Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

# Sciensano's contribution to the EDPB Guideline entitled

*" Guidelines 2/2026 on Anonymisation, version 1.0, adopted 7 July 2026"*

***30th October 2026***

***Prepared by:***

***Roxana Albu*** *Scientific Expert,* ***Joke Sas*** *Scientific Expert,* ***Wannes Van Hoof*** *Head ELSI,*

***Marion Louis*** *DPO,* ***Melissa Van Bossuyt*** *Head DPO & Coordinator Information Security*

## CONTENTS

**Introduction** ..... 2

**Positive elements** ..... 2

**Key issue 1: Need for operationalisation** ..... 3

**Key issue 2: Legal analysis and internal inconsistencies** ..... 3

**Key issue 3: Reasonably likely means and foreseeability** ..... 6

**Key issue 4: Technical measures and risk assessment** ..... 6

**Key issue 5: Health data linkage and EHDS** ..... 8

**Key issue 6: AI, omics, and emerging technologies** ..... 9

**Key issue 7: Contracts, governance, and European consistency** ..... 10

**Key issue 8: Documentation and accountability** ..... 11

**Key issue 9: Mixed anonymous and personal data** ..... 11

**Summary of requested clarifications** ..... 12

**Conclusion** ..... 14

**ABOUT SCIENSANO** ..... 15

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

## Introduction

Sciensano welcomes the publication of the **EDPB Guidelines 02/2026 on Anonymisation** and supports the objective of improving legal certainty regarding the distinction between personal and anonymous data under Regulation (EU) 2016/679 (GDPR).

**Sciensano** is Belgium's federal public health institute and performs statutory tasks in epidemiological surveillance, health monitoring, public health research, biobank and omics research, and health data linkage involving hospital records, disease registries, mortality data, laboratory data, administrative datasets, and European research infrastructures. The Institute has extensive operational experience with pseudonymisation, secure linkage infrastructures, trusted third parties, secure processing environments, and cross-border health research.

The draft guidelines are an important update to Opinion 05/2014 and correctly acknowledge the contextual nature of anonymisation and the relevance of CJEU case law. However, from the perspective of a public health authority and research institution that must perform concrete anonymisation assessments, the draft remains predominantly conceptual and would benefit from significantly more operational guidance. Sciensano therefore submits the following comments with a view to improving the final guidelines.

## Positive elements

We particularly welcome the recognition that:

- data may be personal for one entity and anonymous for another;
- anonymity must be assessed from the perspective of the relevant entity;
- pseudonymisation is not anonymisation;
- anonymisation is a process that may produce anonymous data even if original data are retained; and
- re-identification risk must be assessed in light of technical, organisational, and contextual factors. The draft expressly recognises the contextual nature of anonymity and the need to assess identifiability from the perspective of relevant entities. It also introduces the three criteria of **No Record Isolation, No Linkage and No Inference** as part of the technical assessment framework. These elements are valuable and align with modern data governance environments. These elements are particularly relevant for public health research and European data infrastructures.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

## Key issue 1: Need for operationalisation

**The guidelines remain largely descriptive rather than operational.** The draft devotes substantial space to explaining legal concepts and recent case law but provides limited assistance for controllers that must conduct practical anonymisation assessments. More than a decade after the WP29 Opinion 05/2014 on Anonymisation, public authorities and research institutions need guidance that is implementable in day-to-day governance.

**Recommendation:** the final guidelines should include:

- sector-specific annexes (health, research, statistics, genomics);
- practical anonymisation assessment templates;
- worked examples for common research scenarios;
- indicative standard practices or principles;
- indicative risk matrices;
- examples of acceptable technical and organisational measures; and
- documentation templates for accountability purposes.

Stakeholders need such tools; otherwise, we risk that different supervisory authorities and institutions are likely to apply divergent thresholds.

## Key issue 2: Legal analysis and internal inconsistencies

**Contextual approach and the relative nature of personal data.** The draft correctly recognises that data may be personal from one entity's perspective but anonymous from another's. This is consistent with C-413/23 P EDPS v SRB and C-582/14 Breyer.

For public health research, this principle is essential where:

- identifiers are removed before transfer;
- linkage keys are held by a trusted third party;
- the research institute has no practical access to identifiers; and
- the recipient acts independently.

