated queries, overlapping populations and the combined effect of multiple releases.

• Providing non-exhaustive examples of technical evidence and circumstances that may warrant risk-based reassessment for systems that depend on cryptographic separation.