Response to the Public Consultation on the EDPB Guidelines 1/2026 on Processing of Personal Data for Scientific Research Purposes

Submitted by

Mireille M. Sant
Associate Professor and Head of the Department of Media, Communications and Technology Law
Principal Investigator, Data Integrity and Stewardship Research Cluster (DISC)
Faculty of Laws, University of Malta

Claude J. Bajada
Senior Lecturer, Department of Physiology and Biochemistry,
Chair, University of Malta MRI Research Platform
Faculty of Medicine and Surgery, University of Malta

Cyril Pernet
Associate Professor,
Neurobiology Research Unit, Rigshospitalet
Department of Health Technology, DTU, Denmark

Jochem Rieger
Prof. Dr. rer. nat. habil.
Applied Neurocognitive Psychology Lab,
Principal Investigator, DFG Center for Open and Reproducible Neuroscience Tools
Chair, COST Action INDoS CA24161
Department of Psychology, Carl von Ossietzky University, Oldenburg, Germany

June 2026

Introductory observations

We welcome the European Data Protection Board's preparation of dedicated guidance on the processing of personal data for scientific research purposes. The Guidelines address many long-standing areas of uncertainty and have the potential to provide useful clarification concerning broad consent, further processing, transparency, data subject rights, the allocation of responsibility and safeguards under Article 89(1) GDPR.

Our comments focus primarily on the practical application of the Guidelines within universities, hospitals, research infrastructures and international research consortia. These organisations vary considerably in their financial resources and technical capacity. Measures that are proportionate for a large national research infrastructure may be difficult to implement within a smaller university, regional hospital or investigator-led research group.

We write from an academic perspective, with particular experience in neuroimaging research and research data infrastructures. Several of our examples, therefore, draw on medical imaging, brain MRI, research repositories and secondary use of health-related datasets. These examples are intended to illustrate broader issues that arise across data-intensive scientific research. However, we would recommend a stronger acknowledgement of the diversity of practices across different fields of scientific research, ideally through the active involvement of practising researchers.

The final Guidelines should therefore distinguish more clearly between mandatory legal requirements, recommended good practice, and safeguards that may be appropriate only in particular circumstances. Without that distinction, non-mandatory recommendations may be treated by institutions, ethics committees or supervisory authorities as universal compliance requirements. Additionally, in order to be effective and efficient, they should further avoid duplication of assessment and avoid introducing slippery slopes for the freedom of science.

The overarching premise

The protection of personal data is a fundamental right and must be taken seriously. However, the right to data protection is not absolute, nor does it operate in isolation. It is a right that, by its nature, requires a careful balancing of interests. Personal data may be processed where there is a valid lawful basis and where the relevant conditions, safeguards and principles are respected.

This balance is particularly important in the context of scientific research, which is guaranteed to be free by fundamental rights at the EU level and in many member states. The protection of research participants is essential, but it must be considered alongside the substantial public interest in enabling scientific progress, innovation and discovery. Scientific research contributes to knowledge, public health and the development of methods to diagnose, prevent and treat debilitating diseases and disorders. However, the value of scientific research cannot always be easily quantified. The cost of not using or sharing data responsibly should therefore also be recognised: less data means less research, fewer discoveries and reduced capacity to address serious societal challenges.

Accordingly, the appropriate balance must be struck. Data protection is a fundamental right, but it is not the only right at stake. The rights to privacy and to the protection of personal data may be subject to limitations where those limitations are provided for by law, pursue a legitimate public interest, and are necessary and proportionate in a democratic society. In this context, the regulatory framework should ensure robust protection for individuals while also enabling, rather than obstructing or unduly stifling, scientific research carried out in the public interest.

1. The concept of scientific research

We recognise that controllers and supervisory authorities require sufficient guidance to determine whether processing is genuinely undertaken for scientific research purposes under the GDPR. However, the EDPB should resist extending this task into a general definition of scientific research.

The factors set out in paragraph 11 are presented as indicators for determining whether processing is motivated by scientific research purposes. Several of them, however, concern the character and merit of the underlying research itself, including its methods, ethical framework, modes of review, qualifications of the researchers, anticipated societal benefits, and contributions to knowledge. Applied broadly, these factors risk becoming criteria by which regulators, legislators or research infrastructures determine whether a study, method or field is sufficiently scientific.

This approach may interfere with the freedom of scientific research protected by Article 13 of the Charter and the defence rights of science against state intervention, as defined by member states, e.g., in the German constitution (Article 5(3)) or the French constitution (Conseil constitutionnel, 83-165 DC of 20 January 1984). Scientific methods, publication practices, and evaluation standards vary considerably across disciplines. Exploratory, qualitative, interdisciplinary, citizen-led and emerging forms of research may not satisfy conventional indicators concerning systematicity, peer review, qualifications or foreseeable social benefit, while remaining legitimate scientific activity. Research-enabling infrastructures such as biobanks, research repositories and shared data platforms may also be adversely affected if the indicators are applied too rigidly.