However, the draft does not sufficiently distinguish between:

1. independent research recipients with no realistic access path to identifying data; and
2. recipients that remain functionally connected to the original controller through ongoing linkage mechanisms.

**Recommendation:** add a dedicated health research example illustrating when an independent public health institute may assess anonymity from its own perspective.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

**Inconsistency regarding the need to reassess previously anonymised datasets.** The draft states that a controller that assessed a dataset as anonymous under Opinion 05/2014 is not expected to conduct a new assessment, although periodic reassessment is described as good practice. However, later sections emphasise evolving capabilities, data leaks, and technological developments, including AI-assisted re-identification, in a manner that could be interpreted as requiring ongoing reassessment whenever new techniques emerge. The draft also notes that capabilities may change over time, for example following a data leak.

This creates legal uncertainty.

**Recommendation:** clarify explicitly that:

- periodic reassessment is a **risk-based governance measure**, not an automatic legal obligation;
- reassessment should be triggered by material changes in datasets, access conditions, linkage possibilities, or re-identification techniques; and
- controllers are not required to continuously monitor all hypothetical technological developments.

A footnote in the final text should explain the relationship between the non-retroactivity statement and the later discussion of evolving capabilities.

**Potential contradiction regarding transfers.** The draft suggests that data may be personal where an entity could transfer them to another entity that might identify individuals. Yet the cited CJEU judgments concerned actual or realistically foreseeable transfers, not abstract possibilities.

**Recommendation:** the final guidelines should clarify that identifiability must be assessed in relation to concrete, reasonably foreseeable transfer scenarios and not merely theoretical transfer possibilities.

**Singling out versus identification.** The draft sometimes appears to move from the concept of record isolation or singling out to a conclusion of identifiability. Under Recital 26 GDPR, singling out is an example of a means that may contribute to identification; it is not necessarily sufficient by itself.

The draft does not sufficiently define singling out or explain how it relates to the three criteria of No Record Isolation, No Linkage and No Inference. This creates uncertainty about how the criteria should be applied in practice, particularly where a record can be distinguished from others without the available information necessarily enabling the identification of the natural person to whom it relates. Under Recital 26 GDPR, singling out may contribute to the identification of a person, but the uniqueness or isolability of a record should not, on its own, be treated as conclusive evidence that the person is identifiable. The assessment should consider whether the record can be linked to an identified or

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

identifiable natural person, taking into account the means reasonably likely to be used, the context of processing, and the availability of additional information.

We would recommend *clarifying* the definition and practical application of singling out, and explaining how it should be assessed in conjunction with the three criteria, so that:

1. No Record Isolation addresses whether an individual record can be distinguished or isolated from the dataset, while clarifying that record uniqueness or isolation does not automatically establish that the corresponding natural person can be identified.
2. No Linkage addresses whether the record can be linked to information from the same or other datasets in a way that enables the identification of a natural person, taking into account the availability, accessibility, and reasonable likelihood of using such additional information.
3. No Inference addresses whether information about a natural person can be inferred from the data, while distinguishing the ability to infer attributes or characteristics from the ability to identify the person to whom those attributes relate.

The Guidelines should further clarify whether these criteria are intended to operate as independent tests, cumulative conditions or complementary analytical perspectives, and how their results should inform the overall assessment under Recital 26 GDPR. In particular, the Guidelines should avoid implying that failure to satisfy any one criterion automatically establishes identifiability, without considering the full context, persons accessing the data and the circumstances and the means reasonably likely to be used to identify the data subject.

For public health registries, genomic datasets and linked health research data, a record may be unique because it contains a rare diagnosis, an unusual combination of clinical characteristics or a distinctive genomic variant. However, whether that uniqueness enables identification depends on the availability of auxiliary information, the possibility of linkage and the practical context in which the data may be accessed and used. The Guidelines should include concrete examples illustrating these distinctions, including cases where a record can be isolated but the available means do not enable the identification of the natural person concerned.

**Recommendation:** clarify that:

- uniqueness of a record is not automatically equivalent to identification; and
- additional conditions are required to establish that a natural person can be identified in practice.

