Contribution to EDPB Public Consultation on Guidelines 1/2026

(Processing of Personal Data for Scientific Research Purposes)

Author
Tomasz J. Skajster
Facharzt für Neurochirurgie
Consultant Neurosurgeon
Berlin, Germany

1. Scope of Contribution

This submission addresses the interpretation of necessity, proportionality, and safeguards in the processing of health-related personal data where clinical care and research contexts overlap or are operationally interdependent.

The draft Guidelines focus on scientific research; however, the same principles operate in clinical environments, where their interpretation bears directly on patient safety. The considerations set out below are submitted in that context.

2. Core Observation

Healthcare institutions frequently implement restrictive, ex ante access controls to personal data systems by reference to GDPR principles of data minimisation and purpose limitation. Where such controls introduce latency into access to patient data, they produce effects that require assessment against the full proportionality framework of the Regulation, not merely its data-protective limb.

The question requiring clarification is whether ex ante access limitations remain proportionate under Articles 5(1)(c), 5(2), 6(1)(d), and 9(2)(h) GDPR where timely access to data is itself a precondition for lawful and clinically effective processing. This question arises in particular where the operational context renders the timing of access inseparable from the legitimate purpose served.

An access-restrictive approach premised on precaution may not fully reflect the GDPR's risk-based and accountability-oriented framework, which requires proportionality assessments to account for the rights and interests on both sides of the processing relationship, including, where applicable, the right to health protection under Article 35 of the Charter of Fundamental Rights.

3. Access and Use: A Necessary Distinction

For the purposes of applying the principle of data minimisation under Article 5(1)(c) GDPR, a distinction must be drawn between technical access to data — availability within a defined role-based permission structure — and actual use of data, meaning processing undertaken for a specific, identified purpose at a specific moment in time. These are analytically distinct operations, and the principle of data minimisation governs the latter, not the former.

Data minimisation requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. It does not, in terms, require the pre-emptive architectural restriction of access rights. Critically, access limitations — whether role-based or temporal — do not in themselves ensure compliance with data minimisation if they prevent the use of data that are necessary for a lawful processing purpose. An access restriction that forecloses necessary use produces an outcome that is inconsistent with Article 5(1)(c), not expressive of it.

This has specific implications for temporal access limitations implemented as an expression of the need-to-know principle. Restricting access to historical data on the basis of predefined time thresholds represents an ex ante determination of necessity that is made in the abstract, without reference to the concrete clinical situation in which the data will be required. The necessity of accessing prior data cannot be assessed in advance; it can only be assessed in relation to the specific clinical facts present at the time of the encounter. Predefined temporal thresholds therefore risk excluding clinically relevant information on the basis of criteria that are structurally incapable of reflecting actual necessity.

An interpretation that equates data minimisation with ex ante limitation of access conflates system design with lawful processing. Its practical consequence is that data which are present within the system, and which would be necessary for a lawful processing purpose, are not accessible at the point of care — thereby preventing the context-sensitive assessment of necessity that lawful processing under Article 9(2)(h), subject to the minimisation requirement of Article 5(1)(c), presupposes. The design of access controls accordingly forms part of the proportionality assessment under Article 25(1) GDPR, and an access architecture that systematically forecloses necessary use is not an appropriate measure within the meaning of that provision. The implications of this for the clinical assessment of necessity are examined in Section 4 below.

4. The Situational Character of Clinical Necessity and Its Implications for Access Design

The draft Guidelines appear to assume processing environments in which the necessity of accessing personal data can be determined in advance and subjected to prior administrative control. That assumption does not correspond to the operational structure of clinical healthcare provision.

Clinical necessity is inherently situational. It emerges in the course of the clinical encounter, in response to information that becomes available only progressively as examination, history-taking, and diagnostic reasoning proceed. The treating healthcare professional cannot, prior to accessing a patient's data, fully anticipate which specific elements will be required for clinical decision-making, nor can that determination be adequately made by an administrative process conducted in advance of the encounter.