Particular caution is required regarding anticipated societal well-being. The value of fundamental or curiosity-driven research may not be foreseeable when the work is undertaken. Scientific freedom includes the ability to pursue questions whose relevance is uncertain, whose results may challenge prevailing policy, or whose contribution becomes apparent only through later research.

The final Guidelines should therefore minimise, or better yet refrain from, the use of substantive criteria defining scientific research. To protect freedom of scientific research, negotiations over what is considered scientific must be left to the scientific community's critical assessment, with its dynamically evolving approaches and criteria. This is the basis of scientific progress and innovation. Any indicators should be expressly limited to determining whether the relevant processing is genuinely connected with a scientific research purpose under the GDPR. They should be non-exhaustive, non-cumulative and interpreted by reference to the standards of the relevant research field.

2. Purpose limitation and further processing

2.1 Presumption of compatibility and continuing lawfulness

Paragraphs 19 to 23 distinguish between the presumption of compatibility under Article 5(1)(b) GDPR and the requirement that further processing remain lawful under Articles 5(1)(a) and 6 GDPR. We agree that compatibility and lawfulness are distinct requirements. However, the treatment of the original legal basis risks substantially limiting the practical effect of Recital 50.

Recital 50 states that, where further processing is compatible with the initial purpose, no separate legal basis from that which permitted the original collection is required. The Guidelines do not explain what is added by the suitability assessment once compatibility has been presumed. Therefore, such double evaluations should be avoided as they produce enormous overheads in already heavily challenged infrastructures.

2.2 Provision of data to another controller

Paragraph 26 usefully confirms that neither the providing controller nor the receiving controller is required to undertake an Article 6(4) compatibility assessment where data are provided for scientific research purposes. It also confirms that each controller must identify an appropriate Article 6 basis and, where applicable, an Article 9 condition.

Further operational guidance is nevertheless required for the providing controller. Disclosure or provision of data is itself a processing operation. A hospital, public authority or other data holder must therefore determine the legal basis on which it may make data available to an independent research controller.

This issue commonly arises where clinical information was originally processed on the basis of contractual necessity, vital interests, a legal obligation or consent relating to treatment. The receiving research institution may have a clear basis for its subsequent research processing, while the hospital remains uncertain whether and on what basis it may disclose the data.

The final Guidelines should include examples addressing:

- disclosure by a healthcare provider to a university or research infrastructure;
- disclosure of legacy data collected before a research project was contemplated;
- disclosure where the original consent did not include external research;
- disclosure under a statutory public-interest or research power;
- disclosure of pseudonymised data through an intermediary or trusted third party; and
- remote access arrangements that do not involve the transfer of a local copy.

The Guidelines should also clarify that re-contacting patients is not the only available mechanism. Seeking new consent during acute, traumatic or highly sensitive treatment may be inappropriate and may place additional burdens on patients. Where another lawful basis and Article 9 condition are available, the GDPR should not be interpreted as requiring consent solely because it appears administratively familiar.

2.3 Storage limitation

We welcome the recognition that personal data may need to be retained following the completion of a research project for verification, peer review, scientific scrutiny and reproducibility.

The final Guidelines should provide further guidance on the criteria that may justify retention after active analysis has ended. Relevant considerations may include:

- disciplinary standards concerning research record retention;
- contractual or grant obligations;
- the period during which research findings may reasonably be audited or challenged;
- the need to investigate research misconduct;
- requirements imposed by publishers, regulators or clinical-trial legislation;
- the feasibility of retaining a reduced or pseudonymised dataset for data reuse and sharing; and
- the possibility of retaining an analysis-locked version while deleting unnecessary working copies.

Fixed retention periods will not be appropriate for every field.

3. Consent under the GDPR

3.1 GDPR consent and consent to participate in research

We welcome the distinction in paragraphs 53 and 54 between consent as a GDPR legal basis and consent to participate in research arising from ethical or other legal requirements.

This distinction should be maintained consistently throughout the Guidelines, including the executive summary and examples. We recommend using the following terminology:

- consent as a legal basis under Article 6(1)(a) GDPR;
- explicit consent under Article 9(2)(a) GDPR; and
- ethical consent to participate in research.

The simple term “consent” should be avoided since it will be unclear which of the above three types of “consent” is intended. The first two types of consent, in our opinion, can reasonably be categorised as “GDPR consent”, while the last may be termed “ethical consent.”

