Comments on EDPB Guidelines 1/2026

on the processing of personal data for scientific research purposes

Contribution to the public consultation

(Guidelines adopted on 15 April 2026, public consultation version)

Introduction

This document gathers observations on the Guidelines 1/2026 of the European Data Protection Board (EDPB) on the processing of personal data for scientific research purposes, submitted by certain members of the working groups engaged, in Italy, in the redrafting of the rules of professional conduct (regole deontologiche) on the processing of personal data for statistical and scientific research purposes — a process initiated following the measure of the Italian Data Protection Authority (Garante): decision no. 298 of 9 May 2024, "Rules of professional conduct for processing for statistical or scientific research purposes pursuant to Articles 2-quater and 106 of the Italian Personal Data Protection Code (Codice Privacy)".

The observations stem from the experience gained in that context and are signed by the individual signatories, each in their own area of expertise and affiliation.

The document is organised by blocks of paragraphs of the Guidelines. For each block, it sets out the topic and the relevant paragraphs, a summary of what the text states, an assessment of its significance, the reformulated comment intended for the EDPB and, where possible, a concrete proposal for amendment or an example. Textual quotations are taken from the English version of the Guidelines; the comments were drafted in Italian and translated into English for the purpose of submission.

1. Compatibility test (§§ 17, 19–23)

Paragraph 17 distinguishes three situations: (a) scientific research as the primary purpose; (b) further processing for another research purpose not covered by the primary purpose, qualified as "further processing for another purpose"; (c) further processing for research purposes of data originally collected for non-scientific purposes.

Paragraph 19 provides that, for further processing for scientific research purposes, the presumption of compatibility under Article 5(1)(b) GDPR applies and the test under Article 6(4) is not required. Paragraph 20 reproduces Recital 50. Paragraphs 21–22 distinguish compatibility of purposes from lawfulness: the initial legal basis may be reused, but not always — in particular, it is "not always possible to rely on the same legal basis" where the initial basis is consent or a legal obligation.

Paragraph 23 attaches significant weight to the societal value of research in the balancing exercise under Article 6(1)(f).

Assessment

Two comments arise in relation to the paragraphs above:

– the combined reading of § 17 and § 19 does indeed give rise to ambiguity. Paragraph 17 qualifies the transition "research A → research B not covered by the primary purpose" as "further processing for another purpose" — an expression which, unlike "further processing for another research purpose", suggests a different purpose, one that is "other" than scientific research. As a result, the reader might infer exclusion from the presumption of compatibility (since the presumption is framed for "further processing for scientific research purposes"). In reality, research B is still research, and the presumption therefore

applies; but this is not made explicit. Paragraph 19 clarifies, a contrario, only the opposite case (research → non-research), leaving the intermediate case (research A → research B) to the reader's interpretation.

– footnote 35 to § 22 clarifies that, where the initial legal basis was consent, a new consent must be obtained or another suitable legal basis identified. But this appears in a footnote: the body of § 22 states only that it is "not always possible" to reuse the initial basis, leaving the reader without operational guidance.

For those who have practised in this field since before the GDPR — when consent was regarded as the default basis — the most natural reading of the body of § 22 is the restrictive one rightly flagged in the comment.

Suggestions for the EDPB

Section 3.1.1 should draw a clearer distinction, in the body of the text and not only in a footnote, between two aspects that the Guidelines deliberately keep separate but that readers continue to conflate:

(a) the presumption of compatibility of purposes (Article 5(1)(b)); and

(b) the assessment of lawfulness (Article 6(1)).

In particular, it should be made explicit that the presumption of compatibility also applies in the "research A → research B not covered by the primary purpose" scenario (that is, the situation described in § 17 as "further processing for another purpose"), while the question of the legal basis remains a separate matter. It should also be made explicit in the body of § 22 — and not only in a footnote — what the operational outcome is where the initial basis is consent, given the enormous practical impact on data already collected in the past on the basis of consent (a typical situation for pre-GDPR clinical research and biobanks).

2. Disclosure of data to another controller (§ 26)

Paragraph 26 governs the disclosure of personal data between controllers, in the scenario where controller B intends to process the data received from controller A for its own scientific research purposes. The provision is clear in stating two things: (a) the disclosure constitutes further processing only if it was not one of the primary purposes at the time of collection; (b) neither A nor B is required to carry out the compatibility test under Article 6(4) GDPR. Footnote 40 recalls that both must nonetheless comply with all other obligations under the Regulation, in particular identifying an autonomous legal basis under Article 6(1) and, where applicable, a derogation under Article 9(2).

