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

The Small GDPR Network (the network) is a network of lawyers at Swedish universities and higher education institutions who regularly coordinate and discuss data protection issues. Most are public authorities; others are foundations that, to varying degrees, are subject to rules of public law.

1. GDPR in relation to research and archiving obligations

In Sweden, most universities are required to archive research data, often for an indefinite period. The network considers that the Guidelines lack clearer reasoning on how such legal requirements should be weighed against the requirements of the GDPR.

We would particularly welcome clarifications on:

- how the right to withdraw consent under Article 7.3 GDPR operates where consent is used as the legal basis, while archiving is also required by law
- how the rights in Articles 15–21, in particular Article 17 and the exceptions in 17.3 (b) and 17.3 (d), should be understood where data may not be erased due to archiving requirements.

Example:
A Swedish university receives registry data from another authority. When the data arrive at the university, the data become an official document that must be archived. A data subject requests erasure. The university may possibly refrain from further research using that person's data, but may not erase the research data itself from the archive.

We ask that the EDPB describe more clearly how such conflicts between archiving obligations and data protection should be handled in research contexts. It risks being misleading for a research participant to give consent that, in reality, cannot be withdrawn, because the archiving responsibility often entails at least continued processing for archiving purposes.

2. Pseudonymised data, public registers and information obligations

Many research projects work only with pseudonymised data where the research principal does not have access to the coding key. This is used both as a safegaurd and because directly identifying data are not necessary for the research.

In light of the SRB judgment, we would welcome clarifications on:

- when pseudonymised data held by a higher education institution should be regarded as personal data, if the coding key remains with an authority that discloses the data
- whether the higher education institution is expected to request directly identifying data solely in order to fulfil information obligations under Articles 12–14 GDPR
- whether it is instead reasonable for the authority that collected the data to be responsible for informing the data subjects, even without being a joint controller or processor.

In Sweden, some higher education institutions understand that register-holding authorities rely on the exception in Article 14.5 (c) GDPR when they disclose research data. In practice, the procedure often results in neither the authority nor the higher education institution informing data subjects about extensive, recurring research projects using pseudonymised registry data.

We would therefore appreciate guidance on how the EDPB views the allocation of information responsibilities in such cases.

We would also be grateful if the EDPB could clarify whether and in which situations “data” are personal data for the university where the university:

- has no access to the coding key,
- has no legal or realistic means of gaining access to the coding key,
- is contractually prohibited from attempting to re-identify the individuals and also does not receive sufficiently detailed data to single out individual persons.

3. Section 5.2, Example 14 of the Guidelines - preserved safeguards

In Example 14, it is proposed that the controller asks its processor to compile information for the data subject, which is then provided to the data protection officer and thereafter to the data subject. This means that the controller gains access to more identifying information than before.

In this situation, many higher education institutions would instead allow the processor to respond directly to the data subject, in order to:

- maintain the safeguard that the controller does not know the identity
- simplify the handling, in line with the spirit of Article 11.

We ask that the EDPB clarify whether such a working method is compatible with the GDPR, and what requirements should then be imposed on the contract and instructions between the controller and the processor.

4. Exceptions from information obligations for pseudonymised registry data (section 5.4)

When higher education institutions obtain pseudonymised data from public registers, the question arises whether it is always necessary to obtain additional identifying data solely in order to inform the data subjects or to handle requests to exercise data subject rights.

In Sweden, it is technically straightforward to supplement the data with, for example, personal identity numbers and addresses, but this also leads to the higher education institutions processing more directly identifying data than the research requires, with increased risks as a result. It can be argued that obtaining directly identifying data solely for the purpose of providing information under Article 14, even where such identifiers are technically or legally accessible, may conflict with the principle of data minimisation, Article 11, data protection by design and safeguards under Article 89.

In addition, the Swedish Ethical Review Authority may approve exceptions from requirements for informed consent. Researchers sometimes perceive this as meaning that the information obligations under the GDPR also cease to apply, and invoke Article 14.5(c). In this situation as well, it can be argued that Article 11 could be interpreted as meaning that the controller should not be required to take measures that break a safeguard in order to facilitate the exercise of data subject rights.

We would like the EDPB to:

- discuss the interplay between Articles 11 and 14.5 (b)–(c) and national rules on ethical review and consent

- provide practical examples of whether and, if so, when it may be proportionate to exempt large register-based research projects using pseudonymised data, in whole or in part, from full information obligations, or alternatively to clarify how and by whom information should be provided.
- The example should not require information to be sent back to the controller where this would break an intentional separation measure. The Guidelines should recognise that the processor, in accordance with the controller's instructions and subject to contractual safeguards, may communicate directly with the data subject on behalf of the controller where this better preserves the protection under Article 11 and Article 89.

5. AI-related questions

Generative AI tools trained on large datasets may in some cases affect the assessment of whether data are "sufficiently" pseudonymised.

The network would welcome guidance on:

- how such AI-related risks should be taken into account when assessing whether data are personal data or not, and
- how this affects the assessment of pseudonymisation as a safeguard under Article 89.1 in research situations. AI methods may be used to re-identify individuals by indirect means.
- Guidance on the assessment. Is the risk assessment hypothetical, or based on realistic access to technology and data at present? Theoretical versus realistic risk of re-identification (SRB)

6. Allocation of responsibility: controller and processor

We find the examples on the allocation of roles in the Guidelines very useful, but more examples close to research practice are needed.