This distinction is particularly important for rare disease and omics datasets.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

## Key issue 3: Reasonably likely means and foreseeability

**Need to distinguish realistic from speculative scenarios.** The draft correctly refers to means reasonably likely to be used, but several examples appear to rely on hypothetical chains of events. For public health authorities, anonymisation assessments must remain manageable and foreseeable.

**Recommendation:** introduce an explicit foreseeability test based on:

- practical accessibility of additional data;
- legal and organisational barriers;
- realistic opportunity for access;
- expected effort; and
- expected benefit of re-identification.

This would better align with Recital 26 GDPR and the Breyer law case.

**Unauthorised actors and unlawful access.** The draft includes unauthorised actors such as cybercriminals among potentially relevant entities. Sciensano agrees that Article 32 GDPR requires controllers to assess security risks from malicious actors, but this should not automatically determine whether data are personal under Article 4(1) GDPR. Otherwise, any hypothetical future data breach could prevent data from ever being considered anonymous.

**Recommendation:** clarify that:

- unlawful access scenarios are relevant for security risk management;
- identifiability assessments should focus on reasonably foreseeable lawful or realistically accessible means; and
- effective technical and organisational security measures may limit the relevance of unauthorised actors for the anonymisation assessment.

## Key issue 4: Technical measures and risk assessment

**Need for concrete technical guidance.** The draft identifies the three criteria but does not explain how controllers should test them in practice.

The final Guidelines should provide a practical, evidence-based framework identifying the technical standards, methods and assessment procedures that can be used to evaluate whether data have been effectively anonymised. They should clarify which standards are recognised at EU or international level, whether they are applicable across all Member States, and how their suitability should be assessed in different contexts. The Guidelines should also identify the expert bodies and institutions responsible for developing, validating and updating these standards.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

- **Identify recognised standards and competent bodies:** Reference relevant technical standards, methodologies and guidance developed by recognised standardisation organisations and expert bodies, including ISO/IEC, Eurostat and the European Commission's Joint Research Centre, where applicable. Clarify their scope, evidential basis and limitations, and distinguish legally binding requirements from voluntary standards and technical recommendations.
- **Promote harmonised and comparable assessments across Member States:** Explain which assessment principles and minimum requirements should be applied consistently across the EU, while allowing proportionate adaptation to the type of data, intended use, release model and identification risks. Clarify whether different technical approaches can support equivalent levels of protection and how this equivalence should be demonstrated.
- **Specify technical measures and their limitations:** Provide practical examples, including aggregation thresholds, k-anonymity and related approaches, suppression and generalisation, differential privacy where appropriate, synthetic data, secure query interfaces, output checking and secure processing environments. Explain what each measure protects against, its limitations, the risks it does not address and when combinations of technical and organisational safeguards are necessary. In particular, clarify that applying a single technique or meeting a numerical threshold does not automatically establish anonymity.
- **Define a reproducible assessment methodology:** Set out the steps, criteria and evidence needed to assess the effectiveness of anonymisation. Explain how to identify plausible re-identification scenarios, assess available auxiliary information and relevant technical capabilities, test the effectiveness of the selected measures, document residual risks and determine when reassessment is needed. The methodology should support transparent, reproducible and independently reviewable conclusions.
- **Provide practical assessment questions and examples:** Include questions that organisations can use to select and evaluate methods, such as:
    - What data are released, at what level of detail, and for what purpose?
    - Who could access the data, what additional information might they reasonably obtain, and what technical capabilities could they use?
    - Which identification, linkage or inference scenarios are relevant, and how have they been tested?
    - What evidence demonstrates that the selected measures are effective in the specific context?
    - What residual risks remain, and how do the measures affect data utility?
    - When should the assessment be repeated in response to new data sources, technologies or re-identification techniques?
    - How should the assessment be adapted for rare disease, genomic and other high-dimensional health data?
- **Identify sources of technical expertise and ongoing validation:** Specify which European and international expert bodies, research institutions and standardisation organisations can provide validated methods, technical guidance, assessment

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

tools and relevant benchmarks. Clarify how these resources will be maintained and updated as re-identification techniques and available technologies evolve.