Assessment

The text of § 26 is clear as to what it states, but it confines its scope to two aspects only — the qualification of the disclosure as further processing and the exemption from the compatibility test — without expressly addressing the overall framework within which the disclosure sits. A reader looking to § 26 for a complete set of rules on disclosure between controllers in scientific research must reconstruct it by cross-referencing § 26 with other paragraphs of the Guidelines, located in different sections and not referred to in § 26 itself.

Three connections, in particular, seem to us necessary to give § 26 full operational effect.

First connection — with §§ 21–22 on the legal basis for further processing. Paragraph 26 merely establishes that a disclosure not envisaged at the time of collection is further processing, and that the compatibility test is not required. It does not, however, clarify whether and to what extent the legal basis of the initial processing automatically extends to the disclosure. Paragraphs 21–22 address this point in general terms for any further processing for research purposes, distinguishing compatibility (presumed) from lawfulness (to be verified autonomously) and flagging, in particular, the difficulties that arise where the initial basis was consent or a legal obligation. It would be appropriate for § 26 to refer expressly to this distinction, since it is decisive for operational purposes.

Second connection — with § 47 on the scope of broad consent. Paragraph 47 states, in terms, that broad consent may cover the "provision of data (e.g. by way of transmission or giving access through a secure processing environment)", provided that the processing remains within the declared area of research and within the data subject's reasonable expectations. This means that, where the disclosure is envisaged in the original privacy notice and falls within the scope of the broad consent, it is covered by the consent obtained. Paragraph 26 does not refer to § 47, and a reader who stops at § 26 may fail to grasp that a disclosure envisaged in the privacy notice does not pass through the rules on further processing but remains covered by the original legal basis. This connection should likewise be made explicit.

Third connection — with Section 5 on information obligations. Paragraph 26 governs disclosure at the level of the qualification of the processing, but not at the level of the information to be provided to the data subject. Section 5 contains the general transparency obligations and, at §§ 84–89, the obligations relating to further processing. What is missing, however, is specific guidance on how to describe, in the privacy notice, the existence of a disclosure relationship between controllers for scientific research purposes — in particular where the disclosure is ongoing or where it involves several recipients operating in the same area of research. It would be useful for § 26 to include at least a cross-reference to the relevant paragraphs of Section 5.

Reformulated comment for the EDPB

The text of § 26 is clear as to what it states, but the scope of the rule is limited to two aspects — the qualification of the operation as further processing and the exemption from the compatibility test — leaving the reader to reconstruct the overall framework by cross-referencing other paragraphs of the Guidelines. Given the importance of the subject, it would be appropriate for the Guidelines to specify this framework more clearly, making explicit in § 26 the connection with at least three aspects: (i) the rules on the legal basis for further processing under §§ 21–22, with particular reference to situations where the initial basis was consent; (ii) the scope of broad consent under § 47, which expressly covers the provision of data to another controller where this falls within the declared area of research; (iii) the information obligations under Section 5, in particular as regards the description of the disclosure relationship in the privacy notice provided to the data subject.

3. Storage limitation (§§ 27–29)

Paragraph 27 establishes the obligation to determine the storage period (or the criteria for determining it) before processing begins.

Paragraph 28 allows storage for future further research, even beyond the exhaustion of the original purpose, but frames the principle in cautious terms: "it may be permitted to store the personal data for such projects".

Paragraph 29 introduces two limits: storage cannot be justified by "generic" research purposes, and future activities must be "reasonably foreseeable" in relation to the relevant field of research.

Assessment

On "it may be permitted" — the conditional wording of § 28 ("may be permitted") remains operationally suspended. The conditions can be derived from §§ 29–31 (delimitation to an area of research, reasonable foreseeability, minimisation, safeguards under Article 89(1), periodic review), but § 28 does not refer to them expressly.

Moreover, the relationship with the information obligation is not clarified in § 28: the requirement for the controller to inform data subjects of the further processing is indeed governed at §§ 84–89, but § 28 does not refer to it. A reader who stops at § 28 may reasonably wonder whether a subsequent privacy notice is required when the future research project is launched.

The concept of "specific area of research" remains abstract at § 29. An example would help to calibrate the level of specificity required.

Reformulated comment for the EDPB

Paragraph 28 should (a) expressly refer to the conditions set out in §§ 29–31, in particular reasonable foreseeability, minimisation and periodic review of the storage format; and (b) refer to the information obligations on further processing (§§ 84–89; Article 13(3) GDPR), clarifying that storage for future research does not exempt the controller from the obligation to inform data subjects before the further processing begins. It would also be appropriate to include a concrete example at § 29 illustrating the acceptable level of specificity for defining the "area of research".

