Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

Sciensano's contribution to the EDPB Guideline entitled

" *Guidelines 1/2026 on processing of personal data for scientific research purposes*"

25th June 2026

Prepared by:

Roxana Albu *Scientific Expert,* ***Joke Sas*** *Scientific Expert,* ***Marion Louis*** *DPO,* ***Luc Maes*** *DPO*

Wannes Van Hoof *Head ELSI,* ***Melissa Van Bossuyt*** *Head DPO & Coordinator Information Security*

Contents

EXECUTIVE SUMMARY 2
SECTION-SPECIFIC GAPS 3
1. Strengthening the six key-indicative factors through public-health-relevant examples 8
Issue statement 8
Need for clearer articulation in the Guidelines 9
2. Persistent ambiguity around the definition of "purpose" in research creates structural barriers to lawful secondary use 10
Issue statement 10
Need for clearer articulation in the Guidelines 11
Concrete examples from public health research 12
3. Overestimate the feasibility of consent-based models in long-term, population-level research infrastructures 13
Issue statement 13
Need for clearer articulation in the Guidelines 15
4. Ethical consent vs GDPR consent 16
Issue statement 16
Need for clearer articulation in the Guidelines 17
5. PUBLIC INTEREST as legal basis 19
Issue statement 19
Context and practical implications 19
Need for clearer articulation in the Guidelines 19
Clarification on the use of Article 6(1)(e) GDPR (Public Interest) in health research 20
Operational limitation: absence of the one-stop-shop mechanism 20
6. Transparency obligations for long-term scientific research remain insufficiently operationalised 20
Issue statement 20
Need for clearer articulation in the Guidelines 21

Concrete proposals 22

7. Proportionality and legitimate interest assessment (LIA) 22

Issue statement 22
Need for clearer articulation in the Guidelines 23
Concrete proposals 23

8. Lack of operational clarity on documenting and applying the presumption of compatibility for scientific research 24

Issue statement 24
Need for clearer articulation in the Guidelines 26
Concrete proposals 26

9. Lack of guidance on proportionate, risk-based pseudonymisation in research 27

Issue statement 27
Need for clearer articulation in the Guidelines 28
Concrete proposals 29

10. International data transfers for scientific research are insufficiently addressed 29

Issue statement 29
Need for clearer articulation in the Guidelines 30
Concrete proposals 31

11. Genetics, omics and special categories of data 32

Issue statement 32
Need for clearer articulation in the Guidelines 32
Concrete proposals 33

12. Unharmonised interpretation of complex research roles 35

Issue statement 35
Need for clearer articulation in the Guidelines 35
Concrete proposals 35

13. Rights of data subjects whose data are used in research 36

Issue statement 36
Need for clearer articulation in the Guidelines 36
Concrete proposals 37

CONCLUSION 39
ABOUT SCIENSANO 42

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

Executive summary

The European Data Protection Board (EDPB) Guidelines 1/2026 represent an important step toward clarifying the application of the GDPR to scientific research. However, when examined against the operational realities of public health, clinical research, long-term cohort infrastructures, and emerging EU data-governance frameworks, several structural gaps remain. These gaps are not marginal; they affect the feasibility, legal certainty, and cross-border continuity of scientific research across the Union. They also risk undermining the coherence between the GDPR and the rapidly evolving EU health-data ecosystem, including but not limited to the European Health Data Space Regulation (EHDS), the Data Governance Act (DGA), the Clinical Trials Regulation (CTR), the *In Vitro* Diagnostic Medical Devices Regulation / Medical Devices Regulation (IVDR/MDR), and the Artificial Intelligence Act (AI Act).

Across Member States, researchers, public bodies, ethics committees, and data-protection authorities face divergent interpretations of core GDPR concepts: purpose, legal basis, pseudonymisation, compatibility, controllership, and data-subject rights. These divergences create fragmentation that directly impedes scientific progress, delays approvals, and generates inconsistent expectations for controllers. The Guidelines, while conceptually robust, do not yet provide the operational clarity needed to ensure harmonised implementation in complex research settings.

A key element missing from the current guideline is the operationalisation of GDPR as it applies to health and scientific research. We really need a new and coherent approach to data governance for reuse of data and scientific health research. The current discussion remains too narrowly focused on privacy and data protection issues.

The real challenge is to build a framework that enables research (an "*YES, we can*" GDPR), validation, cross border data reuse, and algorithmic improvement lawfully and proportionately. This requires a shift in perspective: research should not be treated as an exception to be constrained, but as a core public interest activity that needs clear, workable mechanisms rather than abstract principles. It also requires genuine coordination across all oversight bodies.

The EDPB cannot operate in isolation from the EMA, national competent authorities, ethics committees, AI ethics experts, and health data governance bodies. These actors approach the same questions from different angles. Without shared principles, standards, and operational definitions, fragmentation will continue. Europe needs the equivalent of Good Data Protection Practices for Health Research: a harmonised, jointly endorsed framework that clarifies roles, safeguards, and lawful pathways for data reuse.

Despite early concerns, the GDPR has not stopped but has instead disrupted research in Europe. What persists instead is uncertainty, divergent interpretations, and a lack of harmonised guidance, which creates significant operational burden for research organisations.

Key concepts relevant to scientific and public-health research remain insufficiently defined, generating administrative workload across privacy, regulatory, and contractual teams without demonstrable benefit for data-subject protection. In some cases, this lack of clarity also creates institutional inertia, where human and organisational behaviour becomes increasingly risk-averse rather than proactively resolving cross-institutional barriers or apparent divergences.

To safeguard Europe's capacity for high-quality, ethically conducted health research, EU institutions, including the European Commission, the EDPB, DPAs, EMA, and national competent authorities, must provide coherent, harmonised, and practically applicable guidance that enables lawful data use while ensuring proportionate and effective safeguards.

Several cross-cutting recommendations occur from Sciensano's analysis:

1. Operationalise the GDPR for health and scientific research. The Guidelines should move beyond abstract principles and provide practical, operational guidance aligned with existing scientific, ethical, and regulatory standards (e.g., ICH GCP, CTR, IVDR/MDR, EHDS). GDPR bodies should not redefine research concepts but ensure GDPR is applied coherently within established research frameworks. A coherent European data-governance framework should recognise the specificity of health research, rely on already established sectoral standards, and encourage stakeholders to develop harmonised principles for data protection in research in the same spirit as internationally recognised frameworks such as International Conference Harmonisation – Good Clinical Practice (https://www.ich.org/). We recommend creating Good Data Protection Practices or Code of Conduct, applied to Clinical and Public Health Research.

In addition, there is a clear need for more detailed and differentiated data-governance guidance for Public Health Institutes. Their statutory tasks, monitoring and surveillance, maintaining registries, providing policy advice, and conducting research, are fundamentally different in purpose, legal basis, and operational requirements. Each of these functions requires a distinct but coherent governance approach. The Guidelines should explicitly acknowledge this diversity and provide principles that enable Public Health Institutes to fulfil their mandates effectively while ensuring proportionate and lawful data protection.

2. Provide a harmonised, research-specific interpretation of "purpose". Scientific research within a defined field, infrastructure, disease area, or statutory mandate should be treated as one overarching purpose, rather than fragmented into separate purposes for each project, dataset, or analytical step. A harmonised, research-specific interpretation of purpose is essential to reduce fragmentation, avoid institutional inertia, and ensure proportionate governance across Member States. This interpretation must explicitly recognise that research does not always begin with a narrowly formulated hypothesis: exploratory, data-driven analyses, such as identifying early-warning patterns in rich, longitudinal cohort datasets to infer disease onset decades in advance, serve the same overarching public-health purpose as downstream confirmatory studies. A coherent definition of purpose is also critical for enabling structural linkages and the long-term maintenance of population cohorts and research infrastructures. These resources should not be forced into repeated cycles of deletion and reconstruction simply because a specific project-level purpose has ended; their continued existence and enrichment fall under the broader, enduring research or public-health purpose defined by law or mandate. Moreover, clarifying purpose must be accompanied by a clearer articulation of roles and responsibilities, particularly around controllership. In practice, controllership is purpose-specific, not permanent, and the transitions in responsibility, especially under the EHDS Regulation, between data holder, HDAB, and data user during a secondary-use request, remain a source of operational uncertainty. While distinct from the definition of purpose, these role allocations are tightly interlinked: without clarity on both, institutions default to risk-averse interpretations that hinder legitimate research and complicate the governance of linked, longitudinal datasets.

A research-appropriate framing of purpose, coupled with explicit guidance on role boundaries and the permissibility of maintaining structural linkages, would support continuity, reuse, and long-term stewardship of health data while maintaining strong data-subject protection.

3. Strengthen examples for the six key indicative factors. We do not believe that the definition of scientific research should be fragmented across multiple EU regulations. Instead, it should be

governed by clear, stable principles developed by multidisciplinary teams with expertise in health research. Such principles already exist in internationally recognised frameworks, such as the Helsinki Declaration, the Nuremberg Code, the Taipei Declaration, the Oviedo Convention, and guidance from WHO and OECD, which collectively articulate the ethical and scientific foundations of research.

However, ff the EDPB intends to further elaborate criteria or provide examples, this work should build on these established principles rather than create parallel or conflicting definitions. In that context, the Guidelines should include public-health-relevant, domain-specific examples, such as surveillance systems, national registries, long-term cohorts, and biobanks, to support consistent interpretation of what qualifies as scientific research across Member States. This should explicitly reflect the diverse statutory tasks of public-health institutes (monitoring and surveillance, policy advice, and research), each of which requires distinct yet coherent data-governance principles.

4. Clarify the interplay between GDPR and other EU laws. Provide explicit guidance on how the GDPR interacts with the EHDS Regulation, CTR, IVDR/MDR, DGA, and the AI Act, particularly regarding legal bases, secondary-use conditions, and access requirements. This clarification should also address the allocation of roles and responsibilities, which remains a practical source of uncertainty. In the EHDS context, controllership is purpose-specific, not permanent, yet current guidance does not clearly explain how responsibility shifts between the data holder, the HDAB, and the data user throughout a secondary-use request. These transitions, distinct from but closely linked to the definition of purpose, create operational blockers and risk-averse interpretations when institutions cannot determine who is responsible for which processing stage. Clear, harmonised guidance on both purpose and roles is therefore essential to ensure consistent implementation, reduce administrative friction, and support lawful, proportionate data reuse across the EU research and public-health ecosystem.

5. The Guidelines should explicitly acknowledge that GDPR consent-based models are not feasible as the primary legal basis for long-term reuse of data, population-level research infrastructures or research on linked data from several sources. In health research that reuses data collected over many years, links datasets from multiple sources, or relies on public-health surveillance, national registries, or long-term cohorts, re-contacting individuals is often impossible or disproportionate. Insisting on re-consent in these contexts risks blocking essential research. The GDPR already provides appropriate alternatives, such as Article 6(1)(e) together with Articles 9(2)(i) or 9(2)(j), supported by Article 89 safeguards; and the Guidelines should clarify that broad or dynamic consent is an optional enhancement where feasible, not a baseline expectation. Explicit recognition of these structural limits would reduce fragmentation, promote consistent interpretation across Member States, and safeguard the continuity of vital research. At the same time, the Guidelines should acknowledge that new studies launched today will fall under the future secondary-use framework of the European Health Data Space Regulation, which may introduce obligations that appear to contradict current expectations around "future processing" in consent forms. Clear, forward-looking guidance is therefore needed on what information must be included in consent-based studies so that participants are not misled and researchers are not forced to revise consent materials repeatedly as EU law evolves.

6. Clarify the distinction between GDPR consent and ethical consent without imposing dual tick-box systems that confuse patients. While the distinction between GDPR consent and ethical/Helsinki consent may be clear to professionals, it is not meaningful or intuitive for patients, especially for vulnerable populations. Participation in research by design requires the processing of personal data, and introducing two separate tick boxes (one for study participation and one for GDPR

consent) creates a high risk of inconsistent choices. A patient may agree to participate in the study but inadvertently decline data processing, making full participation impossible. This approach is unreliable, confusing, and contrary to a patient-centred, accessible consent process. To avoid this contradiction, the Guidelines should explicitly allow a single, integrated consent statement that reflects the operational reality of research. A clear and patient-friendly formulation could be: *"If you agree to participate in this study, you also accept that your data will be processed for the purposes of this research."*

This preserves transparency, respects autonomy, and avoids unnecessary administrative complexity, while ensuring that participants are not misled by artificial distinctions that do not reflect how research is conducted in practice.

7. Recognise the interdependence of research and infrastructure. Acknowledge that research and the infrastructures enabling it, registries, biobanks, secure platforms, and federated environments, are not separate purposes but operationally inseparable components of lawful scientific research. These infrastructures are not merely technical service providers: they are scientifically governed, security and technical compliant, GDPR-compliant expert centres that ensure data quality, continuity, linkage, and controlled re-identification where scientifically necessary. They should therefore be treated, financed, and evaluated as integral parts of the research ecosystem, not as external utilities. Their long-term operation, including the maintenance of structural linkages and enriched cohorts, falls squarely within the overarching research purpose and should not be subject to repeated deletion or reconstruction cycles tied to individual project-level purposes. Recognising infrastructures as embedded research actors, rather than separate entities, supports data quality, scientific validity, regulatory compliance, and the sustainability of high-quality public-interest research.