**Recommendation:** The EDPB should

- establish a **harmonised, evidence-based technical framework** with common assessment principles and methods that can be adapted to the specific context, data characteristics, access conditions and stakeholders involved.
- clarify **when an anonymisation assessment must be performed and repeated**, including before data are released, shared or made available for secondary use, and whenever material changes may affect identification risks.
- specify the **principles and criteria for these assessments**, including the reasonably likely means of identification, available auxiliary information, linkage and inference risks, the effectiveness of technical and organisational safeguards, residual risks and the impact of technological developments. The framework should define minimum documentation requirements and explain how assessments can be validated, reviewed and updated to ensure consistent and transparent application across Member States.

**Absence of practical risk levels.** Controllers need a structured way to distinguish low, medium, and high residual risk.

**Recommendation:** include a **qualitative matrix** based on:

- dataset size;
- rarity of attributes;
- dimensionality;
- availability of external datasets;
- accessibility of linkage information;
- technical expertise required;
- computational resources required; and
- governance safeguards.

This would greatly improve consistency across Member States.

## Key issue 5: Health data linkage and EHDS

**Linkage is insufficiently addressed.** For Sciensano, data linkage is a central operational activity. The draft recognises linkage risk but provides little methodological guidance for distributed environments involving registries, hospitals, laboratories, mortality databases, and European research networks.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

**Recommendation:** add a dedicated section on:

- deterministic and probabilistic linkage;
- trusted third-party linkage;
- separation of duties;
- key management;
- governance controls;
- linkage quality metrics; and
- residual risk assessment after linkage.

**Interaction with the European Health Data Space (EHDS).** The final guidelines should explicitly address the interaction with Regulation (EU) 2025/327 on the European Health Data Space (EHDS). The EHDS does not harmonise anonymisation standards across the Union. The regulation allows Member States to determine certain aspects of secondary use governance, including conditions relating to anonymisation and access to health data. As a result, national approaches may continue to differ. For institutions participating in cross-border health research infrastructures, divergent national anonymisation expectations create significant operational challenges.

**Recommendation:** the EDPB should clarify:

- how anonymisation assessments interact with EHDS secure processing environments;
- the relationship between anonymisation and health data access body decisions;
- the status of outputs generated within secure processing environments; and
- expectations for cross-border consistency.

## Key issue 6: AI, omics, and emerging technologies

**AI-assisted re-identification.** The draft rightly notes that AI may reduce the cost and time of re-identification. However, the analysis should be aligned with Regulation (EU) 2024/1689 (AI Act), which adopts a risk-based approach and does not presume that every AI-assisted inference constitutes identification.

**Recommendation:** clarify that:

- AI-assisted matching must still meet the threshold of reasonably likely identification;
- accuracy and reliability of AI-generated matches are relevant;
- probabilistic outputs alone are insufficient; and
- the assessment should consider the actual deployment context.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

**Omics and genomic data.** Sciensano is involved in several European omics and genomics initiatives. Genomic data present particular challenges because of their high dimensionality and potential uniqueness.

**Recommendation:** add a dedicated annex on genomics and omics covering:

- rare disease cohorts;
- genomic variants;
- polygenic scores;
- multi-omics integration;
- family linkage risks; and
- aggregate versus individual-level genomic outputs.

## Key issue 7: Contracts, governance, and European consistency

**Role of contractual safeguards.** The draft states that contractual prohibitions on re-identification are not equivalent to legal prohibitions. While contractual measures alone are insufficient, public research infrastructures rely on a combination of:

- technical controls;
- access restrictions;
- audit rights;
- sanctions;
- ethics oversight; and
- institutional accountability.

**Recommendation:** recognise more explicitly that combined technical, organisational, and contractual safeguards may materially reduce practical re-identification risk.

**Consistency with other EU regulatory approaches.** The draft should avoid creating unnecessary divergence from other EU data governance frameworks, including:

- the EHDS;
- the Data Governance Act;
- the Data Act; and
- sectoral approaches that recognise combined technical and governance safeguards.

A coherent European approach is particularly important for public health research infrastructures.

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

## Key issue 8: Documentation and accountability

Sciensano agrees that anonymisation assessments should be documented. Documentation is essential for accountability, auditability, and demonstrating the reasoning underlying the assessment.

**Recommendation:** the final guidelines should provide a model documentation structure including:

- dataset description;
- purpose;
- recipient perspective;
- risk factors;
- technical measures;
- organisational safeguards;
- residual risk conclusion; and
- review triggers.