In addition, there are a great many retrospective studies that analyse data used for earlier research in new fields — and not only in medicine — that were not even foreseeable a few years earlier and that open the way to discoveries, especially but not exclusively in the medical field, regarding correlations between events and conditions once considered unrelated. An opening in this direction as regards storage and reuse would be useful (also in terms of the declared objective referred to in § 11).

There remains a tendency to flatten scientific research onto predeterminable aims: the true value lies precisely in the unexpected discovery that opens up multiple avenues for further investigation.

Proposed example

An example at § 29 such as:

> "An IRCCS (Scientific Institute for Research, Hospitalisation and Healthcare) stores the clinical data collected in a completed observational study on the treatment of acute paediatric leukaemias, with a view to possible future research projects within the same area (treatment of haematological malignancies in paediatric age). Specifying the area in this way is sufficient. By contrast, the mere indication of 'oncological research' or 'medical research' would not be sufficient, as these would amount to the notion of generic purpose excluded by § 29."

4. Single consent for healthcare and research (§ 38)

Paragraph 38 states that the controller "can obtain a single consent for clinical research that involves the processing of personal data which are necessary both for the purposes of providing healthcare and conducting scientific research, since those purposes are interrelated". It prohibits, however, making the provision of healthcare conditional on consent to research where the two purposes are not interrelated.

Assessment

The statement in § 38 is ambiguous in its wording, because it appears to equate two figures that, within the GDPR system, are clearly distinct: (i) GDPR consent under Article 6(1)(a) and/or Article 9(2)(a) as the legal basis for processing; (ii) the ethical-clinical consent to participation in research, which is a different matter (as the EDPB itself correctly recalls at §§ 53–55 of the Guidelines).

The legal basis for processing for healthcare purposes is, as a rule, Article 9(2)(h) GDPR (preventive medicine, diagnosis, healthcare) — not consent. The legal basis for processing for clinical research purposes may be consent under Article 9(2)(a) or a derogation under Article 9(2)(g), (i) or (j) (in the Italian system: Article 110 of the Codice Privacy).

Read in strictly technical terms, therefore, a "single GDPR consent" covering both healthcare and research does not hold up: healthcare does not require GDPR consent.

What § 38 probably means is that the data subject may sign, in a single operational interaction, two distinct expressions of will: the ethical-clinical consent to participation and the GDPR consent to research (the latter only for the research). But if that is the intended meaning, it must be stated explicitly, because the current wording is misleading.

This is also the point on which the Italian position (a clear separation between healthcare and research) and the EDPB position appear to diverge: our Group, in the rules of professional conduct, maintains the separation. It is worth flagging this to the EDPB as a substantive tension, not merely as a request for clarification.

Reformulated comment for the EDPB

Paragraph 38 warrants technical reformulation.

As drafted, it appears to suggest that a single consent under Articles 6(1)(a) and 9(2)(a) GDPR may cover both processing for healthcare purposes and processing for scientific research purposes. This is not consistent with the structure of the legal bases under the Regulation: processing for healthcare purposes is, as a rule, grounded in Article 9(2)(h), not in consent; processing for research purposes is grounded, alternatively, in Article 9(2)(a) or in the derogations under (g), (i) or (j). The EDPB should clarify whether the intent of § 38 is to allow the integrated collection, in a single interaction, of two distinct expressions of will (the ethical-clinical consent to participation and the GDPR consent to research), or something else. In any event, it should be made explicit that the legal basis for processing for healthcare purposes does not change and remains Article 9(2)(h) GDPR.

Proposed amendment

Replace the first sentence of § 38 with wording such as:

> "In the field of clinical research, controllers can obtain — in a single interaction with the data subject — both the ethical-clinical consent to participation in research and the GDPR consent to the processing of personal data for scientific research purposes, where the processing for healthcare and the processing for research purposes are interrelated. It must however be made clear to the data subject that the GDPR consent covers only the processing for scientific research purposes, the legal basis for the processing for healthcare purposes remaining Article 9(2)(h) GDPR."

5. Broad consent: introduction of the concept (§ 40)

Paragraph 40 introduces the figure of broad consent: in the context of scientific research, it is possible to rely on consent even where the purposes of the research are not fully known at the time of collection, provided that specific additional safeguards are adopted and the ethical standards of the sector are respected.