8. Provide research-tailored guidance on international data transfers. Current transfer tools, SCCs, TIAs, and ad hoc clauses, are not fit for multi-actor, long-term scientific health research. Publicly funded and academic organisations often cannot conduct individual Transfer Impact Assessments (TIAs) or sign the existing Standard Contractual Clauses (SCCs) in their commercial form, yet rely on cloud-based analytics, federated models, and multi-year processing of pseudonymised data. Existing transfer instruments are also unstable, frequently challenged or revised, creating uncertainty for infrastructures that must guarantee continuity and reproducibility. We therefore strongly recommend that the EDPB establish research-appropriate transfer routes that allow lawful sharing of health data, especially pseudonymised data, when SCCs or adequacy decisions are unavailable, legally impossible, or disproportionate. This should include solutions for public bodies unable to sign SCCs, secure cloud processing, and federated data-visiting models. Such routes are essential to ensure that high-quality, long-term public-interest research can operate without recurring legal and administrative dead-ends.

9. Clarify the cumulative application of Articles 6 and 9 GDPR. Explain how Articles 6 and 9 operate together in light of the EHDS, and ensure that combinations of legal bases do not circumvent EHDS safeguards for AI training, testing, and evaluation.

10. Promote coordinated training across oversight bodies. Recommend mandatory training modules:

- Ethics committees should receive training on GDPR principles and limits.
- DPAs should receive training on clinical research, public-health methodologies, and sector-specific frameworks.

This is essential to reduce inconsistent interpretations.

11. Provide guidance on proportionate, risk-based pseudonymization. Clarify how pseudonymisation should be applied in research, recognising the risk spectrum of genetic and omics data and avoiding one-size-fits-all requirements that hinder scientific feasibility.

12. Harmonise interpretation of data-subject rights in research. Offer operational guidance on how rights (erasure, objection, access) apply when:

- data are pseudonymised,
- multiple controllers are involved,
- re-identification is not permitted or possible.

This is needed to avoid unrealistic expectations and inconsistent national practices.

These unresolved issues show that, while the Guidelines offer a solid conceptual basis, they still require substantial development to ensure harmonised, feasible, and legally certain implementation across the EU research ecosystem.

The recommendations proposed below by Sciensano ELSI and DPO teams aim to support the EDPB in strengthening the Guidelines so that they fully reflect the realities of modern scientific research, enable responsible data reuse, and uphold the fundamental rights of individuals while safeguarding Europe's capacity for high-quality, cross-border research.

We also note that recent documents issued by EU institutions, including the European Commission, the EDPB, and the European Parliament, sometimes provide divergent or partially contradictory recommendations regarding the reuse of health data for research. This fragmentation risks creating uncertainty for controllers, processors, and research infrastructures, particularly in Member States preparing for EHDS implementation. Greater alignment between the GDPR, the EHDS Regulation, and sector-specific frameworks (e.g., clinical research, public health surveillance, AI Act) is essential to ensure legal certainty and operational feasibility.

Sciensano appreciates the EDPB's efforts to clarify the application of the GDPR to scientific research and supports the overarching aim of enabling responsible, high-quality research while protecting fundamental rights. To maximise the Guidelines' impact, we encourage:

- further alignment with parallel EU initiatives,
- clearer operational guidance for public research institutions, and
- explicit recognition of the interdependence between primary and secondary use in health data ecosystems.

In preparing our submission, Sciensano has reviewed each section of the Guidelines and highlighted both elements that are clear and directly usable, and areas where further development or operational guidance is needed.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

Section-specific gaps

Scientific and public-health research operates in environments that are fundamentally different from commercial data processing. Research ecosystems involve multi-actor chains, statutory mandates, population-level datasets, long-term infrastructures, and high-risk data types such as genetic and omics data. Generic GDPR guidance cannot capture these operational realities. A sector-specific approach is therefore essential to ensure that GDPR principles are applied in a way that is proportionate, harmonised, and scientifically feasible, while still protecting individuals' rights. Without tailored guidance, Member States, DPAs, and ethics committees will continue to interpret key concepts inconsistently, creating fragmentation that directly impedes cross-border research and undermines Europe's ability to generate high-quality evidence for public health and clinical innovation.

Health research is already governed by a dense and mature ecosystem of scientific, ethical, and quality standards, including ICH GCP, clinical-trial legislation, biobanking frameworks, and disease-specific governance structures. The principles that define what constitutes scientific research, and what is required to ensure its validity, integrity, and auditability, are therefore best established by the expert bodies that regulate and oversee these domains, not reinvented within data-protection guidance. In this context, the role of GDPR-governing bodies should be to operationalise the GDPR for research, ensuring that its requirements align with and build upon existing scientific and regulatory standards, rather than redefining research concepts or introducing parallel criteria. A coherent European data-governance framework should recognise the specificity of health research, rely on established sectoral standards, and encourage stakeholders to develop harmonised principles for data protection in research in the same spirit as internationally recognised frameworks such as ICH GCP (https://www.ich.org/). What is needed is a principled, harmonised articulation of how "purpose" should be interpreted in the research context, one that recognises the continuity of scientific inquiry, the legitimacy of broad public-interest research aims, and the safeguards embedded in Article 89. Importantly, this articulation should be developed jointly by sector-specific health-research regulators, GDPR authorities, and research stakeholders, drawing inspiration from collaborative international frameworks such as ICH, where scientific, ethical, and regulatory expertise converge to produce coherent, widely accepted standards. Without such coordinated guidance, purpose fragmentation will continue to generate avoidable re-consent demands, legal uncertainty, and operational delays, ultimately weakening Europe's capacity to conduct high-quality, cross-border research.

1. Strengthening the six key-indicative factors through public-health-relevant examples

Issue statement

A central weakness in the current Guidelines is that the six key indicative factors for determining whether processing qualifies as scientific research remain too abstract to guide real-world decision-making in public health, surveillance, and long-term cohort research. While the factors are conceptually sound, they are presented at a level of generality that does not reflect the operational realities of research ecosystems that function at population scale, rely on statutory mandates, and evolve over decades. These research domains depend on registries, surveillance systems, and biobanks where data are collected continuously, often without direct contact with individuals, and where secondary use is essential for scientific progress. In such settings, controllers, Ethics Committees, and emerging Health Data Access Bodies under the EHDS must interpret the six factors in contexts that differ fundamentally from project-based, short-term, or individually consented research.

The lack of concrete, domain-specific examples creates significant interpretative gaps across Member States. Without illustrations that reflect the operational realities of public health surveillance, disease registries, and long-term cohort infrastructures, authorities are left to apply the six indicative factors in inconsistent ways. This inconsistency is already visible in practice: divergent readings of what qualifies as "scientific research" hinder secondary use, delay approvals, and leave controllers uncertain about

how to demonstrate compliance. In some jurisdictions, the factors are applied so narrowly that long-term or population-level research risks being excluded altogether; in others, they are interpreted so broadly that they lose their practical value. Both tendencies undermine harmonisation and weaken the broader health research ecosystem.

What is needed is a set of examples that translate each of the six factors into the contexts where scientific research depends on continuity, scale, and statutory mandates. Illustrations drawn from public health surveillance, national disease registries, and longitudinal cohort studies would give controllers concrete guidance, support consistent assessments by Health Data Access Bodies, and ensure that population-level and long-term research are clearly recognised within the GDPR framework. Without such operationalisation, the six factors remain abstract principles rather than usable tools, leaving researchers and regulators without the clarity required to support lawful, high-value scientific research across the Union.

Need for clearer articulation in the Guidelines

The six key indicative factors for determining whether processing qualifies as scientific research are conceptually sound but require additional examples tailored to public health, surveillance, and longitudinal cohort research. To maximise the practical value of the six key-indicative factors, the Guidelines would greatly benefit from concrete examples that reflect the realities of public-health research, surveillance systems, and long-term cohort infrastructures. These research domains operate at population scale, often over decades, and rely on statutory mandates, registries, and biobanks where recontacting individuals is impossible or disproportionate. Without clear, domain-specific illustrations, controllers, ethics committees, and Health Data Access Bodies under the EHDS may interpret the factors inconsistently, leading to fragmentation across Member States and uncertainty for researchers.

Providing concrete examples would promote a harmonised understanding of what constitutes "scientific research" under the GDPR, support consistent decision-making across the EHDS ecosystem, and offer controllers practical guidance to demonstrate compliance. Most importantly, examples grounded in real-world research practice would ensure that long-term, population-level, and public-interest research, essential for public health and scientific progress, is clearly recognised and appropriately supported within the GDPR framework.

We therefore recommend that the Guidelines include domain-specific examples illustrating how each of the six key-indicative factors applies in public-health, surveillance, and cohort-based research. Such examples would help ensure consistent interpretation across Member States, support Health Data Access Bodies in their assessments, and provide controllers with concrete guidance on how real-world studies meet the criteria for "scientific research" under the GDPR.

Key-Indicative Factor	Example	Description
1. Methodical and systematic approach	**A. National cancer registry linkage study**	A national public health institute links cancer registry data with mortality records to evaluate 10-year survival trends, following a predefined statistical analysis plan, registry linkage protocol, and quality-control procedures.
	B. Longitudinal birth cohort follow-up	A cohort established in 1995 continues to collect follow-up data on environmental exposures and chronic disease outcomes. Despite evolving hypotheses, the research follows a structured protocol, governance framework, and documented data-collection methodology.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

	C. Sentinel infectious-disease surveillance	Weekly reporting from sentinel GP practices is analysed using a standardised epidemiological protocol to detect unusual increases in influenza-like illness.
2. Adherence to ethical standards	**A. Secondary use of stored biosamples**	A biobank established for cancer research allows secondary use of stored serum samples for disease profiling under ethics-committee oversight and in line with national biobank legislation.
	B. Surveillance with ethical safeguards	A public health authority conducts antimicrobial-resistance surveillance using pseudonymised laboratory data, overseen by an independent ethics board ensuring proportionality and risk minimisation.
3. Verifiability and transparency	**A. Publication of cohort methodology**	A longitudinal cohort publishes its recruitment strategy, data dictionary, and statistical methods, enabling external researchers to assess reproducibility.
	B. Peer-reviewed validation of algorithms	A research team developing an AI-based early-warning model for sepsis publishes the model architecture, validation metrics, and limitations.
4. Autonomy and independence	**A. Independent public-health analysis**	A national institute analyses vaccination effectiveness using its own methodology, independent of the vaccine manufacturer that supplied the product.
	B. Academic–industry collaboration with independent scientific lead	A university leads a pharmacoepidemiological study using real-world data. Although industry provides funding, the academic team independently defines the research questions, methods, and publication plan.
	C. Independent cohort governance	A cohort's scientific committee—composed of independent researchers—approves data-access requests and ensures analyses are not influenced by funders.
5. Contribution to generalisable knowledge	**A. Long-term trends in chronic disease**	A 30-year cohort study identifies risk factors for diabetes and cardiovascular disease, producing generalisable findings applicable to EU populations.
	B. Surveillance informing public-health policy	Analysis of national vaccination data identifies regional disparities in coverage, informing targeted public-health interventions.
	C. Environmental exposure research	A study linking air-quality data with hospital admissions generates evidence relevant for environmental-health policies.
6. Dissemination of results	**A. Annual epidemiological reports**	A public health authority publishes annual reports on cancer incidence, antimicrobial resistance, or chronic-disease trends.
	B. Public dashboards and open summaries	A national institute provides aggregated, anonymised indicators (e.g., influenza trends, environmental exposures) through public dashboards.

2. Persistent ambiguity around the definition of "purpose" in research creates structural barriers to lawful secondary use

Issue statement

A persistent challenge in applying the GDPR to health research is the lack of a clear, operational understanding of the appropriate granularity of "purpose." In sectors such as human resources or marketing, purposes are routinely defined at a high level, such as "execution of the employment contract" or "marketing activities", with multiple processing operations carried out under that single purpose. By contrast, in the research domain some authorities and organisations treat each research

project, or even the infrastructure hosting health data, as a separate purpose, even when projects fall within the same disease area, methodology, or long-term scientific programme. This approach is disproportionate and conceptually misaligned with the nature of scientific inquiry, which depends on continuity, reuse, and long-term stewardship of data. For public-interest bodies such as Sciensano, whose mandates and purposes are defined in law, the difficulty is even greater: the purpose must follow the legal mandate, yet legislation cannot be amended every time scientific needs evolve, making it challenging to strike the right balance and avoid uncertainty. A more coherent interpretation would allow purposes to be formulated at the level of the scientific domain or statutory mission, for example, "building, maintaining, and reusing health-data infrastructures for cancer research and related diseases", which aligns with EDPB Opinion 3/2019, where clinical trials are considered processing activities rather than standalone purposes. The current lack of clarity has significant downstream effects: controllers are pushed toward repeated re-consenting exercises, long-term infrastructures become difficult to operate, and secondary use is hindered by procedural obstacles that do not enhance data protection. What is needed is a principled, harmonised articulation of how "purpose" should be interpreted in the research context, one that recognises the continuity of scientific inquiry, the legitimacy of broad public-interest research aims, and the safeguards embedded in Article 89. Without such clarification, purpose fragmentation will continue to generate avoidable re-consent demands, legal uncertainty, and operational delays, ultimately weakening Europe's capacity to conduct high-quality, cross-border research.

The practice of classifying every project as a new purpose is an excessive and unjustified expansion of the GDPR's purpose limitation principle.