Where processing relies on tasks carried out in the public interest (Article 6(1)(e)) together with the scientific research exemption (Article 9(2)(j)), ethical consent will operate as an ethical or organisational safeguard, but will not be the legal basis for processing. In that setting, the validity and scope of the ethical consent should be assessed in accordance with the applicable ethical and

sectoral frameworks, while the lawfulness of data processing should be assessed separately under the GDPR.

This distinction is important because withdrawal from participation, withdrawal of GDPR consent and exercise of a data subject right may have different legal consequences.

3.2 Documenting the boundaries of broad GDPR consent

Paragraph 46 requires the controller to consider, before an individual project begins, whether the proposed processing remains within the boundaries of the broad GDPR consent. This is a reasonable accountability requirement, but the Guidelines do not specify how the assessment should be undertaken or documented.

The final Guidelines should indicate whether the assessment may form part of an existing research protocol, data-access application, ethics submission or data-management plan. A separate, extensive legal assessment for every use of a research database would be disproportionate, particularly for student projects and small investigator-led studies.

A proportionate record could identify:

- the area of research covered by the original consent;
- the relationship between the proposed project and that research area;
- the reasonable expectations communicated to participants;
- any material change in risks, recipients or methods;
- the safeguards applied; and
- the person or body responsible for approving access.

Templates or worked examples would reduce inconsistent interpretations between institutions and Member States.

It should be noted that while such an assessment could be mandated for GDPR consent, it should not be mandated for ethical consent, which is considered a safeguard under the GDPR. In the latter case, the requirements governing the boundaries of the ethical consent should be within the remit of ethics committees.

3.3 Information concerning new projects

Paragraph 48 recommends that detailed information be made available as research progresses and suggests mechanisms such as webpages or subscription-based updates. While we support transparency, attempts to turn broad consent into dynamic consent should be resisted, as they pose additional, disproportionate burdens on researchers who have decided to obtain broad consent and on participants who are willing to give it. The final Guidelines should clarify that no universal waiting period is required between publication of information about a project and commencement of processing. The appropriate period should depend on the nature of the processing, the risks involved, the expectations created by the original information and the practical ability of data subjects to exercise their rights.

The Guidelines should also distinguish clearly between:

- withdrawal of consent;
- an objection under Article 21 GDPR;
- a request for erasure under Article 17 GDPR; and
- withdrawal from participation under research ethics rules.

Withdrawal of GDPR consent does not retrospectively invalidate processing that was lawful before withdrawal. Nor does it automatically require the retraction of published findings or the recomputation of anonymous aggregate results. Continued processing or retention of identifiable or pseudonymised data must, however, have an appropriate legal basis or fall within an applicable exception.

Where data have been disclosed to another controller, the originating controller should not be expected to guarantee another independent controller's compliance, but it should take reasonable steps within the parties' respective responsibilities and contractual arrangements.

The final Guidelines should also recognise the recurring administrative and financial costs associated with maintaining project registers, updating public information, operating participant-notification systems and coordinating data subject requests across successive research projects. These requirements may be manageable for large research infrastructures but disproportionately burdensome for smaller institutions, student projects and investigator-led research.

3.4 Independent oversight and proportionality

Paragraph 49 presents independent data trustees, time-limited consent and oversight bodies as possible safeguards. It recognises that an existing ethics committee may provide sufficient oversight.

The final Guidelines should state more clearly that an independent trustee or new oversight body is not required with broad consent. The appropriate governance arrangement should reflect the scale, risk and institutional setting of the processing.

Where an oversight body is considered necessary, the Guidelines should address:

- whether it may be internal to the institution while remaining functionally independent;
- whether an existing ethics committee or data-access committee may perform the role;
- the expertise and representation that may be required;
- proportionate procedures and response times;
- management of conflicts of interest; and
- circumstances in which review may be expedited or delegated.

Without such guidance, institutions may establish duplicative committees with uncertain authority. This would impose disproportionate delays on smaller projects without necessarily improving the protection of participants. The cumulative effect may also increase consumption of limited resources and widen existing disparities between institutions and Member States with different levels of funding, infrastructure and access to specialist legal and governance support.

4. Special categories of personal data

4.1 The scope of special-category data and inferred information

Paragraph 64 states that Article 9 includes data that can be collated or used to deduce special-category information, as well as information inferred from other data. We recognise that this reflects the broad interpretation adopted in the case law of the Court of Justice.

The final Guidelines should nevertheless provide a workable threshold for determining when ordinary personal data become data revealing an Article 9 characteristic. A purely theoretical possibility that data could contribute to a sensitive inference should not, without further consideration, cause every dataset to be treated as special-category data.

The assessment should consider:

- the purpose for which the data are processed;
- the methods actually applied or reasonably contemplated;
- the nature and reliability of the inference;
- whether the data are labelled or organised by reference to an Article 9 characteristic;
- the availability of auxiliary information;
- the context in which the data were collected; and
- the objective likelihood that the processing will reveal special-category information.

