UNIVERSITY OF TURKU

25 June 2026

Public consultation reference: 1/2026

Comments on the EDPB Guidelines 1/2026 on processing of personal data for scientific research purposes

The University of Turku thanks the European Data Protection Board for the opportunity to provide feedback on the draft Guidelines.

We welcome the EDPB Guidelines on the processing of personal data for scientific research, which are timely and much needed. Some aspects would benefit from further clarification to make the Guidelines easier to apply consistently across Member States.

Lawfulness

The Guidelines provide extensive guidance on consent as a lawful basis, which is understandable given the well-known challenges associated with its use in research.

In practice, however, a large share of scientific research is carried out on the basis of public interest (Article 6(1)(e) in combination with Article 9(2)(j)), often as defined in Member State law.

Although this legal basis is acknowledged, it is not reflected in the examples or discussed in detail. Given its importance in several Member States, more concrete guidance on its application in research, including in relation to transparency, would be useful.

Open science

Researchers are increasingly expected to balance open science requirements with data protection obligations. A few practical examples illustrating when data can be shared openly and when access should be restricted would improve the usability of the Guidelines.

Transparency obligations in research practice

The Guidelines rightly emphasise transparency towards data subjects. At the same time, the GDPR recognises a special regime for scientific research, which reflects both its public interest function and its basis in fundamental rights, including the freedom of science. This framework relies on ethical oversight and appropriate safeguards.

In practice, a key difficulty arises in situations where the controller carrying out the research does not have access to data subjects' contact details. This is common in research infrastructures where data are provided through a central authority acting as an intermediary. In such cases, the Guidelines assign responsibility for informing data subjects to a controller who may have no practical means to do so, resulting in a misalignment between responsibility and control.

University of Turku
Postal address FI-20014 University of Turku, Finland / Telephone +358 29 450 5000 / Business ID 0245896-3
www.utu.fi/en

Against this background, the special regime for scientific research should be more clearly reflected in how transparency obligations are applied in practice. In particular, the Guidelines should clarify how Article 14 should be applied in situations where individual notification is not realistically achievable, and how alternative forms of transparency can be used together with appropriate safeguards.

Allocation of transparency responsibilities between controllers

While the Guidelines clarify in Section 5.4 that the receiving controller is responsible for providing information under Article 14, it remains unclear how this obligation should be fulfilled in practice.

This is particularly relevant in research contexts where personal data are obtained from another controller and processed by a different controller for its own purposes, such as between research organisations, and where the receiving controller does not have access to contact details of the data subjects.

In such cases, the guidance refers to cooperation between controllers as a good practice. However, it would be helpful to clarify how responsibilities should be allocated and fulfilled where the receiving controller cannot directly inform data subjects, and the extent to which reliance on the providing controller or on indirect forms of information is considered sufficient.

Data minimisation and identifiability

Some aspects of the guidance are difficult to reconcile with data minimisation (Article 5(1)(c)) and Article 11 GDPR.

In many research settings, identifying information is removed as soon as it is no longer needed. However, if transparency obligations are interpreted as requiring controllers to retain or reintroduce identifying data in order to inform individuals at later stages, this creates a clear tension with these principles.

Article 11 makes clear that controllers are not required to keep or obtain additional information solely to identify data subjects. Read together with the principle of data minimisation, this suggests that controllers should not be expected to retain or recreate identifiers solely in order to comply with information obligations.

This point would benefit from clearer guidance in the Guidelines.

Pseudonymisation and re-identification risks

The suggestion that data subjects could be informed through pseudonyms does not fit well with systems where pseudonymisation is specifically designed to prevent any link back to individuals.

Allowing or requiring such linkage would weaken these safeguards. It may lead to identifiers being kept or reintroduced even when they are not needed, which is not in line with the principle of data protection by design and by default.

Means of providing information

More concrete guidance is needed on when indirect forms of information, such as providing information via publicly accessible websites, can be considered sufficient. In particular, it would be helpful to clarify under what conditions website-based information meets the requirements of Article 14, taking into account factors such as the scale of the dataset, the availability of contact details, and whether data subjects are likely to be effectively reached in practice through these means.

It would also be useful to clarify to what extent such approaches may be appropriate more generally, including in research settings where data are collected directly from data subjects.

Disproportionate effort

The concept of “disproportionate effort” under Article 14(5)(b) should not be interpreted too narrowly. In large-scale datasets, contact details may in principle be obtainable, but this may require extensive additional processing and significant administrative effort.

In such cases, proportionality should take into account both feasibility and the limited practical impact on their ability to exercise their rights.

In practice, approaches to individual notification in register-based research vary considerably. Similar types of research may lead to very different outcomes, ranging from situations where no individual notification is provided to cases where significant resources are used for large-scale notification efforts.

This variation suggests that further guidance is needed to clarify when individual notification is required and what constitutes a proportionate approach.

This is further complicated by the fact that obtaining accurate and up-to-date contact details may require retrieving them from population registers. In practice, this involves the use of personal identifiers and the creation of new datasets.

This constitutes a significant additional processing of personal data carried out solely for the purpose of providing information. At the same time, using outdated or incomplete contact details may not effectively reach data subjects.

These factors should be taken into account when assessing whether individual notification is proportionate.

Publicly available data relating to public figures

Different considerations may also apply where research is based on publicly available data relating to public figures. It would be helpful to include examples illustrating how transparency obligations apply in such situations. In particular, clarification would be needed on whether, and under what conditions, individual notification is required where research is based on publicly available data relating to public figures.

Transparency in large-scale research infrastructures

In large-scale research infrastructures, where data are made available for research through central authorities and researchers do not have direct access to data subjects' contact details, transparency cannot be effectively managed on a project-by-project basis. There is a risk of inconsistent outcomes, even where identical datasets are used.

A more workable solution is to address transparency in a consistent, central way, ensuring that information is provided in a consistent and scalable manner, for example through publicly accessible information at system level.

Article 14(5)(c)

Article 14(5)(c) is intended to allow Member States to regulate the use of personal data through statutory frameworks, including research infrastructures.

The interpretation in the Guidelines appears to require a level of information that is close to Article 14 itself. This risks limiting the practical relevance of the exception.

In systems where data are provided on the basis of law through a central authority, individual notification is often not feasible. Without a more flexible approach, the obligation to inform falls on a controller who cannot fulfil it in practice.

It would be helpful to clarify that Article 14(5)(c) can also be met through centralised transparency arrangements, provided that appropriate safeguards under Article 89(1) GDPR are in place. These include, for example, pseudonymisation, secure processing environments, strict access controls, limitations on re-identification, and clear, accessible public information.

Joint Controllership

We would like to emphasize that, under Article 26 GDPR, joint controllers must, in a transparent manner, determine their respective responsibilities by means of an arrangement between them. The essence of this arrangement must be made available to data subjects.

While a joint controllership agreement is often an appropriate tool to document such an arrangement, in certain cases the arrangement may also be reflected, for example, in a privacy notice. We would welcome this being acknowledged in the Guidelines (para. 144).

Conclusion

The Guidelines address important issues and have the potential to improve consistency across the EU. Further clarification on the points above would make the Guidelines more useful in practice and better reflect how research is actually conducted, while maintaining a high level of data protection.