A harmonised, research-specific interpretation of purpose is needed to reflect the realities of modern scientific and public-health research. Current ambiguity leads to fragmented expectations across Member States and creates operational inertia, where institutions become increasingly risk-averse rather than addressing cross-institutional divergences. A clearer, domain-appropriate definition would reduce unnecessary administrative cycles across privacy, regulatory, and contractual teams while maintaining high standards of data-subject protection. Such an interpretation should explicitly recognise that public-interest research does not always begin from a narrowly defined hypothesis. Many legitimate scientific activities, particularly those involving rich, longitudinal, linked cohort datasets, are inherently exploratory, data-driven, or oriented toward early-warning signal detection. These activities remain anchored in a broader, legally defined public-health mission, even when the specific research questions evolve over time. A coherent definition of purpose should therefore accommodate research that seeks, for example, to identify which disease onsets can be inferred from patterns observed 10, 20, or 30 years earlier, where early intervention could yield substantial population-health benefit. By acknowledging that exploratory analyses, pattern detection, and hypothesis-generation fall within the same overarching scientific purpose as downstream confirmatory studies, the Guidelines would provide a stable governance framework that supports continuity, reuse, and long-term stewardship of health data, which are the core features of high-quality public-interest research.

Need for clearer articulation in the Guidelines

The Guidelines do not clarify:

- Whether each research project constitutes a separate purpose.
- Whether secondary use within the same disease area is one purpose.
- How to avoid unnecessary re-consenting due to purpose fragmentation.

Concrete proposals

To avoid fragmentation and unnecessary re-consenting, the EDPB should clarify that, for the purposes of Article 5(1)(b), scientific research within a defined field, research infrastructure, disease area, or

public-health mandate constitutes a broad, overarching purpose. Research activities carried out within this same overarching scientific purpose, such as follow-up studies, additional analyses, or method improvements, should not be treated as new purposes requiring re-consent, provided that Article 89(1) safeguards are applied and the processing remains compatible with expectations at the time of data collection. Re-consent should not be required where recontacting individuals is impossible or disproportionate, where the research remains within the same overarching purpose, and where ethical oversight and robust safeguards are in place.
We propose new wording for the Guidelines:

> *"For the purposes of Article 5(1)(b), scientific research should be understood as a broad, overarching purpose. Research activities conducted within the same research infrastructure, disease area, or public-health mandate should not be considered new purposes requiring re-consent, provided that appropriate safeguards under Article 89(1) are in place and the processing remains compatible with the expectations established at the time of data collection."*
>
> *"Re-consent should not be required where recontacting individuals is impossible or disproportionate, where the research remains within the same overarching scientific purpose, and where ethical oversight and robust safeguards are applied."*

Why this solution is necessary:

- Prevents fragmentation across Member States.
- Avoids unnecessary re-consenting that is impossible in long-term or population-level research.
- Aligns GDPR with EHDS, CTR, and public-health mandates.
- Supports continuity of registries, cohorts, and biobanks.
- Reflects scientific reality: research evolves, but the purpose often remains the same.

Concrete examples from public health research

Topic	Proposed EDPB Clarification	Rationale	Example
1. Not every research project is a separate purpose	A new research project does **not** constitute a new purpose when all the below apply: • falls within the same overarching scientific aim, • uses data from the same research infrastructure (cohort, registry, biobank), • is conducted under the same governance and safeguards, • remains compatible with expectations at initial data collection.	Prevents artificial fragmentation of "purposes" in long-term research ecosystems; aligns with scientific practice where multiple analyses serve one overarching aim.	A cancer cohort established to study long-term health outcomes performs multiple analyses over 20 years (e.g., cancer incidence, environmental exposures). These are **sub-purposes**, not new purposes.
2. Secondary use within the same disease area or research domain is one purpose	Secondary use of data within the same disease area, research domain, or public health mandate should be treated as **one purpose**, provided safeguards under Art. 89(1) are in place.	Ensures continuity of disease-specific research; avoids unnecessary administrative burden; supports public health monitoring.	A national cancer registry uses the same dataset to study survival, treatment effectiveness, late effects, and regional disparities. These fall under the overarching purpose of **cancer epidemiology**.

3. Mechanism to avoid unnecessary re-consenting	Re-consent should **not** be required when: • the new activity is compatible with the original purpose, • recontacting individuals is impossible or disproportionate, • research is under ethical oversight, • safeguards (pseudonymisation, secure environments) are applied.	Aligns with Art. 5(1)(b), Art. 89(1), Recital 33 (broad consent), Recital 50 (compatibility), and Helsinki Art. 32. Supports the feasibility of long-term and population-level research.	A biobank collected samples in 1998 for cancer research. A 2026 genomics study aims to identify hereditary risk factors. Re-contact is impossible. Under Art. 89(1) and Recital 33, **re-consent is not required**.

3. Overestimate the feasibility of consent-based models in long-term, population-level research infrastructures

Issue statement

One positive contribution of the Opinion No 3/2019[1] by the EDPB consists in stressing out the fact that the obligation for informed consent pursuant to clinical research should be distinguished from consent as one of the possible grounds for the processing of personal data under the GDPR. As highlighted in other reports on Opinion 3/2019, presenting subjects with multiple consents that comply with different laws could be confusing for clinical trials participants[2], hence special attention must be paid to the communication between sponsors/investigators and patients in this regard. Moreover, the EDPB and the EU Commission show a clear preference towards the use of other legal bases for the processing of personal data in the context of clinical trial (namely, public interest or the legitimate interest of the controller) rather than relying on consent. And the limits of consent as a legal basis for processing data in clinical research were clearly highlighted (not granular enough, not feasible for research, patient population is vulnerable, consent requires active yes/no tick-boxes, etc..).

However, several crucial topics that are related to the matters discussed in the documents, have been omitted. Among those falls the importance of the One-stop-shop mechanism (hereinafter "OSS") for pan-European clinical research. More specifically, the influence that the choice of the legal basis for the processing of personal data has over whether OSS will apply, or not. In our view, it would be a welcomed development if the EDPB choses to issue further guidance on the issues pertaining to the OSS and the choice of the legal basis for international research activities. The GDPR is lauded for introducing the OSS. The mechanism's rationale is that controllers who conduct cross-border processing of personal data[3] benefit from dealing with a single point of contact (lead supervisory authority[4]) within the EU.

Based on further guidelines for identifying a controller or processor's leading supervisory authority, it is clear, a clinical research open in several Member states, would fall within the scope of these provisions. This reflects the unification and simplification which are proclaimed to be at the heart of the

[1] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf
[2] EDPB issues new opinion on interplay between Clinical Trials Regulation and the GDPR | Data Protection Report
[3] *Article 4(23) GDPR defines cross-border processing of personal data as either "processing of personal data which takes place in the context of the activities of establishments in more than one Member state of a controller or processor in the Union, where the controller or processor is established in more than one Member state", or "processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to affect data subjects in more than one Member state".*
[4] *Article 56 GDPR defines it as the Supervisory authority of the main establishment or of the single establishment of the controller or processor.*

data protection reform. The involvement of several data protection authorities (DPAs) may generally lead to confusion for controllers, conflicts of competence, and uncertainty for data subjects. When analysing the possible legal bases for data processing in the context of a clinical research, of major importance is Recital 128 GDPR, pursuant to which the rules on OSS do not apply where the processing is carried out in the public interest. Further to the Recital 128 GDPR, art 55.2 specify that the notion of the lead supervisory authority (specified in the art.56) does not apply where the processing is carried out in the public interest or when processing is necessary for compliance with a legal obligation. So, choosing the public health or compliance with legal obligation as the legal basis in international led clinical research comes with challenges. First, each member state can further specify conditions which allows to rely on this legal basis, which may not be possible to meet in all concerned countries. Secondly, such legal basis is not compatible with the OSS mechanism.

This means that the data controller would not be able to benefit from a lead supervisory authority in the following cases:

i) Processing of personal data for reliability and safety purposes, where the correct legal basis has been identified unanimously by EDPB and the EU Commission as Article 6(1)(c) in conjunction with Article 9(2)(i) of the GDPR;
ii) Processing operations related to research activities, if one of the following legal bases is chosen by the controller: Article 6(1)(e) in conjunction with either Article 9(2)(i) or (j).

It follows from the foregoing that the legal basis that is left to be the most preferable, is Article 6(1)(f) (legitimate interest) in conjunction with Article 9(2)(j) (scientific research). By choosing it, the data controller would have access to the OSS mechanism concerning the processing of personal data when it is related to research activities.

Further, there is a need to clarify what are other consequences of choosing legal basis which does not benefit from OSS, including just for one international project. Does this means that DPO shall be notified and data breaches are to be reported to all MS's DPAs separately and this just for the sake of one project? What about transversal breaches, which will touch to several activities relying on different basis? Shall the same breach be reported through OSS and in parallel to all other MSs?

In case of the use of consent as legal basis, more clarification is needed in relation to the interpretation of the Article 14.2.d which states that in case of withdrawal, "the lawfulness of processing based on consent before its withdrawal" is not affected. However, in research some processing activities cannot stop, such as safety reporting or archiving for several years after the end of the study. These activities can be based on a different legal basis. However, if processing of data in a clinical research is based on the consent and patients withdraw consent at the late stage of data maturation, can data be still included in the final analysis? Or, can the results of the interim analysis still be re-done to verify the correctness of it using the same dataset if some patients withdrew consent thereafter. Can this dataset be used for some types of the secondary use based on a different legal basis? For example, in the scope of inspection or audit, which is a different processing activity?

Taking an example of a research project which will collect datasets from different EU countries (i.e. form registries) and provided the current heterogeneous interpretation, we may face situations where national subsets would be processed based of different legal basis within the same research project by the same data controller. In this case, not only it became more and more challenging to conduct international studies, but it creates inequalities between patients from different countries in the way their rights are executed. Indeed, different legal basis comes with different application of rights for the data subjects.

A significant gap in the current Guidelines is the assumption that re-contacting individuals is generally feasible and that consent, whether broad or dynamic, can realistically function as a primary legal basis for scientific research across the full lifecycle of long-term, population-level data infrastructures. This assumption does not reflect the operational realities, where clinical research, public health surveillance, disease registries, and long-term cohort studies often span decades, involve multiple generations of data subjects, and rely on datasets collected under statutory mandates or through heterogeneous historical pathways. In these contexts, the possibility of re-contacting individuals is frequently limited not by lack of effort, but by structural constraints: participants may be deceased, lost to follow-up, untraceable due to outdated contact details, or never directly contactable in the first place because the data originated from administrative systems, hospital records, or national registries rather than direct enrolment.

Secondary use of data is often essential for scientific progress, yet re-consent is not feasible in many cases: patients are either lost to follow-up, dead or purely not interested, and insisting on re-contact can render further research impossible or not feasible. This is particularly true for public health bodies operating under statutory mandates, where the purpose of processing is defined in law and where the GDPR explicitly provides alternative legal bases, notably Article 6(1)(e) in conjunction with Articles 9(2)(i) and 9(2)(j). The Guidelines, however, do not sufficiently acknowledge these structural limitations, nor do they provide a realistic framework for how controllers should proceed when re-contact is impossible or disproportionate. As a result, consent is implicitly framed as a default expectation, even in settings where the GDPR itself anticipates that public interest or scientific research legal bases will be more appropriate.

This lack of clarity has practical consequences. Ethics Committees, already struggling with the blurred boundary between ethical and data-protection oversight, often interpret the Guidelines as requiring re-consent for any new research purpose, even when this contradicts the GDPR, the Helsinki Declaration, or national research laws. Controllers are left navigating inconsistent expectations across Member States, with some authorities insisting on consent-based models and others recognising the legitimacy of public-interest or legitimate interest legal bases. The result is fragmentation, delays, and legal uncertainty, precisely the challenges that in many instances block the research. Moreover, the Guidelines' emphasis on dynamic consent does not account for the fact that such models presuppose stable digital infrastructures, ongoing participant engagement, and the ability to maintain up-to-date contact information, conditions that are rarely met in large-scale, population-level research systems.

The outcome is sustained fragmentation, procedural delays, and significant legal uncertainty, which in practice operate as direct barriers to the conduct of research.

Need for clearer articulation in the Guidelines

The Guidelines recognise broad and dynamic consent, but still assume that re-contact is generally feasible and that consent can realistically be the main legal basis in long-term, population-level infrastructures.

> *"Where the purposes of research are not fully known… it is possible… to rely on… broad consent… Controllers can also ask data subjects to consent to different individual research projects… as soon as the purposes… become known (so-called dynamic consent)."*

What is missing is an explicit recognition that consent-based models cannot serve as the backbone of long-term scientific research in public health and epidemiology. The GDPR already provides a coherent legal architecture for these contexts, grounded in public interest and scientific research provisions, combined with Article 89 safeguards. The Guidelines should reflect this reality by acknowledging that the impossibility or disproportionality of re-contact is not an exceptional circumstance but a structural feature of many research ecosystems. Without such clarification, controllers remain exposed to

inconsistent interpretations, and essential research risks being hindered by expectations that are neither legally required nor operationally feasible. In public health surveillance, registries, and long-term cohort linkages, re-contact is often *impossible, disproportionate, or ethically undesirable* (e.g. deceased persons, decades-old data, large national registries).

Concrete proposals

- **Explicitly recognise structural limits of re-contact**: add a subsection stating that in:
  - statutory public health surveillance,
  - national disease registries,
  - long-term cohorts with loss to follow-up, re-contacting individuals for each new study is often *disproportionate* under Article 14(5)(b) and Recital 62, and that reliance on **Article 6(1)(e) + 9(2)(i)/(j)** is normally more appropriate than consent.
- **Clarify that broad consent ≠ operational precondition for research:** state that where Union or Member State law provides a public interest mandate and Article 9(2)(i)/(j) conditions are met, *lack of consent or impossibility of re-contact* does not prevent lawful secondary use, provided Article 89(1) safeguards are implemented.
- **Dynamic consent as optional enhancement, not baseline expectation:** clarify that dynamic consent is a *good practice* where digital infrastructures and stable contact are realistic (e.g. clinical trials, small cohorts), but should not be framed as a default expectation for population-level registries or surveillance systems.