In some collaborations, several higher education institutions and researchers participate in steering groups and methodological decisions, without all parties having actual access to data or control over storage, security and practical handling. A strict interpretation of the concept of "purposes and means" may then lead to parties without actual visibility or control being regarded as controllers, even though they lack the ability to fulfil the requirements.

Interpretative difficulties also arise at the boundary between controllers and processors in situations where a processor is subject to regulatory requirements for its activities that make it wholly or partly an independent controller. This may concern, for example, clinics in clinical trials that collect data within regulated healthcare activities while at the same time participating in research on behalf of, for example, a higher education institution. Does this then become a processor relationship, a controller-to-controller situation, or some kind of combination?

Illustrative example of controllership:
A research project collects data from individual reporters in several countries on the status of climate change and the political willingness to work on these issues in each country. Over time, the research group establishes a recurring panel that responds "anonymously". A survey tool and the digital processing are managed by an external provider that is a processor for the university where the initiating researcher is employed.

The initiating researcher collaborates with three senior researchers at other universities globally. Together, they form a steering group that decides on research questions, survey design and overarching

ethical considerations. The three external researchers have no access to the database, do not decide on storage periods and do not control exactly what data are collected.

It can be argued that the steering group jointly determines the purposes and essential means of the processing and is therefore a joint controller. At the same time, its members have neither technical access to the database nor practical possibilities to fulfil the obligations of controllers. Alternatively, it can be argued that the university where the initiating researcher is employed is the controller.

We would therefore appreciate it if the EDPB would:

- develop more examples of when several research parties should be regarded as joint controllers, and
- when it is more reasonable for a higher education institution alone to be regarded as the controller, even if other researchers have contributed to the design of the study.
- Further develop whether it is possible for a steering group to determine purposes and means without bearing controller responsibility.

7. International collaborations and transfers to third countries

Research is often international and may involve samples or data moving between the EU and third countries. Here, the network sees a great need for more concrete guidance.

Example 1:
A company outside the EU engages a university in the EU to analyse pseudonymised samples and return the analytical results. The analytical method has been developed at the university within the EU, but beyond that there is no collaboration between the parties. The company subsequently links the results to identifying data. The university has neither the key nor identifying information, and obtaining such access would require extraordinary legal measures. The party within the EU has contractually undertaken not to attempt to re-identify the individuals.

Questions that arise include:

- whether the samples or analytical results should be regarded as personal data for the university (the SRB case)
- whether this, if so, means that the full rules on transfers to third countries and standard contractual clauses must be applied, even where neither the data subjects nor the commissioning party are otherwise subject to the GDPR.

Example 2:
A hospital in South America sends urine samples from agricultural workers to a university in the EU for pesticide analysis. The results are shared in pseudonymised form in a joint database in the United States, which several parties (EU and non-EU) use in their research. Only the South American hospital has the coding key. Later, new samples are collected and added to the same database.

We would like the EDPB to:

- explain further how the SRB judgment affects the assessment of when data from actors outside the EU should be regarded as personal data for a higher education institution in the EU that lacks realistic means of gaining access to the coding key
- provide guidance on when the GDPR's transfer rules should be applied in full in such research arrangements, and when this may be considered disproportionate

8. Consent as a legal basis

Many higher education institutions have applied the interpretation that the legal basis of consent is not appropriate in research and have generally instead recommended the performance of a task carried out in the public interest as the legal basis. See also prop. 2017/18:298 Behandling av personuppgifter för forskningsändamål, p. 40 et seq., for a more detailed discussion of the imbalance of power that may exist between the party carrying out the research and the research participant.

Although it is clarified that public-sector research principals may in many cases rely on consent, it is also made clear that an imbalance of power (for students, employees and also in medical research - patients) may make consent inappropriate.

The Guidelines, together with clarifications from the Swedish supervisory authority (Integritetsskyddsmyndigheten), suggest that consent may be used significantly more broadly than the legislator previously expressed in the preparatory works; see example 7 on page 21 of the Guidelines concerning a patient who is considered able to give consent, as long as the disease has not progressed and affected the ability to consent.

Taken together, and together with the exceptions for archiving purposes and further research purposes (section 3.1.2) for which the Guidelines leave scope, there is a risk of diluting the meaning of consent and giving data subjects a false impression that consents can be withdrawn. There is also a risk that consent as a legal basis is conflated with consents that constitute a safeguard (privacy-enhancing consents), which are only briefly addressed in the final part of the Guidelines, in section 8.5.

Example 7 on page 21 also raises questions as to whether corresponding reasoning may be applied in other contexts, for example when assessing whether a data protection impact assessment should be carried out because processing is likely to result in a high risk. See in particular criterion 7 (data concerning vulnerable data subjects) in the Article 29 Working Party's Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

We therefore welcome a more developed discussion in the Guidelines regarding:

- Explicit consent
- Advice and assessment criteria for assessing an individual's ability to give consent independently.
- Consent as a safeguard - what should the effect be if such consent is withdrawn?
- Whether the EDPB's reasoning, including in Example 7, should also be applied in other assessments under the General Data Protection Regulation.