This has particular doctrinal significance where temporal access limitations are implemented as an expression of the need-to-know principle. The determination of which data are necessary for a given clinical situation — including whether and to what extent historical data are required — depends on context-specific medical judgement that is not

reducible to fixed temporal thresholds or predefined access categories. Ex ante assumptions of necessity, expressed as architectural restrictions, risk excluding clinically relevant information on the basis of abstract criteria that cannot account for the specific facts of the clinical situation at hand.

This analysis gives rise to a further doctrinal observation that bears directly on the interpretation of Article 5(1)(c) GDPR: access to relevant data constitutes a precondition for the assessment of necessity, not its consequence. Where access is pre-emptively restricted on the basis of ex ante assumptions about what is necessary, the practical capacity to determine necessity in context is impaired. An access architecture that forecloses the assessment it purports to operationalise is internally incoherent and cannot satisfy the proportionality requirement it invokes.

Requirements for prior administrative authorisation or technical unlocking mechanisms that introduce clinically material latency are, to that extent, inconsistent with the effective application of Article 9(2)(h) GDPR, which predicates the lawfulness of processing on necessity assessed in the context of healthcare provision, and, where the data subject is incapable of giving consent in an emergency, with Article 6(1)(d) GDPR. A restrictive interpretation of these provisions as applicable only to rare or exceptional circumstances does not reflect the operational structure of clinical care, in which situations requiring immediate access to personal data are not exceptional but constitute the normal and foreseeable mode of provision.

Where the legal basis for processing under Article 9(2)(h) is operative, the access architecture must be designed to enable, rather than impede, the clinician's capacity to fulfil that legal purpose. An access control that systematically forecloses or delays the necessity assessment that Article 9(2)(h) requires cannot be characterised as an appropriate measure within the meaning of Article 25(1), and cannot be justified solely by reference to data minimisation objectives that are more appropriately addressed at the level of use, as set out in Section 3 above.

5. Safeguards and Accountability

A tiered safeguard model combining role-based access structures, professional confidentiality obligations under applicable Member State law, and comprehensive tamper-proof audit logging constitutes an appropriate safeguard package within the meaning of Article 89(1) GDPR, capable of satisfying the accountability requirements of Articles 5(2) and 24 without introducing access latency.

The components of this model are not alternatives to access controls but constitute a structured and legally sufficient access control architecture. Role-based permissions define the class of persons authorised to access personal data. Professional confidentiality obligations, enforceable under both national law and the GDPR, govern the purposes for which access may be exercised. Audit logging ensures that every access event is attributed, recorded, reviewable and, where necessary, sanctionable.

In this model, access is not unrestricted; it is fully attributable and subject to ex post accountability. This satisfies the risk-based logic of the GDPR, under which the

proportionality of a safeguard is assessed against its capacity to achieve the protective purpose, not against the degree of restriction it imposes per se.

Comprehensive, role-scoped audit logging, operating in conjunction with enforceable professional confidentiality obligations and institutional sanction mechanisms, should accordingly be recognised as a primary component of an appropriate safeguard architecture for healthcare data processing, sufficient to satisfy the accountability requirement without necessitating record-level prior authorisation mechanisms that are operationally incompatible with the purposes for which the data is lawfully held.

6. Relevance for Scientific Research

These considerations apply with particular force to scientific research conducted in clinical environments, to research relying on routine healthcare data, and to processing operations where the boundary between direct care and research is operationally fluid.

Overly restrictive access architectures do not operate only on clinical care; they simultaneously constrain the feasibility, completeness, and epistemic integrity of research based on real-world clinical data. Where access controls delay or prevent the capture of clinically generated data, the research record is impoverished in ways that cannot subsequently be remedied.

Clinical data processing shares with scientific processing the characteristics of structured evaluation, evidence-dependence, and adherence to ethical and professional standards. The context-sensitivity required by the GDPR's risk-based framework applies in both settings and supports a consistent, purpose-sensitive interpretation of the access principles discussed above.