4. Ethical consent vs GDPR consent

Issue statement

A persistent and deeply consequential problem in the governance of clinical research is the ongoing confusion between the remit of Ethics Committees and the responsibilities assigned under the GDPR. Ethics Committees frequently step into areas that are not legally theirs to determine, particularly regarding the choice of legal basis for processing personal data and the conditions under which secondary use may occur. Since the entry into force of the GDPR, many ECs have begun to impose GDPR consent as the legal basis for research, including in situations where this contradicts the recommendations of the EDPB, national data-protection authorities, or even the practical realities of long-term research. Ethics impose the legal basis (usually consent) for processing personal data in scope of research and in particular, the requested re-consent of the patient in case of secondary use, even though the GDPR assigns this responsibility exclusively to the controller. This tendency is not malicious; it is a symptom of a regulatory vacuum. Because the interface between ethical oversight and data-protection compliance has never been clearly articulated at EU level, ECs are left to fill the gap, often by default rather than by design.

In many instances, and often by necessity due to the absence of clear national guidance, Ethics Committees end up determining the practical legal basis for research activities, even though this responsibility formally lies elsewhere. This situation reflects the persistent uncertainty surrounding the interface between ethical and data-protection frameworks.

The current guideline remains vague and leaves substantial room for divergent interpretations, particularly regarding the respective roles of ethics committees and data-protection authorities. A clearer, jointly developed interpretation is needed. In collaboration with representatives of ethics committees, the EDPB should articulate a shared, operational statement and ensure that training is provided in both directions once agreed. A central element of this clarification must be the distinction between ethical consent and GDPR consent. Ethical consent concerns participation in research under ethical standards, while GDPR consent is a lawful basis for processing personal data under data-protection law. These are not interchangeable concepts. Clarifying this distinction at both EU and

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

national levels would promote consistent interpretation and reduce the current reliance on ethics committees to fill regulatory gaps that fall outside their mandate.

The Guidelines acknowledge ethical standards but do not yet provide sufficient clarity on how these interact with data-protection requirements. In practice, **Ethics Committees often end up determining the effective legal basis for research**, largely because national guidance is limited or absent. This situation creates inconsistency and uncertainty across Member States.

Need for clearer articulation in the Guidelines

To address these issues, the EDPB should provide explicit clarification of the respective roles of Ethics Committees and data controllers. The Guidelines should affirm that ECs are responsible for ethical and scientific oversight, not for determining the legal basis for processing personal data or for imposing GDPR-specific requirements. They should clearly distinguish between ethical consent and GDPR consent, explaining that the former governs participation in research while the latter is only one possible legal basis for processing. The Guidelines should clarify that re-consent is not required for secondary use when it is impossible or disproportionate, provided that Article 89 safeguards and ethical oversight are in place. They should also state that technical and organisational measures, including the level of pseudonymisation, are determined by the controller based on a risk analysis, and that ECs may comment on ethical implications but should not impose technical requirements. Finally, the Guidelines should encourage Member States to harmonise the interaction between ECs and DPAs and support the development of a sector-specific code of conduct for GDPR in clinical research. Such a code would provide a stable, predictable framework that clarifies roles, reduces fragmentation, and supports responsible secondary use of data.

To ensure coherence, the Guidelines should explicitly distinguish between:

- **GDPR consent**: a *legal basis* under Articles 6 and 9, characterised by voluntariness, revocability, and absence of imbalance; and
- **Research or ethical consent**: a *participation agreement* governed by frameworks such as the Helsinki Declaration, the Clinical Trials Regulation, and biobank laws, which may allow waivers, deferred consent, or opt-out mechanisms.

At the same time, the Guidelines should recognise the practical reality that, in scientific and public-health research, a participant's agreement to take part in a study (Helsinki consent) necessarily implies acceptance that their data will be processed for that study. Requiring two separate tick boxes, one for participation and one for GDPR consent, creates confusion, risks inconsistent choices, and may render full participation infeasible if a patient agrees to the study but inadvertently declines data processing. To avoid this contradiction and ensure clarity for participants, we recommend allowing a single, integrated statement in patient-facing materials, such as*: "If you agree to participate in this study, you also accept that your data will be processed for this research."* Legal instruments should be adapted to the realities and feasible to implement and enable research.

The EDPB should clarify that:

- How to separate ethical review from data protection assessment.
- Ethics Committees are not competent to impose or determine GDPR legal bases; their role concerns ethical oversight, not data protection law.
- Ethical consent and GDPR consent serve different purposes and should not be conflated in templates or review processes.
- Secondary use of data should be permissible without re-consent when recontacting individuals is impossible or disproportionate, provided Article 89(1) safeguards and ethical oversight are in place.

The EDPB should clarify that the separation between ethical review and data-protection assessment must be **handled primarily by controllers, ethics committees, and data-protection experts**, not by placing additional informational or decision-making burdens on patients. Ethical review and GDPR compliance are distinct processes: ethics committees assess scientific merit, proportionality, and participant welfare, while they are not competent to impose or determine GDPR legal bases, which fall under data-protection law. Likewise, ethical consent and GDPR consent serve different purposes and should not be conflated in templates or review processes; however, this distinction must be implemented in a way that remains **simple, comprehensible, and respectful** of how patients actually experience consent. Patients consistently report that they do not want to navigate complex legal distinctions or receive multiple overlapping documents; they want clarity, trust, and reassurance that institutions are taking responsibility. Because **controllers remain ultimately responsible** under the GDPR, consent materials and information processes must be feasible for them to implement in practice and **should not be constrained by ethics committee requirements** that impose unjustified or inconsistent obligations that the controllers cannot operationalise. Therefore, consent materials should be co-developed with all relevant stakeholders, including controllers, ethics committees, and patient representatives, to ensure that information is accurate, proportionate, realistically implementable and genuinely patient-friendly. This approach avoids overwhelming individuals with unnecessary legal distinctions, prevents the multiplication of documents that patients neither want nor benefit from, and ensures that responsibilities remain with the institutions best placed to carry them. Finally, the Guidelines should further confirm that secondary use of data may proceed without re-consent when recontacting individuals is impossible or disproportionate, provided that Article 89(1) safeguards and appropriate ethical oversight are in place. This approach protects individuals' rights while avoiding unnecessary procedural burdens that do not benefit patients and may undermine the feasibility of high-quality research.

The independence of these two assessments must be explicitly reaffirmed. Their current conflation is not a minor procedural inconvenience but one of the principal structural obstacles to efficient and legally sound research governance.

Aspect	Research consent	GDPR consent
Form	written consent in many (but not all) areas, dated and signed (ICH-GCP)	any, including oral or by ticking a box or just by providing the data
Explicit/implicit	opt-out allowed in some areas (in bio-banking)	explicit (no opt-out)
Existence of exemptions	yes, provided EC approval (art 32 Helsinki declaration) or deferred consent (emergency)	no (different legal basis shall be used)

Concrete proposals: clarify that compliance with GDPR is different from the need to comply with ethical and legal framework applicable to research.

- **Dedicated box: "Two different consents"**: add a boxed explanation that:
  - research participation consent is governed by ethics and sectoral law (CTR, Oviedo, national research acts),
  - GDPR consent is *only one* possible legal basis and often *not appropriate* in hierarchical or public-interest settings (e.g. public health institutes, registries).
- **Explicitly discourage conflation in templates:** recommend that information sheets and forms:
  - clearly separate "consent to participate in research" from "legal basis for data processing",
  - avoid presenting GDPR consent where Article 6(1)(e) or 6(1)(f) is actually relied upon.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

- **Clarify impact of withdrawal:** explain that withdrawal of *research* consent does not automatically require erasure of all data if further processing is necessary for public interest research under Article 17(3)(d) and Article 89(1), provided that erasure render impossible or seriously impair the achievement of the objectives of that processing and this is transparently communicated.

5. PUBLIC INTEREST as legal basis

Issue statement

A key shortcoming of the current Guidelines is the limited attention given to how **"public interest"** should be defined and operationalised as a legal basis for processing personal data for scientific and public-health research. Although sometimes treated as flexible or open-ended, public interest is **not** an undefined concept. Under the GDPR, Articles 6(1)(e), 9(2)(j) and 89 require that the **existence, scope, and conditions** of a public-interest task be **laid down in Union or Member State law**.

In practice, this means controllers cannot simply invoke public interest at their discretion: the legal basis must be **explicitly established in national legislation**, including the safeguards, limits, and conditions under which research may rely on it. Instruments such as the EHDS may offer a non-exhaustive list of purposes that *may* fall under public interest, but they **do not replace** the requirement for Member States to define this basis in law.

Context and practical implications

A concrete example of predictable and harmonised operationalisation is provided by the **French Méthodologies de Référence (MRs)** issued by CNIL. These frameworks define predefined conditions under which certain categories of health-data research are presumed to be in the public interest, subject to strict requirements such as:

- clearly defined research purposes
- data minimisation
- independent ethical oversight
- transparency obligations
- limits on reuse

This demonstrates that public interest **can** be structured in a way that avoids arbitrary interpretation while supporting responsible research.[5]

The Guidelines currently acknowledge the role of public interest but do not sufficiently clarify how the **sector-specific GDPR application law (EHDS)** interacts with the GDPR. The EHDS should be understood as an **operational layer** that identifies categories of secondary use and establishes procedural mechanisms for access and reuse; **not** as a redefinition of the legal concept of public interest, which remains grounded in the GDPR and national law.

Need for clearer articulation in the Guidelines

To ensure coherence and reduce fragmentation, the Guidelines should explicitly set out what Member States must specify when establishing public-interest legal bases for research. This should include:

- which stakeholders may rely on the legal basis (public bodies, accredited research institutions, private entities under defined conditions)
- criteria for determining when a research activity qualifies as being in the public interest
- requirements for assessing the relevance, necessity, and societal benefit of the research question
- mandatory safeguards and oversight mechanisms
- conditions for data sharing and reuse
- clarify what it means to be "authorized by law" to rely on Article 6(1)(e).
- avoid the current ambiguity that leaves institutions dependent on ethics committees or DPO interpretations.

[5] https://www.cnil.fr/fr/methodologie-de-reference-mr-003-recherches-dans-le-domaine-de-la-sante-sans-recueil-du-consentement

- emphasize that public interest should be defined at EU level, not left to fragmented national laws.

Clarification on the use of Article 6(1)(e) GDPR (Public Interest) in health research

The Guidelines should explicitly recall that Article 6(1)(e) GDPR ("processing is necessary for the performance of a task carried out in the public interest") may only be relied upon when the task is *defined in Union or Member State law*. This requirement is stated directly in the legal text: "…the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." "The basis for the processing shall be laid down by Union law or Member State law." *(Article 6(1)(e) and Article 6(3) GDPR)*

This means that controllers may rely on public-interest research as a legal basis only when the national legal framework explicitly covers the research task or mandate. The Guidelines should therefore encourage Member States to ensure that their national laws clearly define which research tasks fall under public interest, to avoid fragmentation and legal uncertainty, and moreover also align in requirements and definitions with the other MSs.

Of note, Article 35(10) GDPR specifies that when processing is based on such a legal basis and the law already provides for a general DPIA in the context of the adoption of the legal basis, hence, the controller does not need to conduct an additional DPIA, but must comply with all conditions and safeguards laid down in that law.

Operational limitation: absence of the one-stop-shop mechanism

A practical constraint must also be highlighted: relying on public interest as a legal basis **excludes the GDPR one-stop-shop mechanism** (Recital 128). This has significant operational implications for cross-border research and secondary use of health data, as controllers may face multiple supervisory authorities and divergent national interpretations. Clearer guidance from the EDPB would support harmonisation and reduce fragmentation across Member States.

6. Transparency obligations for long-term scientific research remain insufficiently operationalised

Issue statement

A central gap in the current Guidelines concerns the practical implementation of transparency obligations for public bodies that process personal data for scientific research over long periods of time. While the Guidelines acknowledge that controllers must ensure transparency "during the entire processing period" and that processors may provide information on behalf of controllers, they stop short of offering operational models for institutions with statutory mandates, large legacy datasets, and population-level research infrastructures. This omission is particularly significant for public health bodies, which often hold datasets collected over decades, sourced from multiple registries, laboratories, hospitals, and administrative systems. For these actors, individual notification is frequently impossible or would require disproportionate effort, yet the Guidelines do not provide concrete criteria for when Article 14(5)(b) may be relied upon, nor do they describe what alternative transparency mechanisms are expected in such contexts.

In many research settings the Controller does not have access to contact details because the data are pseudonymised in accordance with the safeguards required under Article 89(1) GDPR. Re-identification for the purpose of re-contacting individuals would undermine these safeguards and is often technically or legally impossible. For this reason, we strongly disagree with paragraphs 77, 86, 87 and 88 of the EDPB proposal, which appear to assume that re-contact is feasible or appropriate in contexts where

pseudonymisation is deliberately implemented to protect data subjects. Of note, when datasets are transferred in a sufficiently de-identified or pseudonymised form, the receiving Controller can legitimately rely on Article 11(1) and Article 14(5)(b) GDPR. These provisions recognise that, where the Controller cannot identify data subjects, and identification is not required for the processing, the Controller is not obliged to obtain or retain additional identifiers solely to comply with other GDPR obligations.