Assessment

The request for an example is well founded: broad consent is a new figure in the EDPB's explicit nomenclature (even though the idea is already present in Recital 33 GDPR), and § 40 introduces it in the abstract.

Example 8 (placed at the end of Section 4.1.2.1, after § 50) provides a paradigmatic case (a network of university hospitals, a federated database), but the distance between the introduction of the concept at § 40 and the example makes the latter hard to anchor to a concrete case.

Proposed addition

Bring the example forward or, alternatively, insert at § 40 an express cross-reference to Example 8. It would also be useful to include a simpler example (a single controller, not a network) illustrating broad consent in its elementary form, before moving to the more complex case of a network of controllers sharing the same broad consent.

6. Broad consent shared between several controllers (§ 43)

Paragraph 43 provides that "in certain cases, several controllers can rely on the same broad consent", referring to Recital 33 GDPR and Recital 26 of the Data Governance Act.

Assessment

Paragraph 43 acknowledges that several controllers may rely on the same broad consent without, however, clarifying the nature of the relationship between the various controllers.

Clarification is sought as to whether it is possible to request a broad consent indicating the possibility of further controllers, who may then each complete, in their own way, the level of information required under Articles 13 or 14 GDPR.

This aspect is not addressed in the section on privacy notices.

Reformulated comment for the EDPB

It would be appropriate for § 43 to clarify the criteria for allocating roles where several controllers rely on the same broad consent, with an explicit reference to Section 7. In particular, it should be made explicit that sharing the consent does not in itself amount to either joint controllership or separate controllership, and that the qualification depends on a substantive analysis of the determination of the purposes and essential means of the processing. A cross-reference between § 43 and Examples 22 (independent controllers) and 25 (joint controllers), which illustrate the two opposite controllership configurations, would be useful. Example 8, by contrast, is a case of broad consent and does not resolve the controllership configuration.

7. Broad consent and specification of purposes (§ 44)

Paragraph 44 reiterates, in line with the Guidelines on consent 05/2020, that broad consent cannot circumvent the principle of purpose specification. Controllers cannot merely indicate "scientific research purposes", but must define the purposes of the future research "as clearly as possible".

Assessment

Paragraph 44 sets a quality standard ("as clearly as possible") that is inherently a matter of degree. Without examples of acceptable and unacceptable formulations, the standard remains operationally elusive.

Proposed example

Insert a comparative example: an unacceptable formulation ("scientific research"; "medical research"); an acceptable formulation ("clinical research in the field of oncology"; "epidemiological research in the adult population of region X").

The decisive criterion should be whether the data subject can understand the thematic scope within which their data will be used.

It is also requested that the case of data altruism be analysed — under which a data subject could provide a broad consent to a given research body for several research projects — or that this aspect at least be clarified in the parts dealing with the data infrastructure.

8. Delimitation of the area of research (§ 45)

Paragraph 45 specifies that the purpose may be delimited to a research sector, and expressly gives as examples "medical research in the field of oncology" or "sociological research in the field of criminology". The purpose may also be delimited by reference to the expected outcomes of the research.

Assessment

The comment flags a counter-intuitive point: § 45 uses "oncology" as an example of acceptable delimitation, but in practice "oncology" is an extremely broad field (hundreds of conditions, heterogeneous molecular profiles, widely differing therapeutic approaches).

If "oncology" is the acceptable level of granularity, this should be clarified, because the more cautious reading would call for a much finer granularity.

In short, the level of granularity required needs to be clarified more clearly.

Reformulated comment for the EDPB

Paragraph 45 uses "oncology" as a paradigmatic example of an acceptable area, but the reference is ambiguous.

It would be useful to clarify whether the acceptable level of granularity is really that of the example (an entire medical discipline) or whether the illustrative wording should be read more restrictively (e.g. haematological oncology, paediatric oncology, etc.). This aspect bears directly on the validity of broad consent as a legal basis.

In addition, it is requested that it be clarified that broad consent is, above all, a consent to store data for scientific research, deferring to later stages the expression of the further specific consent that serves as the legal basis (see §§ 44 and 46).

9. Assessment of reasonable expectations (§ 46)

Paragraph 46 provides that, when individual research projects become known, the controller must assess whether their conduct falls within the boundaries of the original broad consent, having regard to the data subject's reasonable expectations.

Where the research falls outside the scope, dynamic consent must be used.