7. Suggested Clarification

The Guidelines should clarify that the design of technical and organisational measures pursuant to Article 25(1) GDPR must be assessed against the operational requirements of the purposes for which personal data are lawfully processed, and that access control architectures which systematically impede the exercise of a lawful purpose are not "appropriate" within the meaning of that provision.

The Guidelines should further clarify that, in healthcare settings subject to Article 9(2)(h), the assessment of necessity is performed by the responsible healthcare professional at the point of care and cannot be predefined or substituted by prior administrative authorisation mechanisms, which, where they introduce clinically material latency, are inconsistent with the effective application of that legal basis.

The Guidelines should clarify that a safeguard architecture comprising role-based access controls, professional confidentiality obligations enforceable under Union or Member State law, and comprehensive tamper-proof audit logging constitutes an appropriate safeguard package within the meaning of Article 89(1) GDPR and satisfies the accountability requirements of Article 5(2), without necessitating record-level prior authorisation mechanisms in healthcare processing contexts.

8. Conclusion

Clarifying the relationship between the design of access controls, the situational character of clinical necessity, and the accountability function of audit-based safeguards would support a proportionate and operationally coherent application of the GDPR across both healthcare and research contexts. The clarification sought does not diminish the data protection objectives of the Regulation; it ensures that the technical and organisational measures adopted in its name do not operate to undermine the legitimate purposes it simultaneously protects.

The cases presented in Annex I document instances in which clinically relevant data were present within the system but not accessible at the point of care due to predefined access limitations, thereby preventing the effective assessment of necessity in the clinical context. They are submitted as operational corroboration of the doctrinal observations set out in Sections 3 and 4 above.

Annex I - Documented Anonymised CIRS Incidents

Introductory Note

The following cases document instances in which access to clinically relevant data was restricted due to the implementation of data protection principles, in particular data minimisation and the need-to-know principle, operationalised through predefined access rules within hospital information systems.

In each case, the relevant data were present within the system and a lawful basis for processing existed in the context of patient care under Article 9(2)(h) GDPR. Access was nonetheless restricted by role-based, temporal, or administrative limitations derived from an ex ante determination of necessity. As a result, the treating healthcare professional was unable to assess necessity in the specific clinical context at the point of care.

The cases are submitted as operational corroboration of the doctrinal observations set out in Sections 3 and 4 of this submission. They illustrate a common structural pattern: the principle of data minimisation is applied at the level of access rather than use, necessity is predetermined at system level rather than assessed by the treating clinician, and the access restriction thereby prevents the context-sensitive lawful processing it purports to safeguard.

Case 1 – Restricted access to primary imaging in acute intracranial haemorrhage

1. What happened?

An unconscious patient with acute subarachnoid haemorrhage was referred for urgent neurosurgical treatment. The complete imaging dataset, including native cranial CT, was present within the system. At the time of clinical assessment, access to the full dataset was restricted by predefined system permissions; only partial data were available to the treating neurosurgeon.

2. What was the problem?

The neurosurgeon holding direct clinical responsibility did not have role-based access to the complete dataset, as system permissions confined visibility to the originally treating department. Clinical decision-making was therefore performed on the basis of incomplete information, notwithstanding the availability of the full dataset within the system.

3. Why did it occur?

Access was restricted by predefined permission structures derived from the application of data minimisation and the need-to-know principle at system design level. Necessity was operationalised as a fixed role-based criterion rather than assessed by the treating clinician in response to the specific clinical situation.

4. Relevance to GDPR interpretation

This case illustrates that the application of data minimisation at the level of access, rather than use, may prevent the treating clinician from determining which data are necessary for the clinical situation at hand. Where necessity is predefined by system design, the clinician cannot perform the context-sensitive assessment that Articles 5(1)(c) and 9(2)(h) GDPR require. Access to the data was a precondition for that assessment; its restriction made the assessment impossible.

