Meta Submission to the EDPB Consultation on the Guidelines 1/2026 on processing of personal data for scientific research purposes

Executive Summary

Meta appreciates the opportunity to contribute to the practical implementation of the scientific research GDPR framework, which is essential to ensure responsible innovation in the EU.
However, we respectfully submit that several aspects of the draft Guidelines require substantial revision to ensure alignment with binding EU law and institutional competence boundaries and to enable scientific research to play its essential role in our societal progress and prosperity. We would like to offer comments on the following key topics:

- **Scope of scientific research and institutional competence (Section 2.1):** The EU legislator has defined "scientific research" broadly and consistently across thirty years of legislation, encompassing applied, industrial, privately funded, and close-to-market research conducted in any sector. GDPR Recital 159 explicitly mandates this broad interpretation. The six "key-indicative factors" proposed in the draft Guidelines introduce requirements that are found nowhere in the legislative definition and, in several respects, contradict it. The EDPB's institutional mandate is the consistent *application* of the law — not its restrictive redefinition. We urge the EDPB to withdraw or substantially revise the six-factor framework to ensure conformity with binding EU law, including Directive (EU) 2016/801, TFEU Article 179(1), GDPR Recital 159, and Article 13 of the EU Charter of Fundamental Rights.
- **Interaction between the GDPR research framework and DSA Article 40 (Sections 2.2 and 2.4):** The EDPB should confirm that processing undertaken to comply with DSA Article 40 is determined by that legal obligation, and that such access mechanisms should not be classified as "research data infrastructures" within the meaning of paragraph 13. Clarification of how the respective safeguards regimes interact is essential to avoid regulatory stacking that risks chilling the provision of researcher access the DSA was designed to mandate.
- **Legal bases and safeguards (Sections 4.1.2 and 4.3):** Safeguards requirements must not exceed what Article 89 GDPR provides. Requirements drawn from specific regulatory contexts (such as clinical trials) should not be generalised into conditions applicable to all forms of scientific research. Only the legislator is entitled to impose new legal requirements.
- **Special categories of personal data — Article 9(2)(e) and inferred data (Section 4.4.2):**
    - The EDPB should include examples of "clear affirmative action" in digital contexts, where platform architecture requires users to actively configure public audience settings.
    - An **intent-derived foreseeability test** should be incorporated for the application of Article 9 GDPR to inferred data. The current expansive formulation is incompatible with the principles of legal certainty, non-impossibility of obligations, intent-based liability, and the relative concept of personal data (*SRB*, C-413/23 P; *Breyer*, C-582/14).

    - Where a platform provides access to data that does not on its face constitute special category data, Article 9 obligations for any subsequent inference should attach to the researcher's processing, not to the platform's provision of access.
    - Guidance on proportionate, system-level compliance approaches for large-scale datasets is essential to avoid rendering the framework unworkable.
- **Right to erasure (Section 6.2):** The assessment of whether erasure would "seriously impair" research should account for the cumulative impact of potential requests, methodological requirements (completeness, representativeness, statistical validity), and research design — not merely the size of the dataset.
- **Attribution of responsibility (Section 7):** The EDPB should reaffirm that responsibility must be proportionate to actual determination of purposes and means. Where a platform provides structured data access and researchers independently determine their own research purposes and methodology (including under DSA Article 40), such arrangements typically give rise to separate, independent controllership — not joint controllership.
- **Appropriate safeguards (Section 8):** The EDPB should confirm that architectural and system-level safeguards (secure processing environments, restrictions on data export, redaction of direct identifiers, contractual prohibitions on re-identification) may constitute appropriate safeguards under Article 89(1) GDPR at the infrastructure level.

Overarching concern:

- The draft Guidelines subordinate the fundamental right of scientific freedom (Charter Art. 13) to data protection. Instead, the Guidelines should balance both rights as EU law requires (Recital 4 GDPR, Charter Art. 52(1)). We urge the EDPB to apply the broad definition of scientific research the EU legislator already determined, apply Article 89 GDPR safeguards proportionately within that scope, and refrain from imposing restrictive conditions that contradict binding EU law or exceed its institutional mandate.
- We remain committed to supporting scientific research that is conducted responsibly and with full respect for all the rights and freedoms and interpretations that are conducive to ensuring societal progress and economic growth in a single digital market and beyond.

1. General Observations

Meta welcomes the opportunity to respond to the public consultation on Guidelines 1/2026. We recognise and appreciate the EDPB's commitment to providing structured guidance on the application of the GDPR to scientific research — an area of significant legal and practical complexity. In addition, we support efforts to advance research and innovation, which are “a backbone of the EU’s vision to deliver a competitive, resilient and sustainable future.”[1]

The Guidelines provide helpful clarifications on several important questions, including the presumption of compatibility for further processing, the permissibility of extended data storage for research purposes, and the availability of broad and dynamic consent mechanisms. These clarifications support legal certainty for controllers and researchers alike.