Assessment

The comment touches on an operationally critical point. The assessment of reasonable expectations is the mechanism that determines whether a given research project can be carried out under the existing broad consent or whether, instead, it requires a new consent. This is the issue that, in practice, determines whether a biobank or a research register functions or grinds to a halt.

Paragraph 46 merely indicates a method (consultation with groups representative of the data subjects) but provides no operational criteria or concrete methodological guidance: who conducts the assessment, according to what parameters, with what documentation, and with what role for the ethics committee, the DPO and any oversight body envisaged by § 49.

Moreover, § 48 introduces "ethical considerations concerning communication with research participants", but this too risks paralysing the use of broad consent. It should be included in the reformulated comment.

Reformulated comment for the EDPB

Section 4.1.2.1 contains an operationally critical point at § 46: the assessment of the correspondence between an individual research project and the scope of the broad consent.

It would be appropriate for the Guidelines to provide more structured methodological criteria for conducting that assessment, in particular with reference to the following elements: (i) who conducts the assessment and with what documentation; (ii) which factors are to be considered (relationship with the declared area of research, intensity of the intrusion, presence of new categories of data or of new processing entities, time elapsed since the original consent, evolution of the scientific context); (iii) what role is played by the ethics committee, the DPO and the oversight body referred to in § 49; (iv) within what timeframe the assessment must precede the launch of the project, also in coordination with the obligation to provide prior information on the further processing (Article 13(3) GDPR and §§ 84–89 of the Guidelines).

10. Reasonable expectations and legitimate interest (§ 62)

Paragraph 62 indicates that the controller must consider the data subject's reasonable expectations.

In some sectors, there may be a clearer expectation that the data will be processed for scientific research purposes. Expectations may be explored through consultation with organisations representative of the categories of data subjects.

Assessment

The request for examples is well founded. Reasonable expectations are one of the most discretionary factors in the balancing exercise under Article 6(1)(f), and their concrete application varies considerably across sectors (the pharmaceutical industry, academia, commercial entities engaged in R&D). Without examples, the standard remains opaque.

Proposed example

Insert at § 62 a comparative example such as:

> "The customers of a commercial company who, in subscribing to a service, provided their data for contractual purposes cannot reasonably expect that the same data will be reused for scientific research purposes aimed at developing the company's products. By contrast, the patients of an IRCCS who, at the point of clinical intake, were informed of the institute's participation in scientific research programmes in its field of specialisation can reasonably expect that their data, following pseudonymisation, will also be processed for that purpose."

11. Derogations under Article 9(2)(g), (i), (j) GDPR (§ 73)

Paragraph 73 establishes that national or EU laws acting as a derogation for the processing of special categories must respect the essence of fundamental rights, observe the principle of proportionality, and provide appropriate and specific safeguards for the fundamental rights and interests of the data subject.

Assessment

Footnote 115 lists examples of national laws (Danish, Finnish, French, German, Icelandic, Italian — Article 110 of the Codice Privacy — and Swedish) and a provision of EU law (Article 57(1)(a)(i) EHDS) presumed to operate as derogations under Article 9(2)(j). But the same footnote expressly states that "the EDPB has not reviewed nor analysed the laws referred to".

The practical result is that the national legislator does not know what it must write for its law to be regarded as a valid derogation, and the controller does not know what to look for in national laws to verify whether processing can be grounded on them. These derogations are applied far less than the structure of the GDPR

would allow, and there is a fallback to consent (with all the problems of specificity and withdrawal that this entails).

Reformulated comment for the EDPB

Section 4.4.3 leaves a margin of applicative uncertainty that, in practice, has paralysing effects. The Guidelines list national laws presumed to operate as a derogation under Article 9(2)(g), (i), (j), but do not analyse their content and do not clarify which elements a national law must contain in order to validly constitute the derogation.

It would be appropriate for the EDPB to provide, at least by way of example, a minimum standard for the required content: identification of the categories of data; identification of the categories of data subjects; identification of the public-interest purposes; indication of the technical and organisational safeguards; designation of the supervisory authority; and arrangements for publicising the derogation.

Without this minimum level of guidance, the system risks operating asymmetrically across Member States and overloading consent as the default basis, with all the consequent problems for scientific research.