The absence of practical guidance leaves public bodies in a structurally ambiguous position. On the one hand, they are expected to maintain high levels of transparency for all processing activities, including secondary use, linkage, and long-term retention. On the other hand, they lack a clear, endorsed model for how to meet these obligations when direct communication with millions of individuals is infeasible. The Guidelines also fail to clarify how processors in a clinical trial conducted by another Sponsor, or initial controllers in a data-transfer or data-sharing arrangement, such as hospitals, laboratories, and diagnostic centres, can act as communication channels for data-subject requests without being inadvertently reclassified as joint controllers. In practice, these entities often hold the identifying information needed to relay requests, while the Sponsor or receiving controller processes only pseudonymised data. Without clear guidance, the act of facilitating communication may be interpreted as influencing the purposes or essential means of processing, thereby creating a risk of unintended joint controllership. In practice, these entities are often the only realistic point of contact for individuals, yet the fear of inadvertently altering controllership roles leads to inconsistent practices and unnecessary caution. As a result, transparency obligations risk becoming either under-implemented or implemented in ways that create legal uncertainty for both controllers and processors.

Specifically, under the GDPR, an entity risks being considered a joint controller when:

- it determines the means or purposes of processing, even partially
- it participates in decisions about how personal data are handled
- it goes beyond a purely technical or operational role

In clinical research, this risk appears when:

- a hospital, lab, or diagnostic centre decides how to handle data-subject requests,
- or determines whether, when, or how to re-identify individuals,
- or interprets the scope of the research purpose or the lawful basis,
- or makes discretionary decisions about what information to pass on to the Sponsor.

Even if unintentionally, these actions can be interpreted as influencing the purpose or essential means of the processing. This is why the lack of clarity in the Guidelines creates legal uncertainty: entities that *must* act as communication channels (because they hold the identifiers) fear being reclassified as joint controllers simply for relaying requests.

Need for clearer articulation in the Guidelines

The Guidelines acknowledge that processors may provide information on behalf of controllers and that exceptions under Article 14(5) exist, but they do not give *operational models* for public bodies with statutory mandates and large, legacy datasets.

> *"If controllers process personal data for long periods of time for scientific research purposes, then they should adopt appropriate measures to ensure transparency during the entire processing period."*

What is missing is a structured, realistic framework that recognises the operational realities of public health research. Public bodies need clarity on how to maintain transparency across decades-long processing cycles, how to communicate effectively with populations they cannot directly reach, and how to rely on Article 14(5)(b) without fear of non-compliance. They also need assurance that processors can support transparency, for example, by providing information at the point of care or handling access and erasure requests under documented instructions, without this being interpreted as joint determination of purposes and means. Without such guidance, the transparency obligations risk being interpreted in ways that are either excessively burdensome or practically unachievable, undermining both legal certainty and public trust.

Concrete proposals

- **Model "layered transparency" for public health bodies:** recommend a layered approach for institutions like Sciensano:
  - **Primary layer:** public, continuously updated web portal describing all main research programmes, data sources, safeguards, and rights.
  - **Secondary layer:** registry- or study-specific pages, with lay summaries and contact points.
  - **Tertiary layer:** on-demand detailed information via central contact (DPO/research office).
- **Clarify acceptable reliance on Article 14(5)(b):** provide criteria for when individual notification is "impossible or would involve a disproportionate effort" in population research, e.g.:
  - very large cohorts/registries,
  - outdated contact details,
  - linkage of multiple administrative sources, combined with robust public communication and easily accessible information.
- **Processors as communication channels**: confirm that hospitals, labs, or other processors may:
  - provide information at point of care,
  - handle access/erasure requests on behalf of the controller, under documented instructions, without becoming joint controllers.

7. Proportionality and legitimate interest assessment (LIA)

Issue statement

A significant gap in the current Guidelines is the absence of a structured, research-tailored approach for applying legitimate interest as a legal basis for scientific processing. Although the Guidelines acknowledge that genuine scientific research carries "significant weight" in a legitimate interest assessment, they stop short of providing a methodological framework that reflects the complexities of research practice. This omission is particularly striking given the challenges in the sector of public health and clinical research where controllers already face fragmented interpretations of legal bases, inconsistent expectations from Ethics Committees, and uncertainty about how to justify the necessity and proportionality of processing in long-term, multi-stakeholder research environments.

In clinical and public health research, controllers routinely process sensitive data for purposes that evolve, require linkage across datasets, and depend on maintaining identifiable or pseudonymised information to ensure scientific validity, minimise bias, and enable follow-up. Without a research-specific LIA structure, controllers are left to adapt generic templates that do not capture the scientific rationale, methodological constraints, or safeguards already defined in this sector. This lack of tailored guidance increases the risk of inconsistent assessments across Member States, reinforces the already-documented fragmentation in GDPR interpretation, and leaves controllers exposed to challenges from Ethics Committees or DPAs who may not share a common understanding of how legitimate interest applies in research.

Health research often operates within hybrid governance models, involving public bodies, academic institutions, private partners, and international collaborators, where the choice between Article 6(1)(e) and 6(1)(f) is not always straightforward. In the absence of clear criteria, controllers may default to consent even when it is inappropriate or unworkable, or they may avoid legitimate interest altogether due to fear of inconsistent scrutiny. This dynamic exacerbates the legal uncertainty already affecting secondary use, long-term follow-up, and methodological innovation. A research-specific LIA framework would not only support controllers in documenting their reasoning but would also promote harmonisation, reduce unnecessary reliance on consent, and provide regulators with a consistent basis for evaluating research activities.

Need for clearer articulation in the Guidelines

The Guidelines would benefit from a clearer and more operational articulation of how Article 6 and Article 9 GDPR must be combined when processing sensitive data for scientific research. As currently drafted, the document places disproportionate emphasis on consent-based models, including broad and dynamic consent, even though the GDPR itself recognises that consent is rarely a feasible or reliable legal basis in research involving vulnerable populations, long-term follow-up, multi-stakeholder infrastructures, or secondary use. This approach risks reinforcing the very fragmentation the Guidelines seek to remedy. In practice, research sponsors and infrastructures need legal bases that are stable, scalable, and compatible with cross-border governance. The legitimate interest under Article 6(1)(f), combined with Article 9(2)(j) for scientific research, is often the only workable basis that both preserves the one-stop-shop mechanism and reflects the real operational conditions of research. Legitimate interest is explicitly recognised in the Guidelines as a valid ground for scientific research, and the EDPB acknowledges that genuine research carries significant societal weight in the balancing test. The Guidelines should therefore clarify when and how controllers may rely on this combination, and provide concrete criteria for distinguishing research-motivated legitimate interests from commercial product development. Such clarification would support harmonisation, reduce unnecessary reliance on consent, and offer a proportionate, risk-based pathway that aligns with the GDPR's architecture and with the needs of modern research ecosystems.

The Guidelines acknowledge that scientific research can be a legitimate interest and that "significant weight" can be given to it, but they do not provide a *research-specific LIA framework*.

> *"A controller that intends to process personal data for scientific research purposes on the basis of legitimate interest can often attribute significant weight to the processing… because genuine scientific research is considered… beneficial for the whole of society."*

What is missing, therefore, is a structured, operational model that translates the legitimate interest test into the realities of scientific research, one that recognises scientific validity, public value, methodological necessity, and the role of safeguards as integral components of the assessment. Without such a framework, legitimate interest remains theoretically available but practically under-used, contributing to the broader uncertainty that continues to hinder lawful, high-quality research across the Union.

Concrete proposals

- **Clarification on the roles and responsibilities:** the responsibility for conducting and documenting the Legitimate Interest Assessment (LIA) must remain with the researcher or sponsor acting as the data controller. Regulatory bodies and ethics committees are responsible for evaluating the overall research protocol, including its ethical soundness and the protection of participants' rights, but they should not prescribe or impose how the LIA itself is performed.
- **Understanding and documenting the reasonable expectations of data subjects:** this is a core element of the balancing test in a Legitimate Interest Assessment. In scientific and clinical

research, this assessment must reflect the **specific context of data collection**, the **nature of the relationship between participant and controller**, and the **foreseeability of secondary use**. This step is often poorly understood and inconsistently applied, leading to unnecessary re-consent demands, misinterpretation by ethics committees, and fragmentation across Member States.

Specifically, a research-specific LIA must include a clear and well-reasoned assessment of the reasonable expectations of data subjects, grounded in the context in which their data were originally collected. Controllers should document the nature of the initial interaction with participants, the information provided at the time (including any reference to future scientific use), and the extent to which further processing within the same disease area, research programme, or public health mandate would have been foreseeable. This assessment should also consider the time elapsed since collection, changes in legal or technological context, and whether re-contact is feasible or appropriate in long-term or population-level research. Expectations must be evaluated in light of the relationship between participant and controller, such as clinical trial sponsors, healthcare providers, registries, and public health authorities each create different baselines of trust and foreseeability. Controllers should capture this reasoning in the LIA, DPIA, and Record of Processing Activities, demonstrating how transparency materials, ethical oversight, pseudonymisation, and secure environments ensure that secondary use aligns with what individuals can reasonably anticipate in a regulated research setting.

- **Research-tailored LIA template**: suggest that for Article 6(1)(f) in research, controllers explicitly assess:
  - **Interest:** scientific validity, public value, alignment with recognised research integrity standards (e.g. https://allea.org/code-of-conduct/).
  - **Necessity:** why identifiable/pseudonymised data are needed (e.g. linkage, follow-up, bias control).
  - **Balancing:** risk factors (vulnerability, stigma, data sensitivity) vs safeguards (pseudonymisation, secure environments, ethics oversight, PETs).
- **Proportionality as cross-cutting principle** Encourage explicit documentation of:
  - data minimisation choices (variables, sample size),
  - access controls (role-based, time-limited),
  - publication safeguards (aggregation, suppression).
- **Clarify when LIA is *not* appropriate**: indicate that for statutory public health tasks, Article 6(1)(e) is normally more appropriate than 6(1)(f), while LIA may be suitable for:
  - public-private partnerships,
  - method development,
  - exploratory analyses outside a strict legal mandate.

8. Lack of operational clarity on documenting and applying the presumption of compatibility for scientific research

Issue statement

In our understanding, GDPR provides three key mechanisms for further processing:

i) Consent
ii) Union and/or National law (which itself can provide legal basis for further processing as per Recital 50 GDPR)
iii) Compatibility of purposes

Given that re-consenting is not always feasible in clinical research context, due to the -mentioned reasons, compatibility of purposes can serve as another option. This, in our view, implies that the

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

controller, in order to enable further processing, is required to justify the compatibility of the initial and secondary purposes of processing. However, this aspect still raises debate in the view of the statement of the Article 5.1.b as some interpretations suggest it releases data controllers from the need to perform the compatibility test. This point of view is supported by the Recital 50 GDPR which states that in case of successful compatibility test, separate legal basis is not required, but at the same time clarifies that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations". Clarification of this element would help sponsors to understand applicable requirements.

Last but not least, the Recital 50 GDPR may suggest that the need for compatibility test may differ from the legal basis used initially (not required in case of the initial consent followed by important objectives of general public interest versus required in case of legitimate interests initially used).

1. **A link between initial and secondary purposes of processing**: the term 'link between purposes may have different interpretations and seems to be quite broad and vague. From our point of view, establishing a link between initial and secondary purposes can be a major indication of their compatibility and thus the main criterion in the compatibility methodology. The more purposes are related and connected to each other, the bigger the chance they are compatible, regardless of the following four criteria. This topic is in relation to the previous considerations about the granularity of purposes. The question that arises here is how different the purposes should be to measure the "distance" between them. In the research environment, it is not always possible to predict further projects of research and thus the need for further processing. For instance, at the stage of data collection, no one can anticipate what exactly tests/analyses will be performed on patients' data. Hence, an "encapsulated", broader purpose of processing should be allowed in our view.

2. **The context of data collection**: the question to ask here is whether the further processing will take place in the same context as the data collection. We believe that providing illustrative examples of contexts to be considered would be helpful to the research community. By context, we understand, for example, the use of data for commercial purposes versus non-commercial purposes. Again, transparency is the key, and researchers shall be able to inform data subjects from the onset about all possible processing activities that can be made, eventually providing some choices where relevant. Narrowing the scope of information provided to data subjects from the onset is not transparency and is detrimental to both data subjects and to the research and ultimately the EU capacity of innovation.

3. **The nature of personal data:** healthcare research always use special categories of data. However, it may also use genetic data. Currently many countries limit the possibilities of use of genetic data considerably and in a very divergent way (based on the article 9.4); this without making any distinction between the type of the data at stake (somatic mutations versus germ line mutations, primary DNA sequence versus results of analysis of the status of a single frequent mutation etc...). This approach is detrimental to research and does not always correspond to any higher protection of data subjects. In our view, there is a need to apply a risk-based approach and all genetic data shall not be treated the same, some do not present more risk as compared to any other health data, others do. On the other hand, data as rich as the primary sequence, whereby less than hundred pairs of nucleotides make it unique, are not eye readable to make any sense of them. "Reading" genetic data requires highly sophisticated specialised software, which in a way protects them.

4. **Consequences of the intended further processing (risk assessment):** there should be a balance made between negative and positive or rather beneficial consequences for data subjects. Examples of positive consequences can be development of effective and acceptably safe medicines or a sense of contribution to innovation aiming to improve either the condition or the knowledge about it. In a way this is a type of the risk benefit assessment well known in

the field of research involving humans. In our view this is where the contribution of an ethics committee would be of a value.

5. **Appropriate safeguards in both initial and further processing**: safeguards used for the initial processing should be re-evaluated if they are relevant for further processing. Such safeguards as encryption and pseudonymization require extra efforts, due to constant technological developments. In many, but not all cases double pseudonymisation can be applied. However, beyond its benefits for the protection of confidentiality, it involves risks to the data accuracy and thus its implementation cannot be automatic but needs to be considered case by case considering all, including technical aspects.

