

Consultation Response: Guidelines 02/2026 on Anonymisation

Respondent: Jiri Svorc, Solicitor and Independent Legal Consultant

General observations

I welcome the EDPB's efforts to provide greater clarity on the concept of anonymisation and the distinction between anonymous and personal data. In practice, this remains one of the most difficult areas of data protection law, particularly as organisations increasingly rely on advanced analytics, artificial intelligence, research collaborations and large-scale data sharing.

The draft Guidelines make a valuable contribution by emphasising that anonymisation is ultimately a contextual exercise. I also welcome the practical framework built around the risks of isolation, linkage and inference, which should help organisations move beyond purely theoretical discussions and towards a more structured assessment of anonymisation outcomes.

From my perspective as a legal adviser working with technology companies and research and innovation projects, the Guidelines would benefit from several further clarifications aimed at improving practical implementation.

Comment 1: Additional guidance for AI-related use cases

One area where additional practical guidance would be particularly valuable is the growing use of artificial intelligence technologies.

Many organisations are now working with foundation models, fine-tuning datasets, retrieval-augmented generation systems, vector databases and embeddings, and synthetic data generation.

While the legal principles governing anonymisation remain unchanged, the technical environments in which those principles must be applied have become significantly more complex.

For example, organisations often struggle to assess whether information remains personal data once it has been transformed into embeddings, model parameters or other derived representations. Likewise, there remains uncertainty regarding the role of anonymisation when synthetic datasets are generated from personal data.

JIRI SVORC

Solicitor

EMPOWERING INNOVATION
ENSURING INTEGRITY

+420 737160737
+44 (0)7588542026
jiri@jiri.legal
www.jiri.legal

167-169
Great Portland Street
London, W1W 5PF
United Kingdom

Vrchlabska
1131/22
Prague, 19700
Czech Republic

I would therefore encourage the EDPB to include a dedicated annex or a series of worked examples demonstrating how the anonymisation framework should be applied in common AI-related scenarios.

In my view, practical examples would be one of the most effective ways of increasing legal certainty and promoting consistent implementation across Member States.

Comment 2: Applying anonymisation principles to AI models and derived representations

Related to the above, it would be helpful to provide additional guidance on how the anonymisation assessment should be applied to AI models and model components themselves.

Recent regulatory discussions have demonstrated that uncertainty remains regarding trained models, model parameters, embeddings, latent representations; and generated outputs.

Many organisations are trying to understand where the boundary lies between personal data, anonymised data and information that falls somewhere in between. While the answer will inevitably depend on the context and the specific technology involved, additional explanation would assist organisations in applying the principles contained in the Guidelines consistently.

A dedicated section addressing these issues would, in my view, significantly improve the usefulness of the Guidelines for organisations developing and deploying AI systems.

Comment 3: A proportionate approach in research and innovation settings

One aspect of the draft that could benefit from further development is how the principles of proportionality and risk-based accountability apply in research and innovation settings.

In my experience, project partners frequently encounter situations where the actual privacy risk appears very limited, yet there is considerable uncertainty about the level of assessment, testing, documentation and governance expected of them. This is particularly common in collaborative projects involving universities, research organisations, SMEs, cultural institutions and public authorities.

A typical example is the collection of basic public engagement or user-feedback information. An organisation may deliberately limit the information collected to a small number of satisfaction or evaluation questions and have no intention of identifying

participants. Nevertheless, a third-party digital tool may process technical information in the background. This can leave project partners uncertain about where to draw the line between sensible risk management and a full-scale compliance exercise that appears disproportionate to the actual risks involved.

The position can become more complex where several organisations participate in the same project. Information that is anonymous from the perspective of one participant may not necessarily be anonymous from the perspective of another participant with access to additional data or contextual information. The Guidelines rightly recognise that anonymisation is contextual, but further examples would help organisations apply that principle in collaborative settings.

I therefore encourage the EDPB to include practical examples covering:

- consortium-based research and data sharing;
- pilot deployments and user testing;
- citizen engagement and public demonstrations;
- educational activities, including activities involving minors;
- cultural heritage initiatives; and
- low-risk evaluation and feedback exercises using third-party digital tools.

The principle of accountability remains essential and should not be weakened. However, the Guidelines should expressly recognise that the depth of an anonymisation assessment, and the associated testing and documentation, should be proportionate to the nature, scope, context and actual risks of the processing.

This would not reduce protection for individuals. It would help organisations concentrate their resources on meaningful identification risks, while avoiding disproportionate exercises directed at largely theoretical risks where data collection has already been deliberately minimised. It would also help project partners distinguish between situations requiring extensive anonymisation analysis and those in which a more limited, documented assessment may reasonably be sufficient.

Conclusion

Overall, I strongly welcome the publication of these Guidelines and the EDPB's efforts to provide greater clarity regarding anonymisation.

The areas identified above all stem from a common practical challenge: organisations increasingly understand the legal principles, but often struggle with their application in complex, technology-driven and collaborative environments.

Additional guidance on AI-related use cases and on the proportionate application of anonymisation requirements in collaborative research and innovation settings would, in my view, significantly increase the practical value of the Guidelines while maintaining the high level of protection that EU data protection law seeks to achieve.

Thank you for the opportunity to provide feedback.