However, in order to advance both the vision of enabling scientific research to promote scientific progress and innovation and the Guidelines’ stated objectives — enabling and facilitating the processing of personal data for scientific research while safeguarding data subjects' fundamental rights – it is important to ensure the Guidelines do not restrict the already existing, broad definition

[1] Research and Innovation, European Commission, https://commission.europa.eu/topics/research-and-innovation_en

of scientific research in EU legislation. The following observations are structured to follow the draft Guidelines' own section numbering and focus on practical implementation considerations.

2. Scope of Scientific Research (Guidelines Section 2)

2.1 Key-Indicative Factors (Guidelines Section 2.1)

EU law already defines "scientific research" and "researcher" broadly and without restrictive conditions over 30 years of legislation:

Source	Year	Key Contribution
EU Charter of Fundamental Rights, Art. 13	2000/2009	Scientific research as a fundamental right — "free of constraint"
TFEU Art. 179(1)	1957/2009	EU objective: European Research Area, ALL research activities, including industry
Decision No 1110/94/EC (Fourth Framework Programme)	1994	Research and technological development broadly defined; industry eligible
Community Framework for State Aid R&D (96/C 45/06)	1996	EU definitions of research categories
Commission Recommendation 2005/251/EC (European Charter for Researchers)	2005	Researcher = professional creating new knowledge, **any sector**
Council Directive 2005/71/EC (Researchers Directive)	2005	Research = "creative work… to increase knowledge… devise new applications"; research organisation = any public **or private** organisation
Regulation 1291/2013 (Horizon 2020), Art. 2	2013	"Whole spectrum" of research and innovation activities
Regulation 651/2014 (GBER), Art. 2	2014	Industrial research and experimental development as legitimate research categories

GDPR Recital 159	2016	**Explicit broad interpretation mandate**; includes privately funded research
Directive (EU) 2016/801 (recast, in force)	2016	Same broad definition; research organisation includes private bodies
Council Recommendation of 18 December 2023 (new Charter for Researchers)	2023	Covers **all types** of research: "frontier, targeted, strategic, applied and close to market"

The central definition, provided by **Directive (EU) 2016/801, Art. 2(9)**, states: *"'Research' means creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications."*

Key features of this definition include:

- **No specific requirements** for peer review, public dissemination, or external ethical board approval.
- **Explicit inclusion** of applied and technological research, specifically the development of new applications.

A broad interpretation is also mandated by **GDPR Recital 159**, which clarifies that research encompasses technological development, demonstration, fundamental research, applied research, and privately funded research. This mandate is further anchored by **TFEU Article 179(1)**, which defines the European Research Area to include "all the research activities deemed necessary," including for industrial competitiveness, and **Article 13 of the EU Charter of Fundamental Rights**, which enshrines scientific research as a fundamental right "free of constraint."

EU law has never restricted "researcher" to academics nor "research" to peer-reviewed, publicly funded activities:

- **Directive (EU) 2016/801, Art. 2(10)** defines "research organisation" as "any public or private organisation which conducts research," encompassing entities that develop new applications.
- The **European Charter for Researchers** (Recommendation 2005/251/EC; updated 2023) defines a researcher as a professional *"engaged in the conception or creation of new knowledge, products, processes, methods and systems"* — independently of sector. The 2023 update covers explicitly *"all types of research, namely frontier, targeted, strategic, applied and close to market."*
- **EU Framework Programmes** (since Decision 1110/94/EC in 1994) have always recognised *"universities, research organisations, industrial companies, including SMEs, or natural persons" as eligible.*

The EDPB's draft Guidelines 1/2026 impose ultra vires six "indicative factors" for research to qualify as "genuinely scientific": These factors introduce requirements (peer review,

publication, ethical standards, researcher independence) that are found nowhere in the legislative definition of research under EU law.