For example, digital handwriting may be collected for linguistic or educational research. The fact that handwriting features can also contribute to research on neurological disease (e.g. Parkinson's disease) should not automatically convert every handwriting dataset into health data. Article 9 would more clearly apply where handwriting is processed to detect, predict or investigate a health condition.

Neuroimaging follows a similar logic. Structural or functional MRI data are commonly collected from healthy volunteers; such data need not necessarily be categorised as a special category unless health-related research is envisaged to be carried out. In the same way, MRI scans do not become special-category biometric data solely because anatomical structures may assist identification. The biometric element of Article 9 applies where biometric data are processed for the purpose of uniquely identifying a natural person.

Examples addressing medical imaging, voice recordings, movement data, and behavioural measurements would materially improve legal certainty.

4.2 Data manifestly made public and third-party information

The high threshold applied to Article 9(2)(e) is appropriate. Data should not be treated as manifestly public unless the data subject intentionally made the relevant information accessible to the general public through a clear affirmative act.

A practical problem arises where researchers collect public online material that contains special-category data about third parties. An individual may, for example, post information about another person's health, political opinions, or private life. The third party has not manifestly made that information public.

Researchers cannot always identify and remove such material without first collecting and inspecting it. Collection, inspection and deletion are themselves processing operations. The final Guidelines should therefore address lawful and proportionate triage procedures for public-source research.

Such procedures might include:

- automated or manual screening within a segregated environment;
- strict access limitations;
- prohibition of substantive analysis before screening;
- immediate deletion or quarantine of material outside the lawful scope;
- documentation of the applicable Article 6 basis and Article 9 condition;
- short retention periods for quarantined material; and
- review of unavoidable residual inclusion in large datasets.

The Guidelines should not suggest that technical screening falls outside the GDPR, but should explain how controllers can minimise unavoidable processing while removing unlawfully or unnecessarily collected information.

4.3 National and Union law

We welcome the recognition that Union or Member State law may provide Article 9 derogations and may impose additional conditions on genetic, biometric and health data.

This area remains a major source of fragmentation. A research consortium may be able to rely on Article 9(2)(j) or on explicit consent in one Member State, but may encounter additional licensing, approval, or statutory requirements in another.

The final Guidelines should provide a framework for identifying the applicable national provisions in cross-border research. It should address:

- the relevance of the establishment of each controller;
- the location at which processing occurs;
- the law governing the data-holding institution;

- the consequences of divergent national conditions;
- allocation of responsibility for legal due diligence; and
- documentation of national restrictions within joint-controller or data-sharing arrangements.

The Guidelines should also acknowledge that Article 9(2)(a) permits Union or Member State law to provide that the Article 9 prohibition cannot be lifted by consent. The practical question is how an international consortium should identify and implement such restrictions consistently. This is especially important if the member state does not have an implementing law for the scientific exemption article 9(2)(j).

5. Transparency and the obligation to inform

5.1 Transparency, data minimisation and security

Paragraphs 86 to 89 address circumstances in which a controller has not retained contact details or did not originally anticipate further research. We recognise the importance of enabling data subjects to remain informed. However, the final Guidelines should more directly address the tension between active transparency, data minimisation and information security.

Retaining names, email addresses, telephone numbers or correspondence tables solely to support future notifications may significantly increase the consequences of a data breach. Research datasets such as brain MRI images may be extremely difficult to associate with an identified person when held independently. Maintaining a direct link between the research dataset and a current contact database may substantially reduce that protection.

The controller should therefore undertake a documented comparison between:

- the benefit of direct individual communication;
- the likelihood and significance of future changes;
- the risks created by retaining identifiers and contact details;
- the availability of indirect transparency measures;
- the ability of data subjects to initiate contact;
- the expected duration of the research infrastructure; and
- the effectiveness of separation, encryption and trusted-intermediary arrangements.

The Guidelines should not be interpreted as creating a general obligation to retain contact details where they are not otherwise necessary.

5.2 Active and passive transparency

The final Guidelines should recognise a range of proportionate transparency mechanisms. Direct email, telephone, or dashboard notifications should not necessarily be the default for every new project within a previously described research area, and planned research projects should not necessarily be made available to the broader public.

Central public or access-limited portals can provide continuing transparency without maintaining direct contact links within each research database. Such portals may describe:

- active and planned research projects;
- categories of data used;
- participating institutions;
- applicable safeguards;
- publication of results;
- procedures for exercising rights; and
- contact details for the relevant controller or intermediary.

Participants could be offered an optional subscription service without requiring the research platform itself to retain contact information for everyone.

A risk-based hierarchy would be preferable:

1. direct notification where required by Articles 13 or 14 or justified by a material change;
2. optional subscription-based updates where continuing engagement is beneficial;
3. public or layered information where direct contact is unnecessary, disproportionate or security-reducing; and
4. use of Article 14(5)(b), subject to its conditions and appropriate safeguards.