It is further suggested that other examples be given, in addition to the EHDS Regulation, of provisions of EU law that may constitute grounds for derogation from the prohibition on processing special categories of data under Article 9(2)(j) GDPR. In particular:

> *– Horizon Europe — Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe, the Framework Programme for Research and Innovation;*
>
> *– Next Generation EU — Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021, published in the Official Journal of the European Union L 57 of 18 February 2021, establishing the Recovery and Resilience Facility of the European Union;*

In these cases too, controllers must adopt "technical and organisational measures, in particular in order to ensure respect for the principle of data minimisation" (Article 89(1) GDPR). Controllers must ensure that scientific, medical or epidemiological research projects approved under EU law (e.g. Horizon Europe or Next Generation EU) follow personal-data processing protocols that are proportionate to the purposes pursued, respect the essence of the right to data protection, and provide appropriate and specific measures to safeguard the fundamental rights and interests of the data subject — for example, through the provision of periodic reporting and audit procedures on compliance with the required data-protection standards, within ethical review processes, including independent review of individual research projects and strict conditions of use for researchers.

12. EHDS as a derogation under Article 9(2) (§ 75)

Paragraph 75 observes that reliance on Article 6(1)(f) in the context of medical research also requires the application of a derogation under Article 9(2) GDPR. It gives as an example Article 53(1)(e) of Regulation (EU) 2025/327 on the European Health Data Space (EHDS) as a provision of EU law constituting a derogation under Article 9(2). The reference is confirmed by Recital 52 EHDS.

Assessment

The reference to the EHDS at § 75 is important because it opens a concrete avenue for biomedical research seeking to rely on legitimate interest, but the wording is concise and leaves an important point open: § 75 cites Article 53(1)(e) as a single provision constituting the derogation, but does not clarify whether the derogation is constituted by Article 53 alone (and the related safeguards under Article 89 GDPR) or whether the entire EHDS framework must be considered (and in particular Articles 53–71 EHDS, which govern in a detailed manner the secondary use of health data).

The difference is operationally significant: in the first case, the controller must verify the existence of Article 53(1)(e) and adopt the safeguards under Article 89; in the second, the controller must also ensure that the processing is framed within the system of health data access bodies, secure processing environments, vetted purposes, etc., provided for by the entire EHDS framework.

Reformulated comment for the EDPB

The reference to the EHDS at § 75 is important and warrants clarification as to its scope. It would be appropriate for the Guidelines to specify whether Article 53(1)(e) EHDS alone constitutes the derogation under Article 9(2)(j) GDPR — subject to the controller's adoption of the safeguards under Article 89(1) — or whether the derogation is constituted by the entire body of EHDS provisions on secondary use (Articles 53–71), with the consequent involvement of health data access bodies and secure processing environments. The difference has significant operational implications, in particular for controllers wishing to carry out medical research outside the institutional EHDS system. It is further observed that the EHDS is referred to twice and on different bases: Article 57(1)(a)(i) in footnote 115 (as an example of a provision constituting a derogation under Article 9(2)(j)) and Article 53(1)(e) at § 75 (for medical research grounded on Article 6(1)(f)). It would be appropriate for the EDPB to clarify the relationship between the two provisions — whether they constitute alternative routes or operate on distinct perimeters (primary use of data vs. secondary use within the EHDS system) — in order to avoid uncertainty as to which provision actually applies.

13. Information on limitations of rights (§ 112)

Paragraph 112 recalls that Union or Member State law may provide for limitations of Articles 12–22 GDPR under Article 23, and derogations from the rights under Articles 15, 16, 18, 19 and 21 under Article 89(2), in so far as necessary for research purposes. The controller must verify the existence of such limitations and inform data subjects of them when fulfilling the transparency obligations.

Assessment

A privacy notice mentioning limitations of, or derogations from, the data subject's rights is a sensitive matter: it must be comprehensible, it must precisely identify the derogating provision and its scope, and it must enable the data subject to understand which rights remain available and how they may be exercised.

Without examples, it is difficult for the controller to calibrate the communication correctly.

Proposed example

Insert an example such as:

> "An IRCCS conducts a retrospective observational study on the basis of Article 110 of the Italian Codice Privacy (derogation under Article 9(2)(j) GDPR). Article 110 provides for limitations on the exercise of the rights of access, rectification, erasure and objection. The privacy notice must precisely indicate: (i) the derogating provision; (ii) the specific limitations applicable to each right; (iii) the means by which the data subject may still approach the controller in respect of the residual purposes (in particular, the exercise of the right to object on grounds relating to the data subject's particular situation, under Article 21(6) GDPR)."

Further points from the re-reading of the Guidelines, for consideration

In addition to the comments above, we note certain points emerging from the re-reading of the Guidelines that the Group might consider commenting on.

