Scientific research: How to lawfully process personal data

EDPB European Data Protection Board

June 2026

When your organisation processes personal data for scientific research purposes, you benefit from specific, flexible provisions under the GDPR. However, this flexibility is conditional on adopting appropriate safeguards to protect the fundamental rights and freedoms of the individuals involved: the research subjects.

The EDPB Guidelines on processing of personal data for scientific research purposes clarify what qualifies as scientific research and how to lawfully process data in this context.

To benefit from the GDPR's research exemptions, your activities must be genuinely scientific.

When determining whether processing is motivated by scientific research purposes, the following six key-indicative factors should be considered:

1. Follow a methodical and systematic approach
2. Adhere to ethical standards
3. Ensure verifiability and transparency
4. Maintain autonomy and independence
5. Pursue research objectives (contributing to society's general knowledge and wellbeing)
6. Demonstrate the potential to contribute to existing scientific knowledge (or apply it in novel ways)

Key responsibilities at a glance

Your duties apply from the initial design of the research project through to the dissemination of the results and storage of data for future research. Here is a checklist of your key responsibilities:

When to act	What to do
Before claiming research exemptions	**Verify the scientific nature.** Assess your project against the six key-indicative factors that should be considered, in addition to the nature, scope, context and purposes of processing. These factors are methodical approach, ethical standards, verifiability, autonomy, societal objectives, and novel contribution. **Ask yourself: Is our research aimed at contributing to society's general knowledge and wellbeing, or is this purely an internal data analytics exercise?**
When obtaining consent	**Determine the type of consent.** Decide whether to use "broad consent" (for a general area of research) or "dynamic consent" (for each specific projects). **Ask yourself: Are the exact purposes of the future research known today, or do we need flexibility?**
During the research lifecycle	**Maintain transparency.** Provide clear information to individuals, even if the research spans many years, using tools like privacy dashboards or project websites. **Ask yourself: Do your research participants know how their data is currently being used and might be used in the future?**
When applying safeguards	**Minimise the data.** Always anonymise personal data when this is possible; if identification is required for the research, you should pseudonymise the data, if possible, and add strict access controls. **Ask yourself: Can we achieve our research goals without knowing exactly who these individuals are?**

Principles in practice: Key issues

1. The presumption of compatibility

If you collect personal data for a specific purpose (even a non-research purpose) and later decide to use it for scientific research, this further processing is presumed to be compatible with the initial purpose. This means you do not need to conduct a standard compatibility test, but you must still ensure you have a valid legal basis (like legitimate interest or public interest) and implement appropriate safeguards.

2. Broad vs. dynamic consent

If the exact research purposes are not fully known at the time of data collection, you can rely on "broad consent" for a certain area of scientific research. However, to compensate for this lack of specificity, you should implement stricter safeguards, such as ethical oversight committees and enhanced transparency measures. Alternatively, "dynamic consent" involves asking users for consent iteratively as new projects or stages arise. It is also crucial to distinguish consent to participate in a study pursuant to ethical requirements, from consent under the GDPR as a legal basis for processing of personal data.

3. Transparency

You should offer research participants different options for how to stay informed about the processing of their personal data. If you want to use personal data from previous research in new research projects, you might not have to inform all research participants directly. However, if you have identifiers, such as a name or administrative identification number, you should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort.

4. Limiting the right to erasure and objection

Individuals have the right to request the erasure of their data or object to the processing. However, you can reject an erasure request if deleting the data is likely to render impossible or seriously impair the achievement of the scientific research. Similarly, you can reject an objection if the processing is necessary for a task carried out for reasons of public interest. These exceptions must be interpreted restrictively and assessed case-by-case.

Practical examples

Here are specific scenarios extracted from the Guidelines illustrating how these rules apply in practice:

Example 1

Presumption of compatibility

(section 3.1.1, paragraph 23, pages 17-18, example 6)

Context: A private research institute lawfully collects social media data to study the use of a particular dialect in written language. Later, they want to use this data to develop an app to conduct research on how to help individuals improve their spelling in that dialect.

What to do: The institute does not have to undertake a compatibility test for this secondary use, as further processing for scientific research is presumed compatible. They only need to assess their lawful basis (e.g., legitimate interest) and ensure safeguards are in place.

Example 2

Broad consent in practice

(section 4.1.2.1, paragraph 50, page 25, example 8)

Context: A network of university hospitals works together to create a federated database using pseudonymised patient data from medical treatment, to make that data available for future research projects across a broad range of specified medical disciplines. The specific research projects are not foreseeable at the time of treatment when consent is obtained.

What to do: Because the specific projects are not foreseeable at the time consent is obtained, the hospitals can rely on "broad consent" covering the broad range of agreed medical disciplines. To compensate for this lack of specificity, they implement safeguards: strict terms of use are followed by researchers; every future project is independently reviewed by an ethics committee; and the validity of consent is limited to five years.

Example 3

Rejecting a request for erasure

(section 6.2.2, paragraph 120, pages 48-49, example 19)

Context: A research institute is studying the historical development of an open-source software using a "merkle tree" that tracks every developer's contribution over time. A developer who changed their first name requests the erasure of their old name from the historical records.

What to do: The institute can reject the erasure request. Modifying the historical facts of the software's development would seriously impair the core objective of the research project, justifying the use of the research exemption.

The accountability checklist

Your organisation's action plan for conducting compliant scientific research:

Action point	Why it matters
1. Document the scientific nature	You should formally document how your project meets the six key criteria for scientific research.
2. Separate ethical and GDPR consent	Ethical consent to participate in a medical trial is not the same as GDPR consent to process data. Ensure that your consent forms or interfaces clearly distinguish between the two.
3. Establish oversight committees	Independent oversight of the research is a safeguard contributing to compliant processing of personal data, especially when relying on broad consent.
4. Implement strong pseudonymisation	Ensure there is a strict barrier between the research data and any contact details or identifiers. Technical measures and contractual penalties should be in place to prevent unauthorised re-identification.
5. Clarify joint responsibilities	In public-private partnerships or multi-university consortia, clearly document who is responsible for compliance with the GDPR, including answering individuals and helping them exercise their data protection rights.

This document provides a simplified overview of the guidelines. For more comprehensive legal explanations and examples, please consult the full text of the guidelines.

Read the complete guidelines