6. Data subjects' rights

6.1 Erasure and backup systems

The Guidelines should address the operation of Article 17 in contemporary backup architectures. Enterprise backups are frequently immutable, encrypted and organised as system-wide snapshots. Selective alteration may be technically difficult, may compromise the integrity of the backup or may make reliable restoration impossible.

This does not remove the controller's obligations under Article 17. It does, however, require guidance on what constitutes erasure without undue delay in systems where immediate record-level deletion is not technically feasible.

The final Guidelines should address practices such as:

- deletion from live and routinely accessible systems;
- restriction of access to backup copies;
- short and documented backup-retention cycles;
- suppression lists preventing erased records from being restored into active processing;
- automatic re-deletion following restoration;
- deletion or destruction of encryption keys where appropriate;
- replacement or removal of identifiers within technically modifiable backups; and
- documentation explaining why direct modification would undermine backup integrity.

The EDPB should also clarify when temporary residual presence in an inaccessible backup is compatible with Article 17, provided that the data are not used for any other purpose and are removed through an established retention cycle.

6.2 Scientific reproducibility and integrity

The application of Article 17(3)(d) should remain case-specific. Nevertheless, the final Guidelines should recognise that erasure from an analysis-locked or published dataset may impair scientific objectives and reproducibility even where the immediate study can technically continue.

Research data often need to remain stable to permit:

- independent verification of statistical results;
- investigation of alleged errors or misconduct;
- regulatory or sponsor audits;
- replication of published analyses;
- examination of adverse events;
- correction of the scientific record; and
- compliance with disciplinary retention standards.

Removal of an individual record will change derived statistics, model parameters, confidence intervals or quality-control outputs. In some fields, it may also prevent exact reproduction of the published analysis.

The Guidelines should provide examples of when those consequences may constitute serious impairment. They should also encourage controllers to consider less intrusive measures before refusing erasure, including restricting processing, removing from future analyses, separating identifiers, implementing access controls, and retaining a locked archival copy.

The publication of a study should not automatically create a permanent exemption from erasure. Equally, a withdrawal or erasure request should not be assumed to require retraction of an article or modification of anonymous aggregate results. The status of the data, the applicable legal basis, the stage of the research and the impact of deletion must be considered separately.

7. Appropriate safeguards under Article 89(1)

7.1 Secure processing environments

Secure processing environments can provide strong safeguards for high-risk data, particularly where researchers require access to detailed personal data but do not require local copies. They cannot and should not, however, be treated as the presumptive solution for all research processing.

Scientific computing frequently depends on specialised local hardware, distributed computing clusters, rapidly changing software environments and collaboration across institutions. A central environment may be unable to support the necessary tools, computational scale or reproducibility requirements. It may also create substantial costs and delays for smaller institutions. The required data and standardised processing procedures to execute analyses may not exist to support new and innovative investigations.

The final Guidelines should state expressly that the selection of safeguards is risk-based and technologically neutral. Relevant alternatives may include:

- federated analysis;
- controlled export of appropriately pseudonymised data;
- remote execution of approved code;
- encrypted computation;
- confidential computing;
- contractual restrictions on re-identification;
- monitored local environments;
- output checking;
- trusted research environments; and
- combinations of these measures.

Where local export is permitted, the controller should assess the recipient's realistic means of identification, the data characteristics, the research purpose, the security controls, and the consequences of unauthorised disclosure.

Article 13 of the Charter protects freedom of scientific research and academic freedom. This supports a proportionate approach, which avoids imposing a single infrastructure model where other, effective safeguards are available.

7.2 Pseudonymisation and the exercise of rights

Paragraph 163 appropriately requires arrangements that enable data subjects to exercise their rights in relation to pseudonymised data. The Guidelines should, however, avoid creating an assumption that every recipient must possess the information needed to re-identify participants.

A safer arrangement is often for the originating controller or a trusted intermediary to retain the re-identification capacity and act on verified requests. The data recipient may then locate, restrict or delete the relevant pseudonymised record without learning the person's identity.

The final Guidelines should compare models, including:

- central management of requests by the originating controller;
- trusted-third-party pseudonymisation;
- participant-held codes;
- controller-generated pseudonyms supplied to participants;

- privacy-preserving record matching;
- separate contact and research domains; and
- mediated requests in which the research controller receives only the minimum information necessary to act.

The objective should be the effective exercise of rights with the least possible distribution of identifying information. It should also consider the possibility that data received by a new controller may have been attributed new ID codes through processing (e.g. consecutive numeric codes for standardised data representations or as an additional safeguard) that may not link to the initial data.