(i) Further processing of special categories (§§ 24–25)

The comment on §§ 17–23 concerns ordinary data, but §§ 24–25 extend the presumption of compatibility to data under Article 9: the controller must nonetheless re-assess the applicable derogation under Article 9(2) and consider any additional conditions imposed by Member State law under Article 9(4). For an IRCCS processing health and genetic data, this is the central issue: the problem of a consent-based initial basis, flagged at § 22, recurs in more acute form at the level of Article 9 where the initial derogation was explicit consent (Article 9(2)(a)). The EDPB could be asked to clarify how the re-assessment of the derogation is structured, in such a case, in the context of further processing.

(ii) Retention of contact details and minimisation (§§ 86–87)

Paragraph 87 requires that contact details not be deleted where further processing for research is envisaged, and § 86 requires that data subjects be kept informed. This guidance is in tension with the minimisation principle, which would push towards eliminating identifiers and contact details that are no longer necessary. For biobanks and longitudinal registers — typical of paediatric research — the constraint is operationally significant: it would be useful to ask the EDPB for criteria to reconcile the retention of contact details for future transparency with minimisation. This point connects with the comment on §§ 27–29.

(iii) Serendipitous and cross-disciplinary research (§ 47 and § 29)

The point on unexpected discovery (comment on §§ 27–29) can be made more incisive by drawing on two footholds: § 47 expressly allows broad consent to cover research that evolves in an unanticipated direction, but only if it remains within the same area of research; and Article 8(4) of the proposed rules of professional conduct already governs unexpected findings. The issue to put to the EDPB is the friction between the criterion in § 29 (future activities reasonably foreseeable in relation to the field of research) and genuinely cross-disciplinary research, in which the discovery is precisely the one that falls outside the declared field. Framed as a precise question on the boundary of the area of research (§ 29 and § 47), rather than as a generic criticism of the flattening onto predeterminable aims, the point becomes difficult to sidestep.

(iv) Safeguards for genetic and biometric data (Section 8.3–8.4)

The draft does not comment on Section 8.3–8.4. The point nonetheless warrants attention, because the Guidelines themselves recognise that genetic profiles are personal data by default and can be regarded as anonymous only in exceptional circumstances, following an analysis of the genetic configuration and its frequency in the population (§ 165); that the risks extend not only to the participant but also to their blood relatives, and that genetic data are immutable and persist beyond the data subject's lifetime (§ 167); and that, when datasets are combined, the risk of re-identification increases (§ 161). It follows that, for genomic data, anonymisation is in practice rarely achievable, and pseudonymisation accompanied by access governance constitutes the realistic minimum threshold, not one option among others.

We therefore propose asking the EDPB for three clarifications. First, that the standard of "strict necessity and proportionality" for processing in directly identifiable form (§ 159) be specified for genomic data, recognising that — given the residual risk of re-identification even after pseudonymisation — the safeguards in § 168 (pseudonymisation, federated storage with access through a secure processing environment, strict role-based access controls, ethical approval) are not merely contingent but constitute the ordinary safeguard for genomic research. Second, that the position of third-party blood relatives — who are not research participants but whose data are implicated by the genetic analysis (§ 167) — be clarified as regards transparency obligations and rights, which is not currently addressed. Third, that the logic of the information campaigns provided for at § 169 for isolated population groups be extended to rare-disease cohorts, where the small numbers and high identifiability pose analogous risks of re-identification, discrimination and stigmatisation.

In support, we propose inserting at § 168 an example such as:

> "An IRCCS conducts a genome-sequencing study on a cohort of paediatric patients affected by a rare disease. Because the genomic profile cannot be anonymised and the small size of the cohort increases the risk of re-identification, the controller stores the data in pseudonymised form within a secure processing environment, with separation of the correspondence table, federated access and role-based controls, subject to ethics committee approval; sharing with other centres takes place solely through that same secure environment, without local copying of the data, consistently with the EHDS secure processing environments and the EDPB Guidelines on pseudonymisation."

This would connect Section 8.4 with footnote 250 (Article 73 EHDS) and with the Guidelines on pseudonymisation already referred to.

(v) Data of deceased persons processed for research (a point not addressed by the Guidelines)

The Guidelines do not appear to address specifically the processing, for scientific research purposes, of data relating to deceased persons, even though this is a recurring situation in retrospective studies, disease registers, biobanks and projects based on clinical, administrative or research archives.

Recital 27 of Regulation (EU) 2016/679 specifies that the GDPR does not apply to the personal data of deceased persons, without prejudice to the possibility for Member States to introduce rules on the processing of such data. In the light of that provision, a clarification on the relationship between data relating to deceased persons and the conditions laid down for scientific research by Article 9(2)(j) GDPR would be useful.

