Dassault Systèmes contribution to the EDPB public consultation on Guidelines 02/2026 on Anonymisation

Dassault Systèmes welcomes the publication of the proposed guidelines on anonymisation and welcomes the opportunity to contribute to the ongoing consultation from a software provider operating in the medical sector's perspective.

Who we are

Dassault Systèmes is an EU-based purpose-driven company creating Virtual Worlds for Real Life with a €6.24 billion revenue in 2025. Our solutions portfolio, increasingly delivered as cloud/SaaS, serves 390,000+ customers across 12 industries. Furthermore, Outscale, our own cloud operator, offers a strategic infrastructure for business experiences based on our solutions.

Background

In life sciences and healthcare, our software supports clinical research, drug development and the modelling of the human body ("virtual twins"). The data we receive is in most cases pseudonymised at source: direct identifiers and re-identification keys remain with the controller and never enter our platforms. Furthermore, numerous safeguards ensuring the non-identification of the persons are often already in place. In this field, our partners (research institutes, hospitals) have a predominant role on the qualification of the nature of the data that is used.

Summary of recommendations

- **Recommendation 1**: Take into account legal obligations that restrict access to identification keys held by another entity.
- **Recommendation 2**: Recognise the contribution of verifiable and enforceable safeguards to the assessment of the risk of identification.
- **Recommendation 3**: Provide a worked example based on the acquisition of clinical datasets by a software provider.
- **Recommendation 4:** Ensure coherence with the Digital Omnibus and the forthcoming EDPB opinion on pseudonymisation and anonymisation.

Detailed recommendations

Recommendation 1: Take into account legal obligations that restrict access to identification keys

Dassault Systèmes recommends that the guidelines specify that an identification key which remains with the transferor, and which the transferor is legally prohibited from disclosing (for instance by medical secrecy or by the confidentiality obligations of the GDPR), should not be considered a means reasonably likely to be used by the recipient. This would complement the

existing guidance on legal prohibitions (paragraphs 32–33) and reflect the realities of data sharing in the healthcare sector.

Recommendation 2: Recognise the contribution of verifiable and enforceable safeguards

Dassault Systèmes recommends that the guidelines recognise that technical, organisational and contractual safeguards, where they are reliable, verifiable and enforceable, may contribute, together with the characteristics of the data, to demonstrating that the risk of identification is insignificant for the recipient.

These safeguards may include:

- the absence of access to keys or linkage attributes;
- the segregation of the dataset from the recipient's other data;
- a prohibition of re-identification and onward transfer, supported by audit rights and sanctions;
- the logging of access.

This approach would be in line with recital 27b of the Council's position, which refers to the actual measures in place, and would encourage the adoption of robust safeguards in the sector.

Furthermore, the guidelines should be coherent on the fact that anonymity does not require the likelihood of reidentification but only that it be insignificant (as entailed in paragraph 22).

Finally, the provision of a concrete example of methodologies and tools (e.g. software) ensuring non-reidentification would be beneficial.

Recommendation 3: Provide a worked example based on the acquisition of clinical datasets

Dassault Systèmes recommends that the guidelines include a practical example in which a hospital supplies pseudonymised clinical datasets, including medical imaging, to a software company for product development. The example should illustrate the assessment of the risks of singling out, linkage and inference from the recipient's perspective, and show that the same dataset may be anonymous for the recipient and personal for the hospital. A contrasting case in which the data remains personal, for instance owing to a rare condition or the possibility of linkage with other data held by the recipient, would further enhance its clarity.

Recommendation 4: Ensure coherence with the Digital Omnibus and the forthcoming EDPB opinion

Dassault Systèmes recommends that the guidelines be reviewed once the Digital Omnibus is adopted, and be aligned with the opinion that the Council's position envisages for the EDPB on pseudonymisation and anonymisation. Dassault Systèmes would welcome the inclusion of the health sector in that opinion, as well as the development of a sectoral code of conduct, in order to support legal certainty and innovation in the European Union.