7.3 Cryptographic and privacy-enhancing techniques

The list of privacy-enhancing technologies in section 8.5 should be expanded. Homomorphic encryption and synthetic data are useful examples, but other techniques may be more accessible to ordinary research institutions.

The final Guidelines should discuss, at an appropriate level:

- keyed hashing and message authentication codes;
- tokenisation;
- secure multiparty computation;
- private set intersection;
- confidential computing;
- differential privacy;
- privacy-preserving record linkage;
- distributed or federated learning; and
- controlled destruction of cryptographic keys.

Properly designed privacy-preserving matching allows a repository to verify and act upon a request without maintaining a directly readable contact table. The Guidelines should encourage the assessment of such architectures that reduce the risk of unauthorised outward identification while preserving the practical exercise of rights.

The Guidelines should also clarify that biometric data fall within the Article 9 biometric category when they result from specific technical processing and are used to uniquely identify a person. Data may still fall within another Article 9 category, particularly health data, even where the biometric-identification condition is not satisfied.

8. International transfers and cross-border research

The Guidelines refer briefly to Chapter V GDPR but do not provide substantive guidance tailored to scientific research. International transfers are central to contemporary research, including multinational clinical studies, global disease registries, distributed imaging projects, studies that require building models from large and distributed datasets (e.g. foundation AI models) and collaborations involving specialist computational facilities.

The final Guidelines should include a dedicated section addressing:

- use of standard contractual clauses in multi-party projects;
- supplementary measures for pseudonymised health, genetic and biometric data;
- remote access from a third country;
- international use of cloud and high-performance computing services;
- onward transfers between research partners;
- changes in consortium membership;
- emergency and public-health research; and
- interaction with participant information and broad consent.

The final Guidelines should also recognise that compliance with Chapter V does not resolve differences between national / regional laws governing access to health, genetic or biometric data.

Consortia require a documented process for identifying those restrictions and determining which partner may make data available, under which conditions and through which technical arrangement.

9. Recommendations

We recommend that the final Guidelines:

1. refrain from attempts to define what scientific research is or is not.
2. explain what is added by the suitability assessment once compatibility has been presumed;
3. provide practical examples concerning disclosure by a clinical or public-sector controller to an independent research controller;
4. establish proportionate documentation expectations for determining whether a project falls within broad GDPR consent;
5. distinguish consistently between GDPR consent, and ethical consent to participate in research. The EDPB should not seek to dictate the boundaries of ethical consent as this should remain the domain of ethics committees;
6. clarify where an oversight body is considered necessary.
7. clarify the threshold at which ordinary data used to infer an Article 9 characteristic become special-category data;
8. provide examples involving medical imaging, behavioural data, and other scientifically common data types;
9. address strictly limited screening of public-source datasets containing third-party special-category information;
10. reconcile continuing transparency with data minimisation and the security risks of retaining contact links;
11. provide practical guidance on erasure in immutable or snapshot-based backup systems;
12. recognise reproducibility, auditability and research-integrity requirements when applying Article 17(3)(d);
13. confirm that secure processing environments are one possible safeguard rather than a universal infrastructure requirement;
14. promote mediated and privacy-preserving mechanisms for exercising rights in pseudonymised datasets;
15. expand the treatment of privacy-enhancing technologies and explain the limitations of ordinary hashing; and
16. include substantive guidance on Chapter V transfers and cross-border research consortia.

These clarifications would improve legal certainty while preserving the risk-based and proportionate character of the GDPR. They would also reduce inconsistent implementation between Member States and between institutions with substantially different levels of technical and financial capacity.

Co-signatories

By adding my name, I support the feedback provided in the document. My signature reflects my personal support and does not engage my institution.

Date	Name	Surname	Affiliation
6/21/2026	**Chneiweiss**	**Hervé**	**INSERM (France)**
6/21/2026	**Paola**	**Galdi**	**Cancer Research UK Scotland Institute**
6/21/2026	**Jordi**	**Solé-Casals**	**University of Vic-Central University of Catalonia**
6/21/2026	**Alessio**	**Giacomel**	**University Hospital Frankfurt am Main**