In particular, the conditions and safeguards laid down by that provision, as well as any national rules adopted on its basis, appear to operate within the scope of application of the Regulation and therefore to presuppose the processing of personal data relating to living data subjects. They do not appear, in themselves, to extend the scope of the GDPR to data relating exclusively to deceased persons.

This point is of particular relevance in research projects that use mixed datasets, composed of both data relating to living persons and information relating to deceased persons. In such cases, greater clarity would help controllers, researchers and ethical review bodies to correctly identify the applicable rules, reducing interpretative and applicative uncertainty.

In the Italian context, for example, there is sometimes a tendency to apply, also to data relating to deceased persons, the safeguards laid down for scientific research on personal data, including the national rules adopted in implementation of Article 9(2)(j) GDPR. Although this is a point also connected with national law, a general clarification on the scope of the GDPR with respect to the data of deceased persons would foster a more consistent reading across Member States.

It might also be useful to include practical examples of governance measures and appropriate safeguards for the use, for research purposes, of data relating to deceased persons. Such measures might concern, among other things, controlled access, pseudonymisation where possible, ethical assessments, data-sharing rules and caution in publishing results, also having regard to the dignity, confidentiality and memory of the deceased person, as well as any interests of family members or other connected persons.

(vi) Information to be provided in the case of disclosure of pseudonymised data

Paragraph 94 and Example 15 appear to presuppose that the disclosure of pseudonymised data to another controller necessarily constitutes a disclosure of personal data and therefore entails the application of the information obligations under Articles 13 and 14 GDPR for the recipient of the data.

On this point, a deeper analysis would be useful, in the light of the recent case law of the Court of Justice on the identifiability of data subjects. In particular, the concrete position of the recipient of the

pseudonymised data should be considered, together with the means available to it, or that it is reasonably likely to obtain, to re-identify the data subjects.

In the context of scientific research, the sharing of pseudonymised datasets between universities, research bodies, healthcare facilities and project partners is frequent. In such cases, it may be that the recipient does not have the additional information necessary for re-identification and has no reasonable means of accessing it. A clarification would therefore help to distinguish situations in which the recipient still processes personal data from those in which, in light of its concrete position, the data subjects are not identifiable and the processing therefore no longer falls within the scope of the GDPR.

A further aspect concerns the reference, among the information to be provided to the data subject, to the pseudonymisation code, contained in § 94. That passage might be interpreted as an indication to disclose that code or equivalent identifiers. It would be useful to clarify whether this is actually required by the GDPR, considering that knowledge of such elements may, in some circumstances, reduce the effectiveness of pseudonymisation as a safeguard under Article 89 and increase the risk of re-identification. Guidance might therefore be useful on how to balance the transparency obligations against the need to preserve the effectiveness of pseudonymisation and other safeguards in the research context, including practical examples.

Milan, 24 June 2026

Silvia Stefanelli, Attorney-at-Law
Stefanelli & Stefanelli Law Firm
Expert in Digital Health Law and Data Law
Member of the Territorial Ethics Committee Nord Emilia Romagna
Milan, Bologna, Rome, Venice

Flavia Cristiano
Data Protection Officer
University of Perugia

Susanna Conti
Italian Society of Medical Statistics and Clinical Epidemiology (SISMEC)

Eleonora Sfreddo
Chief Operating Officer
FROM – Fondazione per la Ricerca Ospedale di Bergamo

Francesca Preite, Attorney-at-Law
Miari Preite Law Firm
Reggio Emilia

Stefania Stefanelli
Full Professor of Private Law

Perugia University

Giorgio Valandro
Data Protection Officer
Director, Legal Affairs Office
University of Padua

Avv. Angelo Loiacono, Attorney-at-Law
Head of Privacy Function - Data Protection Officer
Bambino Gesù Children's Hospital I.R.C.C.S. (Rome)

Patrizia Comite, Attorney-at-Law
Adjunct Professor of Health and Social Care Law at UniUma, Milan
Member of the Territorial Ethics Committee Lombardy 2 (IEO/Monzino)
Member of the Bioethics and Healthcare Liability Committees of the Milan Order of Physicians and Dentists (OMCEO)
Founder and Member of the CAPIRE Observatory of ANMAR ETS

Davide De Luca
Strategic Advisor in Digital Compliance, Cybersecurity and AI;
Data Protection Officer (DPO);
Court-Appointed Technical Expert (CTU)
Global Com Technologies S.r.l.