While the Guidelines correctly recall that further processing for scientific research is presumed compatible with the initial purpose under Article 5(1)(b), they stop short of explaining how controllers should document and rely on this presumption in complex, multi-purpose research environments. In practice, controllers face uncertainty when secondary use involves layered datasets, mixed legal bases, or evolving research aims, for example, when registry data collected for surveillance are later used to study treatment outcomes or genetic correlations. The Guidelines' current wording leaves open whether such reuse requires a separate compatibility test or how controllers should record their reasoning to demonstrate compliance.

This gap is particularly problematic for public health and biomedical research, where data are collected under statutory mandates and reused over decades. Lawful initial collection, genuine scientific purpose, and implementation of Article 89(1) safeguards should suffice to rely on the presumption of compatibility. Yet without explicit guidance, controllers, ethics committees, and data-access bodies interpret this differently, leading to fragmentation and unnecessary procedural burdens. The absence of examples, such as cancer registries used for survival analyses or vaccine surveillance data reused for effectiveness studies, further limits the practical value of the presumption.

What is missing is a clear, operational framework that tells controllers how to document compatibility reasoning within their records of processing and DPIAs, and how to apply the presumption consistently across multi-purpose research infrastructures. Explicit criteria and real-world illustrations would ensure that the presumption functions as intended: to enable lawful, transparent, and proportionate secondary use of data for scientific and public-interest research, without redundant compatibility testing or conflicting national interpretations.

Need for clearer articulation in the Guidelines

The Guidelines rightly recall the presumption of compatibility for further processing for scientific research, but they do not give enough *practical guidance* on how controllers should document and rely on it in complex, multi-purpose environments.

> *"Further processing for scientific research purposes is presumed to be compatible with the initial purpose… However, the controller must still check if the processing is lawful."*

Concrete proposals

- **Clarify the interplay between GDPR and EHDS obligations.** The Guidelines do not explain how compatibility and lawfulness should be assessed in practice when the legal basis for the initial processing is *public interest* under Article 6(1)(e) GDPR, yet under the EHDS the same public institution becomes a *data holder* and is legally mandated to share the data for secondary use. The GDPR presumes that further processing for scientific research is

compatible with the initial purpose, but this presumption does not remove the controller's responsibility to verify that the processing is lawful and supported by an appropriate legal basis. However, under the EHDS, data holders do not have discretion: they must provide access once a permit is issued. This creates uncertainty about how controllers should reconcile (i) the GDPR requirement to assess lawfulness and compatibility, with (ii) the EHDS obligation to share data under controlled-access conditions. Without clear guidance, institutions risk either over-restricting data access or, conversely, assuming that EHDS obligations automatically satisfy GDPR requirements. A more explicit explanation is therefore needed on how these frameworks interact, including:

  - how public-interest legal bases under Article 6(1)(e) and Article 9(2)(j) operate when data sharing is mandated by law;
  - how the compatibility presumption applies when the secondary use is authorised through an EHDS permit;
  - how controllers should document their assessment when the EHDS already defines the safeguards, purposes, and governance conditions.

- **Clarify scope of the presumption**: state explicitly that the presumption applies when:
  - the initial collection was lawful,
  - further use is genuinely scientific research (per the six key-indicative factors),
  - Article 89(1) safeguards are implemented.
- **No separate compatibility test, but documented reasoning**: recommend that controllers:
  - record in their RoPA/DPIA that a given secondary use falls under Article 5(1)(b) second sentence,
  - briefly justify why it remains within the same broad research/public health objective.
- **Examples for public health**: add examples such as:
  - using cancer registry data collected for incidence monitoring to study treatment patterns and survival,
  - using surveillance data to evaluate vaccine effectiveness, as *presumed compatible* further processing.

9. Lack of guidance on proportionate, risk-based pseudonymisation in research

Issue statement

The Guidelines do not address a critical operational gap: how controllers should determine proportionate pseudonymisation measures in scientific and clinical research. In practice, overly rigid interpretations, such as mandatory double pseudonymisation, are increasingly imposed by some authorities or ethics bodies, even though such requirements may be scientifically unnecessary, operationally burdensome, or even harmful to data or sample integrity. Evidence shows that double pseudonymisation can require additional manipulation of data and / or samples, increasing the risk of degradation and compromising the scientific validity of downstream analyses.

What is missing from the Guidelines is explicit recognition that pseudonymisation is not a one-size-fits-all obligation. Controllers must retain the discretion to select safeguards that are proportionate to the actual risks of the processing, taking into account the nature of the data, the research design, the feasibility of re-identification, and the Article 89(1) safeguards already in place. Without clear guidance, controllers face inconsistent expectations across Member States, and research infrastructures are exposed to unnecessary procedural barriers that do not enhance data protection.

The Guidelines should therefore clarify that the choice between single pseudonymisation, double pseudonymisation, or alternative safeguards must be based on a documented, risk-based assessment by the controller, who is best placed to evaluate scientific needs, technical constraints, and the risk profile of the processing.

The Belgian framework illustrates the practical challenges: for data linkage, controllers must obtain an opinion from the Information Security Committee (ISC). [6]However, when public-health data are linked under a legal mandate, it remains unclear what constitutes a "DPIA already provided for in the law" and what safeguards are considered reasonable and proportionate in this context. Article 35(10) GDPR explicitly states that when processing is based on a legal obligation or a public-interest task laid down in Union or Member-State law, and that law already includes a general DPIA, the controller is not required to conduct an additional DPIA but must comply with the safeguards defined in that law.

This principle should be clearly reflected in the Guidelines to ensure that public institutions can rely on the public-interest legal basis in a manner that is operational, rapid, and efficient, rather than burdened by duplicative assessments or unclear expectations. Controllers should not be required to introduce additional layers of pseudonymisation or procedural steps that are not proportionate to the risks, that could compromise the scientific validity of data linkage, or that would lead to unnecessary delays in assessments and the finalisation of requests. A clear and harmonised interpretation, aligned with Article 35(10) GDPR, and the practical realities of public-health data use, is essential to provide public institutions with a predictable, lawful, and workable route for data reuse in the public interest.

The Guidelines should also clarify the interplay between the GDPR and the EHDS with respect to DPIAs, the public-interest legal basis, and the role of additional safeguards. Under the EHDS, public institutions designated as data holders are legally mandated to make data available for secondary use once a permit is issued. At the same time, Article 35(10) GDPR explicitly states that when processing is based on a legal obligation or a public-interest task laid down in Union or Member State law, and that law already includes a general DPIA, the controller is not required to conduct an additional DPIA but must comply with the safeguards defined in that law. The Guidelines should therefore clarify how controllers are expected to reconcile their GDPR obligations with EHDS-mandated data sharing, and specify when additional safeguards are required and when they are genuinely justified. Ideally, national laws enabling public-interest research should establish a clear, efficient, and timely assessed framework, with feasible technical and organisational measures and a predictable route for controllers to rely on: i) defining the public-interest task; ii) embedding a general DPIA at the legislative level; iii) specifying proportionate safeguards; and iv) ensuring that controllers can rely on this framework without duplicative assessments. Such a model would allow public institutions to act rapidly and lawfully, while maintaining robust protections and serving the real operational needs of scientific and public-health research.

Need for clearer articulation in the Guidelines

The Guidelines should explicitly recognise that controllers must retain the discretion to determine the appropriate level of pseudonymisation and related safeguards based on a documented, risk-based assessment. Overly prescriptive requirements, such as mandating double pseudonymisation in all cases, do not reflect the operational realities of health research and may even compromise data and/or sample integrity. The decision on whether single or double pseudonymisation, or alternative safeguards, is proportionate should rest with the controller, who is best placed to evaluate scientific needs, technical constraints, and the risk profile of the processing. The Guidelines should therefore clarify that controllers may select proportionate measures tailored to the specific research context, provided that the reasoning is documented and that Article 89(1) safeguards are implemented, allowing controllers to choose proportionate safeguards based on risk.

EDPB could acknowledge the practical impossibility of anonymisation in most research contexts:

[6] https://www.ehealth.fgov.be/ehealthplatform/fr/comite-de-securite-de-linformation; https://www.smalsresearch.be/basisprincipes-voor-een-moderne-pseudonimiseringsdienst-2/

- Move away from theoretical debates on anonymisation.
- Emphasise that true anonymisation is rarely possible in research.
- Focus instead on risk-based safeguards and secure processing environments.

Concrete proposals

1. Clarify controller discretion and risk-based pseudonymisation (Section 8.3 / 8.5)
Add the following paragraph at the end of Section 8.3 ("Anonymisation and pseudonymisation of personal data") or, alternatively, as a new chapeau paragraph in Section 8.5 ("Determination of other types of appropriate safeguards"):

> *"Pseudonymisation is not a one-size-fits-all obligation. In line with the risk-based approach and the principle of accountability, controllers should retain the discretion to determine the appropriate level and modality of pseudonymisation (e.g. single pseudonymisation, double pseudonymisation, or alternative safeguards) on the basis of a documented risk assessment. This assessment should take into account, inter alia, the nature and sensitivity of the data, the research design, the feasibility of re-identification in the concrete context, and the safeguards implemented pursuant to Article 89(1) GDPR. Overly prescriptive requirements, such as mandating double pseudonymisation in all cases—may be neither necessary nor proportionate and, in some settings, may even bring unjustified delays in the start of the research, or compromise data or sample integrity and thereby the scientific validity of the research."*

2. Clarify the role of ethics / information security bodies versus the controller (Section 8.2 / 8.5)
Insert the following paragraph in Section 8.2 ("Risk analysis and data protection impact assessment") or Section 8.5:

> *"Ethics committees, information security committees and similar oversight bodies play a crucial role in reviewing the overall research protocol, including the protection of participants' rights and interests. However, the decision on which technical and organisational measures (TOMs) are implemented, such as the specific form of pseudonymisation or data linkage architecture, remains the responsibility of the controller, who must conduct the DPIA, assess residual risks and document the chosen safeguards. Oversight bodies should therefore avoid prescribing specific TOMs as a matter of principle and instead focus on advising and collaborating with controllers to identify feasible, proportionate solutions that adequately mitigate risks while preserving scientific robustness."*

3. Provide guidance on data linkage in research infrastructures (Section 2.2 / 8.3)
Add the following paragraph in Section 2.2 ("Research data infrastructures") or Section 8.3:

> *"In many scientific research settings, especially in longitudinal and registry-based studies, controlled data linkage is essential to ensure data quality, follow-up and clinically meaningful outcomes. The Guidelines should be understood as permitting pseudonymisation architectures that enable secure linkage (e.g. via trusted third parties or key-management services), provided that: (i) identifiers are kept logically and organisationally separate from research datasets; (ii) access to linkage keys is strictly role-based, subjected to the national law (if any) and auditable; and (iii) the linkage design is described in the DPIA and forms part of the Article 89(1) safeguards. Controllers should document why the chosen linkage model is necessary for the research aims and how the residual re-identification risk is controlled."*

10. International data transfers for scientific research are insufficiently addressed

Issue statement

The Guidelines provide almost no practical guidance on international data transfers, even though cross-border collaboration is structurally necessary for scientific, clinical, and public-health research. Existing GDPR transfer tools, such as SCCs, TIAs, ad hoc clauses, and Schrems II supplementary measures, were designed for bilateral commercial service provision, not for complex research

ecosystems involving mixed controller/processor roles, federated infrastructures, public bodies, and cloud-based analytics.

The Guidelines do not address how GDPR transfer rules apply when research involves mixed controller-Processor flows, nor how to manage transfers to public research bodies that cannot sign SCCs in commercial form (e.g., ministries, national institutes, public health authorities). They also do not clarify whether cloud hosting or remote access by non-EU providers constitutes a "transfer" in research settings, nor how to apply Schrems II supplementary measures when data are pseudonymised, held in secure environments, or accessed only through controlled queries.

The absence of research-specific guidance leaves controllers facing inconsistent national interpretations, unnecessary delays, and legal uncertainty, particularly for secondary use, registries, surveillance systems, and long-term cohort infrastructures. This gap is especially problematic given the Guidelines' own recognition that scientific research is a fundamental EU objective and that data disclosure to secondary users may itself constitute a research purpose. Without a nuanced interpretation of transfer rules, the presumption of compatibility and Article 89(1) safeguards cannot function as intended.

Need for clearer articulation in the Guidelines

For international data transfers in scientific and public-interest research, clarification is needed on how the GDPR framework interacts with the EHDS, particularly where the legal basis is public interest and the processing is already governed by Union or national law. Article 35(10) GDPR specifies that when such a law includes a general DPIA, controllers are not required to conduct an additional DPIA but must comply with the safeguards laid down in that law. It should therefore be clear how these safeguards are to be reflected in Transfer Impact Assessments and how controllers should assess lawfulness when data sharing is mandated under the EHDS.

Further clarification is also needed on how national law operates as a legal basis for transfers in cross-border or third-country contexts, including how this interacts with the fact that the one-stop-shop mechanism does not apply where the legal basis is public interest, as noted in Recital 128. To support predictable and efficient international data flows for clinical and public-health research, it would be valuable to consider the development of an alternative transfer instrument or a sector-specific Code of Conduct that enables GDPR-compliant transfers without relying on consent and in a manner compatible with national public-interest frameworks.

Clarification is also required on the circumstances under which Article 49(1)(d) GDPR ("important reasons of public interest") may be relied upon for urgent cross-border public-health research, such as outbreak investigations, rapid-response studies, or time-critical epidemiological analyses, ensuring that its use remains limited to situations where it is appropriate, justified, and embedded within documented governance rather than serving as a routine alternative to structural transfer mechanisms.