6/21/2026	**Anđela**	**Šoškić**	**University of Belgrade**
6/21/2026	**Marco**	**Aiello**	**IRCCS SYNLAB SDN (Naples, Italy)**
6/21/2026	**DANISIA**	**HABA**	**UNIVERSITY GRIGORE T POPA IASI, ROMANIA**
6/21/2026	**Thirion**	**Bertrand**	**Inria, France**
6/21/2026	**Marcin**	**Koculak**	**Jagiellonian University (Kraków, Poland)**
6/21/2026	**Mahnaz**	**Arvaneh**	**University of Sheffield (Sheffield, UK)**
6/22/2026	**Vlastimil**	**Koudelka**	**National Institute of Mental Health in CZ**
6/22/2026	**Robert**	**Oostenveld**	**Radboud University Nijmegen, NL**
6/22/2026	**Karam**	**Sidaros**	**Copenhagen University Hospital Hvidovre, DK**
6/22/2026	**Camille**	**Pescatore**	**ETH Zurich, CH**
6/22/2026	**Javier**	**Marta-Moreno**	**Hospital Univ. M. Servet- IIS Aragón (Spain)**
6/22/2026	**Gaëlle**	**Leroux**	**CNRS, France**
6/22/2026	**Burçin**	**Kurt**	**Karadeniz Technical University (Trabzon, Türkiye)**
6/22/26	**Nils**	**Muhlert**	**University of Manchester, UK**
6/22/2026	**Katarzyna**	**Hat**	**Jagiellonian University, Poland**
6/22/2026	**Jan**	**Fousek**	**Masaryk University (Brno, Czech Republic)**
6/222026	**Edvin**	**Zukic**	**Universität Salzburg**
6/22/2026	**Thomas E.**	**Nichols**	**University of Oxford**
6/22/2026	**Rafael**	**Romero García**	**Universidad de Sevilla**
6/22/2026	**Keith George**	**Ciantar**	**Institute of Neuroscience and Medicine (INM-4), Research Centre Juelich (FZJ)**
6/23/2026	**Camille**	**Maumet**	**INRIA, Rennes, France**
6/23/2026	**Kenneth**	**Scerri**	**University of Malta**
6/23/2026	**Francesca B**	**Pizzini**	**Università degli Studi di Verona**
6/23/2026	**Dr. Judy**	**Illes, OC, PhD, FRSC, FCAHS**	**University of British Columbia**
6/23/2026	**Felix**	**Putze**	**University of Bremen**
6/23/2026	**Melanie**	**Ganz-Benjaminsen**	**University of Copenhagen, Denmark**
6/23/2026	**Esin Öztürk Işık**	**Bogazici**	**University, Istanbul, Turkiye**
6/23/2026	**Ioannis**	**Revolidis**	**University of Malta**
6/23/2026	**Alexandros**	**Karakasidis**	**a.karakasidis@uom.edu.gr**
6/23/2026	**Gaëlle**	**LEROUX**	**CNRS, France**
6/23/2026	**Michaela**	**Vanharova**	**Masaryk university**
6/23/2026	**Michal**	**Mikl**	**Masaryk University**
6/23/2026	**Luis**	**Garcia-Larrea**	**INSERM - Institut National de la Santé et la Recherche Médicale**
6/23/2026	**Klaus**	**Eickel**	**Bremerhaven University of Applied Sciences**

6/23/2026	**Maria**	**Dech Pons**	**Fraunhofer Institut für Digitale Medizin, MEVIS, Bremen**
6/23/2026	**Eike**	**Petersen**	**Fraunhofer Institute for Digital Medicine MEVIS**
6/23/2026	**Jovana**	**Bjekic**	**Institute for medical research, University of Belgrade, Serbia**
6/23/2026	**Arno**	**Rossez**	**Forschungszentrum Jülich GmbH**
6/23/2026	**Michał**	**Wierzchoń**	**Centre for Brain Research, Jagiellonian University, Krakow, Poland**
6/23/2026	**Jochen**	**Hirsch Fraunhofer**	**Institute for Digital Medicine MEVIS Bremen**
6/23/2026	**Markus**	**WenzelConstructor**	**University Bremen, Germany**
6/23/2026	**Volker**	**Dicken Fraunhofer**	**MEVIS**
6/24/2026	**Faisal**	**Mushtaq**	**University of Leeds, UK**
6/24/2026	**Yuri**	**Pavlov**	**University of Alabama at Birmingham, USA**
6/24/2026	**Alexandra**	**Bendixen**	**Chemnitz University of Technology**
6/24/2026	**Manish**	**Mohapatra**	**Christ University**
6/24/2026	**Artur**	**Czeszumski**	**University of Warsaw**
6/24/2026	**Heinrich R.**	**Liesefeld**	**University of Bremen, Germany**
6/24/2026	**Gabriela M.**	**Marcu Lucian**	**Blaga University of Sibiu**
6/24/2026	**Franz**	**Wurm**	**Leiden University; Leiden Institute for Brain and Cognition**
6/24/2026	**Mikkel C.**	**Vlnding**	**University of Copenhagen**
6/24/2026	**Natasha**	**Padfield**	**University of Malta**
6/24/2026	**Bernard A J**	**Jap**	**Hong Kong Metropolitan University**
6/24/2026	**Magdalena**	**Senderecka**	**Jagiellonian University in Cracow, Poland**
6/24/2026	**Oscar**	**Esteban**	**University of Applied Sciences and Arts Western Switzerland**
6/24/2026	**Marco**	**Castellaro**	**Department of Information Engineering, University of Padova, Italy**
6/24/2026	**Xhilda**	**Dhamo**	**University of Tirana**
6/24/2026	**Charis**	**Styliadis**	**Aristotle University of Thessaloniki**
6/24/2026	**Marco**	**Aiello**	**IRCCS SYNLAB SDN, Naples, Italy**
6/24/2026	**Xun**	**He**	**Bournemouth University**
6/24/2026	**Marcin**	**Koculak**	**Jagiellonian University (Kraków, Poland)**
6/24/2026	**Artan**	**Berisha**	**University of Prishtina**
6/24/2026	**Roxanne**	**Meilak Borg**	**University of Malta**
6/24/2026	**Behar**	**Baxhaku**	**University of Prishtina**