## Key issue 9: Mixed anonymous and personal data

The draft suggests that when a dataset contains both anonymous information and personal data, the dataset should generally be treated as personal data unless its different parts are treated separately. For large research infrastructures, this approach may be disproportionate if identifiable records can be effectively separated from records that meet the criteria for anonymity.

Sciensano recommends that paragraph 36 clarify how the presence of identifiable records affects the classification of the other records in the same dataset.

- *Reflect recent DPA decisions:* Consider the 2026 decisions concerning IQVIA in France[1] and Italy[2], in which the authorities rejected claims of anonymity where persistent patient indirect identifiers and health information enabled singling out and potential re-identification using reasonably available means. These cases illustrate that removing direct identifiers does not necessarily make health data anonymous where persistent identifiers, detailed information or linkage with other sources can enable identification.

The Guidelines should clarify that separating data does not, by itself, make them anonymous. The assessment must establish whether individuals can still reasonably be

[1] https://www.cnil.fr/en/health-data-fine-5-million-euros-against-iqvia *(accessed on 29/10/2026)*
[2] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10302112 *(accessed on 29/10/2026)*

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

identified, taking into account the available information, linkage possibilities and the entity's actual access and capabilities.

**Recommendation:** Clarify that the assessment may be conducted at the level of individual records, distinguishable subsets or the dataset as a whole, depending on whether the components can be reliably separated and assessed independently. The presence of identifiable records should not automatically determine the status of all remaining records, but those records can be considered anonymous only where the applicable identification risks are sufficiently low. The Guidelines should also clarify that singling out or record uniqueness alone does not establish identifiability without considering whether the individual can realistically be identified in practice.

## Summary of requested clarifications

Sciensano respectfully requests that the EDPB address the following points in the final Guidelines:

1. **Operational guidance:** Provide practical assessment templates, sector-specific annexes, worked examples and indicative risk matrices to support consistent implementation across public health, research, statistics, genomics and other relevant contexts.
2. **Contextual assessment and legal certainty:** Clarify how the status of data should be assessed from the perspective of the relevant entity, distinguishing independent recipients without realistic access to identifying information from entities that remain connected through linkage mechanisms or other access arrangements.
3. **Reasonably likely means and foreseeability:** Establish clear criteria for assessing identification risks, taking into account the practical accessibility of additional information, realistic opportunities for access, legal and organisational barriers, required effort and expected benefit. Distinguish reasonably foreseeable identification scenarios from speculative possibilities and clarify the relevance of unlawful access scenarios.
4. **Singling out and the three assessment criteria:** Define singling out and clarify the relationship between No Record Isolation, No Linkage and No Inference. Explain how these criteria contribute to the overall assessment and clarify that record uniqueness, singling out or the ability to infer attributes does not, by itself, necessarily establish that a natural person is identifiable.
5. **Technical standards and risk assessment:** Provide a harmonised, evidence-based and technically operational framework identifying recognised standards, assessment methods, technical and organisational measures, their limitations and the circumstances in which they should be combined. Include practical criteria for assessing residual risks, examples of their application and references to relevant expert bodies and validation resources.
6. **Timing and review of anonymisation assessments:** Clarify when assessments should be performed, including before data are released or made available to

Sciensano Headquarters
Juliette Wytsmanstraat 14
1050 Elsene
Belgium

recipients, and when reassessment is warranted. Distinguish legal obligations from recommended risk-based governance practices, and identify material changes in data, access conditions, linkage possibilities or technical capabilities that may trigger review.