- **This approach may extend beyond the EDPB's interpretive mandate.**
    - **Recital 159 GDPR mandates breadth**: the EDPB cannot narrow what the legislator deliberately made broad.
    - **The conditions contradict EU law**: Directive 2016/801 defines research without requiring peer review, publication, ethical **standards**, or researcher independence; the Charter for Researchers covers all sectors without qualification.
    - **Institutional competence**: only the EU legislator (Parliament + Council) can define legal concepts. The EDPB's role is the consistent *application* of the law, not its redefinition — and even less a *restrictive* redefinition that contradicts the legislator's express instructions.
- **The restrictive approach of narrowing the EU's legal definition of research, curtails progress and innovation.**
    - **Violates Article 13 of the Charter**: scientific freedom exists because it is what makes progress possible.
    - **Undermines TFEU Art. 179(1)** and the European Research Area.
    - **Subordinates a fundamental right** (research freedom) to data protection, rather than balancing both rights as EU law requires (Recital 4 GDPR, Charter Art. 52(1)). Several aspects of the Guidelines are construed in an overly restrictive manner and lack adequate consideration for practical implementation.
    - **Places the EU at a competitive disadvantage** globally.
    - **Contradicts the EU's own €95.5 billion investment** in Horizon Europe, which funds applied, industrial, and close-to-market research.

Recommendations:

- **Apply the broad definition already ingrained in EU law,** as mandated by Recital 159 GDPR and consistent with 30 years of EU legislation.
- **Apply Article 89 GDPR safeguards proportionately** to protect data subjects' rights within that broad scope, rather than acting as a shadow legislator imposing restrictive conditions with no democratic mandate.
- **Withdraw or substantially revise the six "indicative factors"** to ensure they do not contradict binding EU law (Directive 2016/801, GDPR Recital 159, TFEU Art. 179(1), Charter Art. 13) or the established EU definition of "researcher." In particular:
    - It must be clear that the concept applies to research with dual societal and commercial objectives that would support consistent implementation.
    - The absence of public dissemination (e.g., where results are subject to confidentiality requirements or intellectual property protections) does not, in itself, negate the scientific character of research. This is consistent with the European Code of Conduct for Research Integrity, which acknowledges legitimate reasons for confidentiality.
    - "Scientific research purposes" is interpreted as determined by the legislator, i.e., broadly in accordance with Recital 159 GDPR, encompassing technological development, applied research, and privately funded research conducted with methodical rigour.

2.2 Research Data Infrastructures (Guidelines Section 2.2)

We welcome the draft Guidelines' recognition that entities operating "research data infrastructures" — making data available for others' research — may themselves be processing for scientific research purposes (paragraph 13).

The draft Guidelines do not provide detailed guidance on how the six-factor test applies to entities whose role is primarily to *enable* research by providing structured access to data for vetted researchers, rather than to *conduct* research themselves. For such entities, criteria such as "methodical approach" or "verifiability" may apply differently at the infrastructure level than at the level of the individual research project. The interaction between the GDPR research framework and DSA Article 40 data access obligations raises additional questions regarding regulatory coherence, which we address in Section 2.4 below.

Recommendation:

- **Distinguish infrastructure-level roles from research-level roles.** The Guidelines should clarify how the scientific research concept applies at the infrastructure level, in particular by distinguishing the role of an entity that enables data access from the role of the researcher who conducts the research. These are functionally and legally distinct activities and should be treated as such.

2.3 Ancillary Processing Operations (Guidelines Section 2.3)

The clarification that ancillary processing operations necessary to conduct scientific research (such as data quality checks or pre-processing) can be considered part of the research processing is helpful and reflects operational reality.

2.4 Interaction Between GDPR Research Framework and DSA Article 40

The Guidelines are silent on how the GDPR's scientific research framework interacts with obligations under DSA Article 40(12), which requires very large online platforms to provide vetted researchers with access to publicly accessible data.

Platforms subject to DSA Article 40 are legally required to provide data access to vetted researchers. The processing necessary to comply with this obligation, including the structuring, provision, and governance of data access, is undertaken pursuant to a distinct EU legal requirement. Without clarification, platforms face uncertainty as to whether their compliance with one EU law inadvertently triggers obligations, or activates exemptions, under a different EU framework. This uncertainty affects both the platforms providing access and the researchers relying on that access.

The practical consequences of this may be significant. First, if providing data access under DSA Article 40 is treated as processing "for scientific research purposes" under the GDPR, the platform potentially inherits the full suite of Article 89(1) obligations, the six-factor test, and the specific provisions on data subjects' rights, on top of the DSA's own requirements. Second, because the DSA already mandates its own vetting criteria, access conditions, and safeguards, concurrent application of the GDPR research framework would require platforms to satisfy two potentially inconsistent sets of requirements with no or unclear guidance on how conflicts between them are

to be resolved. The resulting regulatory stacking risks chilling the provision of researcher access that the DSA was designed to mandate.