6/24/2026	**Christophe**	**PHILLIPS**	**University of Liège, Belgium**
6/24/2026	**Michal**	**Bola**	**Jagiellonian University**
6/24/2026	**Alexandra**	**Reichenbach**	**Heilbronn University**
6/24/2026	**Anne-Sophie**	**Dubarry**	**CNRS**
6/24/2026	**Vojislav**	**Jovanović**	**University of Belgrade**
6/24/2026	**Ioana Roxana**	**Podina**	**University of Bucharest, Mindcare for all Association**
6/24/2026	**Sandra**	**Carvalho**	**School of Psychology, University of Minho**
6/24/2026	**Marie-Constance**	**Corsi**	**Paris Brain Institute**
6/24/2026	**Urban**	**Marhl**	**Institute of Mathematics, Physics and Mechanics**
6/24/2026	**Arzu**	**Kursun**	**Giresun University**
6/24/2026	**Corneyllie**	**Alexandra**	**CNRS**
6/24/2026	**Patrica**	**Clement**	**Ghent University**
6/24/2026	**Ladouce**	**Simon**	**University of Cambridge**
6/24/2026	**Roman**	**Mähler**	**Heilbronn University**
6/24/2026	**Dr. Lyuba**	**Zehl**	**EBRAINS AISBL**
6/24/2026	**Maria J**	**MORA CORRAL**	**University of Malta**
6/24/2026	**Christos**	**Tsouras**	**General Hospital of Lefkada**
6/24/2026	**Esra kınacı biber**		**Düzce university, Turkiye**
6/24/2026	**Asier**	**Erramuzpe**	**Biobizkaia Health Research Institute**
6/24/2026	**Buot**	**Anne**	**GHU Paris Psychiatrie et Neurosciences**
6/24/2026	**Soetkin**	**Beun**	**Ghent University**
6/24/2026	**Mateusz**	**Pawlik**	**University of Salzburg/Austrian NeuroCloud**
6/24/2026	**Christoph**	**Brachmann**	**Fraunhofer MEVIS**
6/24/2026	**Petr Dusek**		**Charles University, Prague, Czechia**
6/24/2026	**Maximilien**	**Chaumon**	**CNRS - Paris Brain Institute**
6/24/2026	**Jean-Gabriel**	**Ganascia**	**Sorbonne University**
6/24/2026	**Patrick Brunner**		**FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur**
6/24/2026	**Markos**	**Apostolakis**	**University of Cyprus**
6/24/2026	**Malgorzata**	**Wierzba**	**Nencki Institute of Experimental Biology, Polish Academy of Sciences, Warsaw, Poland**
6/24/2026	**Anna**	**Plachti**	**Leibniz Research Centre for Working Environment and Human Factors (IfADo) at the Technical University of Dortmund**
6/24/2026	**Simon**	**Steinkamp**	**Danish Research Centre for Magnetic Resonance, Department of Radiology and Nuclear Medicine, Copenhagen University Hospital - Amager and Hvidovre, Copenhagen, Denmark**

6/24/2026	**Alina**	**Duca**	**Faculty of Computer Science, „Alexandru Ioan Cuza” University**
6/24/2026	**Milica**	**Janković**	**University of Belgrade - School of Electrical Engineering**
6/25/2026	**Pelin**	**Ismailoglu**	**Recep Tayyip Erdogan University (Turkey)**
6/25/2026	**Granville**	**Matheson**	**Uppsala University**
6/25/2026	**Paul**	**Bezzina**	**University of Malta**
6/25/2026	**Timo**	**Lehmann Kvamme**	**University of Oxford**
6/25/2026	**Patrick**	**Baracho Dittrich**	**Hochschule Heilbronn**
6/25/2026	**Christine**	**Farrugia**	**The University of Edinburgh**
6/25/2026	**Yasmin**	**Hollenbenders**	**Heilbronn University**
6/25/2026	**Clément**	**FRANÇOIS**	**CNRS**