7. **Health data linkage and the EHDS:** Provide specific guidance on deterministic and probabilistic linkage, trusted third parties, separation of duties, key management and residual risks after linkage. Clarify the relationship between anonymisation assessments, Health Data Access Body decisions, secure processing environments and their outputs, including expectations for cross-border consistency under the European Health Data Space.
8. **AI, genomic and other omics data:** Address AI-assisted matching, including the relevance of accuracy, reliability, probabilistic outputs and deployment context. Provide dedicated examples or an annex covering rare disease cohorts, genomic uniqueness, family relationships, multi-omics integration and the risks associated with individual-level and aggregate outputs.
9. **Technical, organisational and contractual safeguards:** Clarify how access restrictions, secure processing, audit mechanisms, contractual conditions, sanctions and institutional accountability may contribute to reducing practical identification risks when combined with appropriate technical measures. Explain the limits of these safeguards and their relevance to the overall assessment.
10. **Documentation and accountability:** Provide a model documentation structure covering the dataset, purpose, relevant entity and recipient perspective, identification scenarios, risk factors, selected measures, supporting evidence, residual risk conclusions and review triggers. Clarify the evidence needed to support an assessment and enable it to be reviewed or independently validated.
11. **Mixed anonymous and personal data:** Clarify when assessments may be conducted at the level of individual records, distinguishable subsets or the dataset as a whole. Explain what effective separation requires in practice and confirm that the presence of identifiable records does not automatically determine the status of all other records, provided that the remaining components can be reliably separated and independently assessed.
12. **Legal consistency and relevant decisions:** Clarify the relationship between the Guidelines, relevant CJEU case law and other applicable EU data governance frameworks, including the EHDS, Data Governance Act and Data Act. Explain the limits of relevant legal analogies and consider pertinent supervisory authority decisions to illustrate the practical application of the criteria for anonymity.

**Overall, Sciensano recommends that the final Guidelines translate the GDPR's principles into a harmonised, evidence-based and practically applicable framework.** This should enable controllers, public authorities, research institutions and data recipients to assess identification risks consistently, select proportionate safeguards, document and substantiate their conclusions, and determine when reassessment is necessary. Common EU-level assessment principles and minimum requirements should support comparable outcomes across Member States while allowing implementation to reflect the specific

data, context, access conditions and stakeholders involved. This is particularly important for health research, data linkage, genomic and other omics data, and cross-border research infrastructures, where legal certainty must be achieved without disregarding realistic identification risks or unnecessarily limiting the scientific utility of data.

## Conclusion

Sciensano supports the EDPB's objective of strengthening legal certainty and promoting a consistent European approach to anonymisation. The key challenge is to translate the legal principles set out in the GDPR into **clear, technically grounded and practically applicable guidance** that enables controllers to assess identification risks in real-world data environments.

The final Guidelines should move beyond conceptual explanations and provide a harmonised, evidence-based methodology for applying the risk-based approach. This should include concrete assessment criteria, recognised technical standards and methods, practical examples, and transparent requirements for documenting and reviewing decisions. It should clarify how the assessment should account for the nature and granularity of the data, the purpose and context of processing, the perspective and capabilities of the relevant entities, the availability of auxiliary information, realistic linkage and inference scenarios, and the technical, organisational and contractual safeguards in place. It should also specify when an assessment should be performed or revisited, how residual risks should be evaluated, and what evidence is needed to support a conclusion that data are anonymous.

Particular attention is needed for health research, registries, genomic and other omics data, and cross-border data infrastructures, where data uniqueness, linkage possibilities, changing access conditions and emerging analytical capabilities can affect identification risks. The Guidelines should explain how common EU-level principles and minimum assessment requirements can be applied consistently while remaining proportionate to different datasets, access models and stakeholder contexts. They should also identify relevant technical standards, expert bodies and validation resources to support reliable and comparable assessments across Member States.

**The overarching recommendation is therefore that the EDPB provide an operational framework that makes the risk-based approach transparent, reproducible and implementable in practice.** This would enable controllers, public authorities, research institutions and data recipients to understand not only which legal principles apply, but also how to assess risks, select and combine safeguards, substantiate their decisions and determine when reassessment is warranted. Such guidance would improve consistency and accountability across Europe while supporting responsible data use and preserving the scientific value of data, without weakening the protection afforded to individuals under the GDPR.

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 of applying the GDPR to scientific research and public health, particularly in relation to anonymisation and pseudonymisation, data linkage, secondary use of health data, and the specific risks associated with genetic and omics data.

Sciensano's contribution to the EDPB Guidelines 02/2026 on Anonymisation aims to support a harmonised, practical and future-proof interpretation of the GDPR. It highlights the need for clear, evidence-based risk assessment, stable technical guidance and common EU-level minimum principles and tools, enabling consistent implementation while safeguarding fundamental rights.

Sciensano remains available to contribute its practical expertise in public health surveillance, health data linkage, registries, biobanks, omics research and secure data infrastructures to support the development of the final Guidelines.