Case 2 – Inaccessibility of clinically relevant data due to administratively enforced access structures

1. What happened?

A patient with a diagnosed intracranial aneurysm presented for urgent specialist evaluation. Relevant imaging and clinical documentation existed within the system but were not accessible during the consultation, as the system required prior administrative creation of a new case and explicit assignment of access rights before any data could be viewed.

2. What was the problem?

The treating physician was unable to access data required for clinical assessment during the encounter, despite holding clinical responsibility for the patient and despite the data being available within the system. No deficiency of legal basis existed; the restriction was structural.

3. Why did it occur?

Access was conditioned on predefined administrative structures implementing a restrictive interpretation of data minimisation and necessity. These structures required formalisation of access rights in advance of the clinical encounter, irrespective of the immediate clinical context. Necessity was thereby determined by administrative process rather than by the treating clinician.

4. Relevance to GDPR interpretation

This case illustrates that where access rights must be established prior to the clinical encounter, the assessment of necessity is displaced from the point of care to an earlier administrative stage at which the clinical context is not yet known. Data minimisation is thereby applied at the level of access rather than use, and the treating clinician is prevented from performing the context-sensitive necessity assessment required for lawful processing under Articles 5(1)(c) and 9(2)(h) GDPR.

Case 3 – Restricted access and functionality in an emergency clinical context

1. What happened?

In an emergency neurosurgical case, the treating physician was unable to access relevant patient data and system functions within the active clinical interface. The data and functionality were present within the system but were not accessible from the clinical

context in which the treating physician was operating, as the permission model implementing data minimisation restricted access by reference to predefined role and system-context parameters.

2. What was the problem?

Initiating necessary clinical procedures required the treating physician to exit the active clinical interface, transition to a different system environment, and re-establish access rights. This sequence introduced a delay in a context in which immediate access to data and system functions was a precondition for timely clinical action.

3. Why did it occur?

Access and functionality were restricted through permission models derived from the application of least-privilege and need-to-know principles, implemented as an expression of data minimisation at system design level. These models defined necessity by reference to predefined role and system-context parameters, without provision for the dynamic allocation of clinical responsibility that characterises emergency care.

4. Relevance to GDPR interpretation

This case demonstrates that data minimisation applied at the level of access, rather than use, may impede lawful processing not through absence of a legal basis but through prior architectural restriction of the means necessary to exercise it. The treating clinician's capacity to assess necessity at the point of care was structurally foreclosed by permission parameters that substituted system-level assumptions for clinical judgement, contrary to the requirements of Articles 5(1)(c) and 9(2)(h) GDPR.

Case 4 – Inaccessibility of historical patient data due to temporal access restrictions

1. What happened?

An unconscious patient presenting with acute neurological symptoms had a clinically relevant prior medical history. The corresponding data existed within the system but were not accessible at the point of care, as access had been restricted following the expiry of a predefined temporal threshold applied after the conclusion of a previous treatment episode.

2. What was the problem?

The treating physician was unable to access clinically relevant historical information during the acute assessment, despite that information being available within the system and despite a lawful basis for processing existing under Article 9(2)(h) GDPR.

3. Why did it occur?

Access to historical data had been restricted on the basis of predefined temporal thresholds implemented as an expression of data minimisation and the need-to-know principle. These thresholds operationalised necessity as a function of elapsed time,

determined at system design level, rather than as a function of clinical relevance to the current presentation.

4. Relevance to GDPR interpretation

This case illustrates that fixed temporal limitations on access represent an ex ante determination of necessity made without reference to any specific clinical situation. Where necessity is predetermined by reference to abstract time-based criteria, the treating clinician cannot assess whether data concerning prior history are necessary for the clinical situation at hand. Data minimisation is thereby applied at the level of access rather than use, and the restriction prevents the context-sensitive assessment of necessity that Articles 5(1)(c) and 9(2)(h) GDPR require. Case 4 is the direct clinical correlate of the temporal threshold argument set out in Section 3 of this submission.