The Guidelines should explicitly acknowledge that international transfers in scientific research differ fundamentally from commercial outsourcing. Research infrastructures often involve:

- multi-party consortia with evolving roles over time,
- public bodies bound by statutory secrecy and ethics regimes,
- federated or distributed analytics where data do not leave the EEA,
- secure processing environments where only aggregated outputs are exported,
- pseudonymised datasets with no direct identifiers,
- data-visiting models where algorithms travel to the data, not vice-versa.

These models do not fit neatly into the SCC-based transfer architecture. The Guidelines should therefore articulate how controllers can comply with GDPR Chapter V (Transfers of personal data to 3rd countries or international organisations) in a way that preserves scientific integrity, avoids unnecessary re-engineering of infrastructures, and recognises the safeguards already embedded in research governance (ethics review, professional secrecy, Article 89(1) measures, pseudonymisation, secure environments). Without such clarification, controllers are left to interpret transfer rules in ways that may be overly restrictive, inconsistent across Member States, or incompatible with the operational realities of public-health and clinical research.

Concrete proposals

1. Call for an EDPB-endorsed research Code of Conduct with:

- model clauses for mixed controller/processor roles;
- rules for transfers to public research bodies unable to sign SCCs;
- safeguards for cloud based analytics;
- risk based transfer assessment tailored to scientific research.

And support development of a sector-specific Code of Conduct on international transfers (Article 40 GDPR).

Add a new paragraph in Section 8.5 ("Determination of other types of appropriate safeguards"):

> *"Given the structural importance of cross-border collaboration in scientific research, the EDPB encourages the development of a sector-specific Code of Conduct under Article 40 GDPR addressing international transfers in research. Such a Code could include: (i) model clauses for mixed controller/processor constellations typical of research consortia and data repositories; (ii) conditions for transfers to public research bodies unable to sign SCCs in commercial form; and (iii) safeguards for federated and cloud-based analytics, including data-visiting and secure processing environments."*

2. Clarify how Art. 49 derogations may be used for public health urgencies, or rare-disease research when no stable transfer tool exists.

3. Provide examples of acceptable governance for federated analysis.

4. Provide research-tailored guidance on Transfer Impact Assessments (TIAs)

Insert a new subsection under Section 8.2 ("Risk analysis and DPIA"):

> *"Only when appropriate and justified, and recognising that conducting Transfer Impact Assessments in scientific research is often resource-intensive and takes place in a field already subject to extensive regulatory, ethical, and quality standards (including ICH GCP and auditable health-data protections), controllers may take into account contextual safeguards such as: (i) pseudonymisation with separation of keys; (ii) the use of secure processing environments in which only query outputs leave the EEA; (iii) statutory or professional secrecy obligations, ethics oversight, or research-specific confidentiality duties applicable to foreign public bodies; and (iv) the scientific necessity of maintaining data integrity for longitudinal, cohort-based, or multi-timepoint analyses. Competent bodies should provide templates and concrete examples illustrating how these factors can reduce residual risk in a Schrems II assessment, and stakeholders across the research ecosystem should be encouraged to develop harmonised standards for such safeguards, in the same spirit as internationally recognised frameworks such as ICH GCP[7]."*

[7] https://www.ich.org/

5. Clarify the application of Schrems II supplementary measures in research settings

Add to Section 8.3 ("Anonymisation and pseudonymisation"):

> *"In research contexts, supplementary measures may include: (i) pseudonymisation where re-identification keys remain exclusively within the EEA; (ii) controlled remote access through secure environments; (iii) output-checking mechanisms; and (iv) governance-based safeguards such as ethics approval and professional secrecy. Competent bodies should clarify that these measures may be sufficient where the data importer cannot access identifiable data or where only aggregated results are exported."*

6. Clarify when cloud hosting by non-EU providers constitutes a "transfer"

Add to Section 3.1.1 ("Presumption of purpose compatibility") or Section 8.3:

> *"Competent bodies should clarify whether cloud hosting or remote maintenance by non-EU providers constitutes a transfer in research settings, particularly where: (i) data are encrypted or pseudonymised; (ii) keys remain exclusively within the EEA; and (iii) the provider has no technical ability to access intelligible data. Clear criteria are needed to avoid divergent national interpretations."*

7. Provide guidance for transfers to public bodies unable to sign SCCs

Add to Section 4.4.3 ("Derogations under Union or MS law"):

> *"In situations where personal data are transferred to public research bodies, such as ministries, national institutes, or public-health authorities, that act as controllers and cannot enter into Standard Contractual Clauses in their commercial form, it should be possible to rely on alternative appropriate safeguards under Article 46 GDPR. These may include statutory or professional secrecy obligations, ethics-committee oversight, or binding administrative arrangements between public authorities, provided they ensure a level of protection that is essentially equivalent to that afforded by SCCs."*

11. Genetics, omics and special categories of data

Issue statement

The Guidelines treat genetic and omics data under the general umbrella of "special categories of personal data," but they do not reflect the **heterogeneous risk spectrum** within omics datasets nor the **practical impossibility of anonymising genomic data** in many research contexts. They also do not acknowledge the **distinct governance needs** of rare-disease and personalised medicine (gen)omics, where identifiability is structurally higher and long-term reuse is scientifically indispensable. As a result, controllers lack operational guidance on how to calibrate safeguards, retention, and reuse for different types of omics data, and ethics committees often impose uniform requirements that do not align with GDPR's risk-based approach.

Need for clearer articulation in the Guidelines

The Guidelines should explicitly recognise that:

1. Genetic/omics data are not homogeneous: WGS/WES, multi-omics datasets, tumour-only somatic profiles, and single biomarkers present very different identifiability, disclosure, and linkage risks. Treating them as a single category leads to disproportionate safeguards and unnecessary barriers to research.

2. Full anonymisation of omics data is rarely feasible: the Guidelines currently imply anonymisation as a preferred safeguard, but do not acknowledge that:

- genomic data are inherently identifying, but never without additional information or very sophisticated reading tools, which per se is a protective and secure measure
- anonymisation often destroys scientific value,
- pseudonymised omics data remain personal data and must be governed accordingly.

3. Controllers need explicit support for long-term retention and re-analysis: rare-disease and (gen)omics requires decades-long retention and periodic reinterpretation. The Guidelines do not provide examples or criteria for documenting necessity under Article 5(1)(e) and Article 89(1).

4. Ethics committees often impose technical measures: the Guidelines do not clarify that the controller, not ethics bodies, is responsible for determining proportionate safeguards through DPIA and risk assessment. This gap leads to rigid requirements (e.g., mandatory double pseudonymisation) that may harm sample integrity or impede data linkage.

The GeNeo study conducted within the Belgian PRECISION initiative, in partnership with Sciensano, demonstrates that omics-based public-health research inherently relies on multi-actor, multi-institutional data flows, centralised infrastructures, and harmonised interpretation frameworks, including national molecular tumour boards, structured data capture, and coordinated variant annotation. These operational realities show that scientific validity and timely clinical decision-making depend on integrated data environments and proportionate safeguards, rather than rigid or prescriptive measures that could delay analyses or undermine the utility of genomic profiling. The study also highlights that access to clinical trials, often cross-border, is essential for patients with rare alterations, underscoring the need for workable international transfer mechanisms that do not rely solely on consent and that are compatible with public-interest legal bases. In this context, clarification is needed on how GDPR and the EHDS interact when processing is grounded in public interest and already governed by Union or national law, including how Article 35(10) GDPR operates in practice and how such embedded safeguards should be reflected in Transfer Impact Assessments. Further clarity is required on the role of national law as a legal basis for cross-border or third-country transfers, the availability of alternative safeguards for public bodies unable to sign SCCs, and the development of sector-specific instruments or Codes of Conduct enabling compliant data sharing for clinical and public-health research. Finally, it is important to specify the circumstances in which Article 49(1)(d) GDPR ("important reasons of public interest") may be used for urgent cross-border public-health research, such as outbreak investigations or rapid-response studies, ensuring that its use remains appropriate, justified, and embedded in documented governance rather than functioning as a routine substitute for structural transfer mechanisms.[8]

Concrete proposals

1. **Provide a taxonomy of genetic/omic data (raw vs derived; inherited vs acquired).**

2. **Clarify when epigenetic data fall under Art. 4(13).**

3. **Encourage Member States to avoid divergent definitions that undermine cross-border research.**

4. **Provide examples of risk-appropriate safeguards for each data type (e.g., WGS -> SPE only; variant lists -> controlled access).**

5. **Introduce a risk-graded framework for genetic and omics data.** Add a subsection under 8.4 Safeguards when processing genetic or biometric data:

[8] *Geneo study: Comprehensive genomic profiling versus limited local reimbursed NGS panels within the belgian Precision initiative - ScienceDirect (2026)*

"Controllers should distinguish between different categories of genetic and omics data when conducting DPIAs and determining safeguards. A risk-graded approach may include:

- *High-risk: whole-genome/whole-exome sequencing, multi-omics datasets, rare-disease profiles;*
- *Intermediate-risk: tumour-only somatic sequencing, panels of common variants;*
- *Lower-risk (still special category): single biomarkers with limited identifiability."*

This aligns with GDPR's risk-based approach and avoids one-size-fits-all safeguards.

6. **Why secure research infrastructures are integral to lawful omics data use.** Add to 8.3 Anonymisation and pseudonymisation:

   "The EDPB recognises that full anonymisation of genomic and multi-omics datasets is rarely achievable in practice without eliminating scientific utility. Controllers should therefore treat pseudonymised omics data as personal data, apply Article 9(2) conditions and Article 89(1) safeguards, and avoid relying on unrealistic expectations of 'anonymous genomics'. A practical interpretation of GDPR Article 9(2)(j) must recognise that research infrastructures which already apply GDPR safeguards and sector-specific rules are themselves part of the research ecosystem, not external or ancillary to it. Modern genomics and multi-omics research depends on secure, well-governed environments that implement pseudonymisation, controlled access, role-based permissions, auditability, data-quality standards, and expert oversight, all safeguards explicitly required under Article 89 GDPR. Infrastructures such as biobanks, federated analysis platforms, secure processing environments, and omics-data repositories therefore meet the requisites of "processing for scientific research purposes" when they operate under these conditions. This interpretation is consistent with the European Health Data Space (EHDS) Regulation, which recognises that electronic health and genomic data may be shared for secondary use only through controlled-access mechanisms. EHDS does not limit research to a single centralised structure; instead, it establishes a governance model in which multiple compliant infrastructures may provide access, provided they apply GDPR-level safeguards and sector-specific protections. It is also aligned with the WHO 2023–2024 Guidance on Human Genome Data[9], which emphasises that genomic data must be handled within secure, quality-assured, expertise-driven infrastructures and warns that governance models should avoid creating barriers to legitimate scientific research. WHO explicitly frames infrastructures as integral components of the scientific process, ensuring quality, integrity, and interpretability across the entire lifecycle of genomic data. For these reasons, infrastructures that implement GDPR Article 9 safeguards, Article 89 research protections, and relevant sector-specific rules (e.g., clinical genomics, biobanking, AI-based analysis) should be considered fully within the scope of "scientific research purposes." They enable, not merely support, the lawful and responsible use of omics data, and they ensure that data can be shared under controlled access in a manner consistent with both EHDS and international best practice. No research can take place in the absence of data. Data are the indispensable starting point of every scientific question, method, and conclusion."

7. **Provide explicit guidance on retention and re-use of omics data.** Add to 3.2 Storage limitation:

   "Long-term retention of omics data may be justified where future re-analysis is scientifically necessary (e.g., rare diseases, evolving interpretation of variants). Controllers should document:

   - *the scientific rationale for long-term retention;*
   - *the safeguards ensuring restricted access;*
   - *the governance for future re-use (e.g., ethics/ELSI review, Article 9(2)(j) conditions)."*

This supports lawful long-term storage without requiring repeated re-consent.

8. **Clarify the controller's role in determining safeguards.** Add to 8.2 Risk analysis / DPIA:

   "The determination of appropriate technical and organisational measures, including the degree of pseudonymisation, rests with the controller, based on a documented DPIA. Ethics committees and information-security committees may provide advice, but should not impose specific technical measures unless required by Union or Member State law."

[9] https://www.who.int/publications/i/item/9789240102149

9. **Add guidance on data linkage for omics.** Add to 8.5 Determination of other types of appropriate safeguards**:**

> *"Where scientific validity requires linkage of omics data with clinical, imaging, or registry data, controllers should document:*
> - *the necessity of linkage for the research purpose;*
> - *the safeguards preventing unauthorised re-identification;*
> - *the governance for linkage keys (e.g., held by an independent trusted third party)."*

12. Unharmonised interpretation of complex research roles

Issue statement

In clinical and health research, roles are structurally complex: sponsors, investigators, sites, laboratories, and data platforms may each act as controller, joint controller, or processor for different processing operations. Investigators often "wear different hats" (care vs research), and DPAs across Member States diverge on sponsor–investigator controllership models. This creates uncertainty for contracts, transparency notices, and allocation of responsibilities.

Need for clearer articulation in the Guidelines

The Guidelines should move beyond generic controller/processor definitions and provide research-specific illustrations that reflect real-world clinical-trial and registry architectures, including the dual role of investigators and the coexistence of multiple controllers in a single project.

