Concept of Scientific Research (Section 2):

Guidelines 1/2026 develop a set of factors intended to determine when an activity may be regarded as scientific research within the meaning of the GDPR. These factors are:

a) A systematic and rigorous methodology.
b) Adherence to ethical and professional standards.
c) Transparency and verifiability of results.
d) Autonomy and independence in the choice of means and purposes.
e) Contribution to the public interest or societal well-being.
f) Contribution to existing scientific knowledge or the innovative application thereof.

Throughout the Guidelines, scientific research activity is associated with the development of a research project, but ancillary processing operations are also included, such as the identification of potential participants, extraction, filtering, grouping, curation, categorisation, anonymisation, or pseudonymisation of data.

Does the EDPB consider that ancillary operations must themselves satisfy the factors used to identify scientific research, or is it sufficient that they are functionally linked to a scientific research project that meets those criteria? Should the qualification of processing as being carried out for scientific research purposes be understood as depending on the intrinsic characteristics of the specific processing operation, or on the broader scientific context within which that operation is integrated?

This clarification would be particularly useful for actors performing essential data management and preparation functions without directly participating in the scientific activity itself.

Compatibility (Section 3.1.1)

Guidelines 1/2026 develop the presumption of compatibility for processing carried out for scientific research purposes, establishing that such processing does not require a compatibility test and that the legal basis which legitimised the initial processing of the data may also be relied upon. As a general rule, this presumption of compatibility requires the use of pseudonymised data.

There is, however, a very common subgroup of studies with a retrospective design (i.e., analyses of events that occurred before the study) which involve direct access to medical records and therefore to special categories of personal data (Article 9 GDPR). These studies are carried out by healthcare professionals belonging to the same clinical team responsible for the patient's care.

In such cases, access to pseudonymised data is not feasible, since the study requires the identification of specific variables within medical records, a task that can only be performed directly by the investigator who possesses the necessary clinical knowledge. Furthermore, pseudonymisation would not constitute an effective safeguard in these circumstances, as the clinical characteristics of the cases often make patients readily identifiable to the healthcare professionals involved in their care.

Would the presumption of compatibility apply to the processing of patient data contained in medical records where a healthcare professional accesses the records of their own patients for research purposes, provided that appropriate safeguards are subsequently implemented, such as working with coded data in secure local environments?

It appears somewhat unclear that compatibility is recognised while, at the same time, the Guidelines require that the legal basis legitimising the initial processing "is also suitable to rely on for the further processing of personal data for scientific research purposes." Moreover, according to the Guidelines, "It is, however, not always possible to rely on the same legal basis when further processing personal data for scientific research purposes. This applies in particular if the initial legal basis for the primary processing is consent or a legal obligation."

This seems to suggest the need to establish a separate legal basis for the research activity itself, thereby undermining the practical significance of the compatibility presumption. In particular, considering that the storage of clinical data for healthcare purposes is a legal obligation in Spain (Article 6(1)(c)/(e) GDPR), and that physicians access such data in order to diagnose or treat patients (Article 9(2)(h) GDPR), should scientific research be regarded as a compatible purpose in this scenario?

Broad Consent vs. the Concept of Scientific Research (Section 4.1.2.1)

As noted above, Guidelines 1/2026 establish that, in principle, activities meeting certain substantive criteria may be regarded as scientific research within the meaning of the GDPR.

However, when addressing broad consent, the Guidelines state that it is not sufficient merely to inform data subjects that their data will be processed for scientific research purposes; rather, a specific research area or field must also be identified.

In this regard, we would welcome clarification from the EDPB regarding the relationship between these two requirements.

In particular, if scientific research already constitutes a legally delimited purpose through the substantive criteria developed in Section 2.1 of the Guidelines, what is the justification for requiring an additional specification of research areas for the purposes of broad consent?

Furthermore, does the EDPB consider that the purpose of "scientific research," understood in accordance with the substantive criteria established in the Guidelines, is in itself insufficiently specific?

This issue is particularly relevant for research infrastructures, biobanks, population cohorts, and data repositories intended to support multiple future scientific projects, where identifying sufficiently specific research areas ex ante may prove difficult or artificial. In some cases, the practical response may simply be to define the broadest possible research area in order to encompass as much future research as possible.

Dynamic Consent (Section 4.1.2.2)

Guidelines 1/2026 present dynamic consent as a mechanism capable of strengthening data subjects' autonomy by allowing consent to be sought repeatedly as new research projects or phases are defined.

However, we would welcome clarification from the EDPB as to how this approach should be reconciled with the legal nature of consent under the GDPR.

In particular, dynamic consent appears to transform consent from a single act of informational self-determination concerning a specific processing activity into an ongoing process involving successive requests for authorisation. In this context, questions arise as to whether the accumulation of multiple consent requests over time may affect data subjects' ability to make genuinely free and informed decisions, especially in light of phenomena such as consent fatigue, routine acceptance of repeated requests, or the creation of long-term relationships between participants and research institutions.

Accordingly, we would welcome clarification from the EDPB as to whether it considers that any substantive or functional limits exist regarding the use of dynamic consent and how it believes that, from the perspective of Articles 4(11) and 7 GDPR, an ongoing succession of consent requests can continue to represent a freely given, specific, informed, and unambiguous indication of the data subject's wishes.

We would also appreciate clarification as to how the sections concerning the delineation of research areas under broad consent should be reconciled with the logic of dynamic consent, and what specific role each of these mechanisms is

intended to play from the perspective of data subject autonomy and the purpose-limitation principle.

Pseudonymisation (Section 8.3)

Guidelines 1/2026 repeatedly refer to pseudonymisation as a key safeguard within the meaning of Article 89 GDPR for the processing of personal data for scientific research purposes.

However, recent case law of the Court of Justice of the European Union, in particular the judgment in *EDPS v. SRB* (Case C-413/23 P), appears to support a contextual and recipient-specific assessment, according to which pseudonymised data may not constitute personal data for a recipient that does not possess means reasonably likely to be used to re-identify the data subjects.

In many scientific research contexts, including secure data processing environments, research data infrastructures, trusted research environments, and controlled-access repositories, researchers receive only pseudonymised datasets and do not possess any legal, technical, or practical means of accessing the additional information necessary for re-identification.

In this context, could the EDPB clarify whether, and under what conditions, the assessment of pseudonymised data in scientific research should follow the dynamic, recipient-oriented approach endorsed by the CJEU?

More specifically, does the EDPB consider that a researcher or research institution receiving pseudonymised data without access to the additional information necessary for re-identification should always be regarded as processing personal data, or should that assessment depend on whether the recipient has means reasonably likely to be used to identify the data subjects?

Clarification on this issue would be particularly relevant for the operation of research data infrastructures and for ensuring legal certainty in scientific research projects conducted across multiple institutions within the European Research Area.