Concrete proposals

- **Explicitly recognise "multi-role" actors in research**
  - **Sponsor:** Usually a controller for research-related processing (designs protocol, defines endpoints, determines data flows).
  - **Investigator / site:**
    - controller for patient-care processing (medical record, routine care, safety follow-up beyond protocol);
    - controller or joint controller *or* processor for research-specific processing, depending on whether they co-design the protocol and essential means.
  - The Guidelines should endorse this "different hats" model and recommend that controllers *describe it explicitly* in DPIAs, contracts, and information notices.
- **Provide structured criteria for sponsor–investigator roles**
  - **Joint controllership indicators:**
    - co-drafting of protocol and essential means;
    - shared decisions on endpoints, data categories, and follow-up;
    - shared scientific responsibility for the study design.
  - **Processor indicators:**
    - investigator follows a sponsor-defined protocol without meaningful influence on purposes and essential means;
    - processing is limited to implementing sponsor instructions for data collection and reporting.
  - The Guidelines should encourage a *processing-activity-by-processing-activity* analysis (e.g. recruitment, on-site data capture, central lab analysis, long-term storage, secondary use), rather than a single label for the entire project.
- **Address divergent DPA interpretations with a "safe harbour" logic**
  - **Acceptable role models:** The Guidelines could present a small set of *acceptable* role configurations (e.g. "Model A: sponsor controller / investigator processor for research

data; investigator separate controller for care data"; "Model B: sponsor and investigator joint controllers for research data"), and state that, if one of these models is transparently adopted and documented, it should generally be considered compliant.
    - **Documentation and transparency:**
        - recommend that sponsors/controllers keep a "controllership map" describing roles per processing operation and per jurisdiction;
        - require that this map underpins:
            - joint-controller arrangements (Art. 26),
            - data-processing agreements (Art. 28),
            - and layered information to participants (who does what, for which purpose, under which legal basis).
- **Clarify that ethics-committee views on roles are not determinative under GDPR**
    - The Guidelines should state that ethics committees may *comment* on roles, but the legal qualification of controller/processor is ultimately a GDPR question for controllers and, where relevant, DPAs.
    - Where ethics-committee expectations diverge from DPA guidance, controllers should:
        - document the conflict,
        - prioritise compliance with binding data-protection law,
        - and, where possible, explain to ethics committees how the chosen model still ensures high protection for participants.

13. Rights of data subjects whose data are used in research

Issue statement

The Guidelines acknowledge that certain rights, particularly erasure (Art. 17) and objection (Art. 21), may be restricted when their exercise would "render impossible or seriously impair" scientific research. However, they do not provide **operational guidance** on how these rights should be exercised in **multi-layered research ecosystems**, where:

- data flow across **controller-to-controller** and **controller-to-processor** chains,
- sponsors typically hold only **pseudonymised datasets** and **cannot re-identify individuals**,
- investigators "wear different hats" (clinical care vs. research),
- registries, repositories, and public-health bodies act as **independent controllers**,
- and data subjects may not know which entity is responsible for which part of the processing.

In practice, most data-subject requests are handled by the investigator or treating site, because they are the only party that can directly identify the participant. The sponsor, who receives only pseudonymised data, has neither the legal right nor the operational ability to access the re-identification key. As a result, sponsors are not expected, and should not be required, to communicate directly with clinical-trial participants to fulfil data-subject rights.

The absence of operational models creates uncertainty for controllers, ethics committees, and DPAs, and risks inconsistent implementation across Member States.

Need for clearer articulation in the Guidelines

The Guidelines should clarify **how data subject rights are to be exercised and fulfilled in complex research chains**, without undermining scientific validity or violating pseudonymisation safeguards. Specifically, the Guidelines should:

- Distinguish between **rights exercisable at the point of care** (source records) and rights exercisable **at the level of the research sponsor**.

- Explain how rights apply when the sponsor **cannot re-identify** the data subject and therefore cannot directly fulfil access, rectification, or erasure requests.
- Clarify how Article 17(3)(d) and Article 21(6) apply in practice, including documentation expectations.
- Provide guidance for **registries, repositories, and secondary-use infrastructures**, where data subjects may not have direct contact with the controller.
- Encourage harmonised communication models to avoid contradictory expectations from ethics committees, DPAs, and research institutions.

Concrete proposals

1. Provide operational models for exercising rights in research chains. The Guidelines should include examples illustrating how rights can be fulfilled **without re-identification**, such as:

- **Primary care provider / recruiting site as the natural contact point**
  - When the site acts as processor for the sponsor, it can fulfil access, rectification, or erasure requests **in the source medical record**, without disclosing the key code to the sponsor.
  - When the site is an independent controller for care, it fulfils rights **in its own capacity**, while informing the sponsor only of necessary downstream implications (e.g., exclusion from future linkages).
- **Sponsor or public-health institute fulfilling rights indirectly**
  - The sponsor acknowledges the request, informs the data subject that it cannot re-identify them, and **coordinates with the site** to implement feasible actions.
  - This preserves pseudonymisation and avoids unlawful re-identification.
- **Registries and repositories**
  - Provide a model where the registry acts as the **central rights-handling point**, even when data originate from multiple controllers.

2. Clarify the application of Article 17(3)(d) and Article 21(6). The Guidelines should explicitly state that:

- **Erasure and objection may be restricted** when fulfilling them would "render impossible or seriously impair" the research objectives, provided Article 89(1) safeguards are in place.
- Controllers should **document this assessment** in the DPIA and in internal governance records.
- Controllers should offer **alternative mitigations**, such as:
  - exclusion from future linkages,
  - restriction of further use,
  - cessation of re-contact,
  - removal from future follow-up datasets.

Once data are pseudonymised and integrated into analyses, **individual deletion may no longer be technically feasible** without compromising scientific validity.

3. Provide template language for transparency notices and Patient Information Sheet/Informed Consent Forms. The Guidelines should recommend standard wording for research contexts, including:

- **On pseudonymisation and limits of erasure**
  - *"Once your data are pseudonymised and integrated into aggregated analyses, it may no longer be possible to delete them individually without compromising the scientific validity of the research."*
- **On who handles rights requests**

  - *"Your primary contact for exercising your rights is your treating physician or the site where you were enrolled. The research sponsor does not hold identifying information and cannot directly access your identity."*
- **On remaining rights**
  - Clarify that access to general study results, rectification of source records, and complaint routes remain available.

4. Clarify rights in secondary-use and public-health research. The Guidelines should explicitly address:

- How rights apply when data are reused under Article 5(1)(b) compatibility presumption.
- How rights apply in **public-health surveillance**, where individual erasure may undermine population-level monitoring.
- How rights apply in **secure processing environments** (EHDS-data sharing route), where controllers may not have direct access to identifiers.

5. Encourage harmonised national approaches. Given the documented, the Guidelines should:

- Encourage DPAs to adopt **consistent interpretations** for rights in research.
- Recommend that ethics committees **do not impose contradictory requirements** (e.g., demanding erasure where pseudonymisation prevents it).
- Promote alignment with the other sector-specific regulations such as CTR, IVDR/MDR, EHDS, and the cross-sector DGA governance models.

CONCLUSION

The EDPB Guidelines 1/2026 represent a meaningful step toward clarifying how the GDPR applies to scientific research, yet they fall short of what is needed to support the operational realities of Europe's health-research ecosystem. When assessed against the daily work of public-health institutes, clinical research infrastructures, long-term cohorts, and cross-border data-reuse frameworks, several structural gaps become evident. These gaps directly affect feasibility, legal certainty, and the continuity of research across Member States, and they risk undermining coherence with the rapidly evolving EU health-data architecture, including the European Health Data Space Regulation, the Data Governance Act, the Clinical Trials Regulation, the *In Vitro* Diagnostic and Medical Devices Regulations, and the Artificial Intelligence Act.

Across Europe, researchers, public bodies, ethics committees, and data-protection authorities continue to interpret core GDPR concepts, purpose, legal basis, pseudonymisation, compatibility, controllership, and data-subject rights, in divergent ways. This fragmentation delays approvals, complicates cross-border collaboration, and creates inconsistent expectations for controllers. While the Guidelines offer a solid conceptual basis, they do not yet provide the operational clarity required for harmonised implementation in complex, multi-actor research settings.

What is missing is a genuine operationalisation of the GDPR for health and scientific research. Europe needs a coherent, research-appropriate data-governance framework that moves beyond a narrow focus on privacy risks and instead enables lawful, proportionate data reuse, cross-border collaboration, validation studies, and algorithmic improvement. Research should be recognised not as an exception to be constrained, but as a core public-interest activity requiring clear, workable mechanisms rather than abstract principles.

Achieving this requires coordinated action across all oversight bodies (Ethics Committees, European Medicine Agency, Data Protection Authorities, European Commission…). The EDPB cannot define research governance in isolation from the EMA, national competent authorities, ethics committees, AI-ethics experts, and health-data governance bodies. Without shared

principles, standards, and operational definitions, fragmentation will persist. Europe urgently needs the equivalent of Good Data Protection Practices for Health Research: a harmonised, jointly endorsed framework that clarifies roles, safeguards, and lawful pathways for data reuse.

Although the GDPR has not halted research in Europe, it has disrupted it. Persistent uncertainty, divergent interpretations, and the absence of harmonised guidance have created significant operational burdens without demonstrable gains in data-subject protection. Key concepts remain insufficiently defined, fuelling institutional inertia and risk-averse behaviour rather than enabling solutions.

Public-health institutes, clinical research sponsors, biobanks, registries, and emerging EHDS infrastructures all operate in environments where research is longitudinal, multi-actor, and dependent on the reuse of data collected over decades. For these ecosystems, legal certainty is not an abstract aspiration but a prerequisite for fulfilling statutory mandates, ensuring scientific integrity, and protecting individuals' rights and interests.

To achieve this, the Guidelines should:

1. Operationalise the GDPR for health and scientific research by providing practical guidance aligned with existing scientific, ethical, and regulatory standards and tailored data-governance models for Public Health Institutes.

2. Adopt a harmonised, research-specific interpretation of "purpose" that enables structural linkages, long-term infrastructures, and clear role allocations across data holders, HDABs, and users.

3. Strengthen examples for the six indicative factors by grounding definitions of scientific research in established international frameworks and adding public-health-relevant, domain-specific cases.

4. Clarify the interplay between GDPR and other EU laws by explaining legal bases, secondary-use conditions, and shifting controllership roles under EHDS, CTR, IVDR/MDR, DGA, and the AI Act.

5. Acknowledge that GDPR-consent models are not feasible for long-term, multi-source research and provide forward-looking guidance for consent wording in light of future EHDS secondary-use obligations.

6. Clarify the distinction between GDPR consent and ethical consent and avoid dual tick-box systems by allowing a single integrated statement linking participation to data processing.

7. Recognise the interdependence of research and infrastructure by treating registries, biobanks, secure platforms, and federated environments as embedded research actors, not external service providers.

8. Provide research-tailored guidance on international data transfers by establishing alternative transfer routes for public and academic bodies when SCCs, TIAs, or adequacy decisions are unavailable or impractical.

9. Clarify the cumulative application of Articles 6 and 9 GDPR to ensure lawful combinations of legal bases without undermining EHDS safeguards for AI training, testing, and evaluation.

10. Promote coordinated training across oversight bodies so ethics committees understand GDPR and DPAs understand clinical and public-health research methodologies.

11. Provide proportionate, risk-based pseudonymisation guidance that reflects the specific risk spectrum of genetic and omics data without imposing one-size-fits-all requirements.

12. Harmonise interpretation of data-subject rights in research.

Sciensano strongly supports the EDPB's commitment to enabling responsible scientific research while safeguarding fundamental rights. Strengthening the Guidelines along the lines proposed in this contribution would significantly enhance legal certainty, promote harmonisation across Member States, and ensure that Europe's research ecosystem, public health institutes, academic centres, clinical research sponsors, and EHDS infrastructures, can operate effectively, ethically, and in full compliance with the GDPR. A clearer, more operational, and more harmonised framework is essential not only for regulatory compliance, but for Europe's capacity to generate the scientific evidence needed to protect and improve the health of its population.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

About Sciensano

Sciensano is Belgium's national public and independent scientific institute, bringing together more than **1,000 experts** across human, animal, and environmental health. With **over 120 years of scientific activity**, Sciensano plays a central role in safeguarding public health, supporting evidence-based policymaking, and enabling high-quality research at national and European level.

Sciensano is deeply involved in shaping the future European health data landscape. It contributes to and collaborates with major EU initiatives, including **HealthData@EU**, **TEHDAS2**, **SHAIPED**, and multiple cross-border research infrastructures. These engagements position Sciensano at the forefront of operationalising the **European Health Data Space (EHDS)**, the EU's flagship framework for the secondary use of electronic health data.

As both a **data holder** (custodian of large-scale health datasets, registries, surveillance systems, and biobanks) and a **data user** (conducting epidemiological, biomedical, environmental, and public health research), Sciensano operates at the intersection of science, data governance, and regulatory compliance. This dual role provides a unique, implementation-level perspective on how GDPR provisions function in practice across complex research ecosystems.

In its daily work, Sciensano must simultaneously ensure:

- **scientific integrity**,
- **robust data protection**,
- **ethical and societal oversight**, and
- **public-interest mandates** grounded in national and EU law.

This combination of responsibilities gives Sciensano first-hand insight into the practical challenges faced by controllers, processors, researchers, and public bodies when applying the GDPR to scientific research, particularly in areas such as secondary use, pseudonymisation, international transfers, genetic and omics data, and the interplay between GDPR and emerging EU legislation.

Sciensano's contribution to the EDPB Guidelines 1/2026 reflects this operational experience and aims to support a harmonised, realistic, and future-proof interpretation of the GDPR that enables high-quality research while safeguarding fundamental rights.