Recommendations:

- **Exclude legally mandated data access mechanisms from the scope of "research data infrastructures."** Where an entity provides data access pursuant to a separate EU legal obligation, such as Article 40 of the DSA, its processing purpose is determined by that legal obligation, not by the downstream research activity. The Guidelines should confirm that such access mechanisms fall outside the concept of "research data infrastructures" as described in paragraph 13.
- **Clarify the interaction between GDPR scientific research provisions and DSA data access obligations.** The Guidelines should clarify the interaction between GDPR scientific research provisions and DSA Article 40 data access obligations to support coherent implementation across EU regulatory frameworks.
- **Confirm that a regulatory mandate constitutes a sufficient legal basis.** The Guidelines should clarify that, where an entity provides data access under a legal obligation (such as DSA Article 40), the regulatory mandate itself is the legal basis to conduct that data transfer on a controller-to-controller basis (separate and independent controllers), without requiring separate justification under the GDPR scientific research framework. The recipient controller (i.e., the researcher in the art. 40 DSA case) will be subject to the purpose limitation principle (only process the data received under the legal mandate to comply with the purpose included in this legal mandate) and any other GDPR duty that may be applicable to its processing activities.

3. Data Protection Principles (Guidelines Section 3)

3.1 Purpose Limitation — Presumption of Compatibility (Guidelines Section 3.1)

We welcome clear confirmation that further processing for scientific research purposes is presumed compatible with the initial purpose under Article 5(1)(b) GDPR. The example addressing further processing of publicly available social media data for related research on page 17 provides useful practical guidance.

For entities that collect personal data for platform services and subsequently facilitate research access (whether to internal research teams or external, vetted researchers), the presumption of compatibility is of significant practical importance. Additional examples addressing the application of this presumption in digital platform contexts — including the use of publicly available content for observational research — would support consistent application.

Recommendations:

- Retain and, where possible, expand the practical examples illustrating the presumption of compatibility, including for research using publicly available data from digital environments.
- Clarify the interaction between the presumption of compatibility and the controller's obligation to identify a lawful basis for further processing.

3.2 Storage Limitation (Guidelines Section 3.2)

We strongly welcome the EDPB's clarification that controllers may store personal data for scientific research purposes for longer periods, even after original processing purposes have been fulfilled. The acknowledgment that research results may give rise to future, unforeseen research projects — and that storage for potential future projects within a certain area of research is permissible — is practical, proportionate, and essential for longitudinal studies, reproducibility, and the iterative nature of scientific inquiry.

Recommendation:

- We encourage the EDPB to retain these provisions in the final Guidelines without modification, as they provide important legal certainty.

4. Lawfulness — Legal Bases and Special Categories (Guidelines Section 4)

4.1 Broad and Dynamic Consent (Guidelines Section 4.1.2)

We welcome the recognition of broad consent and dynamic consent as workable approaches where research purposes cannot be fully specified at the time of data collection. These mechanisms reflect the practical realities of scientific research while maintaining meaningful data subject involvement.

The availability of broad consent, subject to appropriate safeguards that are already identified in art. 89 GDPR, provides important flexibility for research programmes where the precise scope of future analysis is not yet fully defined at the point of data collection. However, the addition of new safeguards not regulated in the GDPR and imported from a very specific kind of research such as clinical trials that are subject to regulated ethics oversight and adherence to legally established ethical standards cannot be extended to all the different kinds of scientific research that the broad concept set forth in EU law encompasses.

Recommendations:

- Confirm that broad consent, accompanied by appropriate safeguards, provides a stable and legally certain basis for ongoing research programmes, and that the requirement for purpose specification is met through the identification of a defined area of research combined with safeguards.
- Safeguards' requirements should not exceed what Article 89 GDPR provides. While it may be appropriate to reference examples of safeguards that are legally imposed in specific regulatory contexts (such as independent ethics review for clinical trials), such context-specific requirements must not be generalised into conditions applicable to all forms of scientific research. Only the legislator is entitled to impose new legal requirements; the draft guidelines should not be used to introduce obligations that go beyond the legislative framework.

4.2 Legitimate Interest (Guidelines Section 4.3)

We welcome the acknowledgment that legitimate interest under Article 6(1)(f) GDPR may serve as a legal basis for scientific research processing, including where the research has commercial applications. However, this should not be subject to the six-factor framework that is not regulated

in the GDPR and, as discussed before, is contrary to the definition of scientific research established in EU law.
Additional guidance on the application of the balancing test under Article 6(1)(f) in the research context would support consistent implementation. In particular, controllers may benefit from guidance regarding the potential weight of public interests and reasonable expectations of data subjects on societal progress and economic growth whose publicly available data is processed for research, the relevance of safeguards and governance measures in the balancing exercise, and the weight to be afforded to the societal benefits of research outcomes.

Recommendation:

- Provide practical guidance on conducting the legitimate interest balancing test for scientific research processing, including relevant factors and the role of safeguards in supporting a favourable balance.

4.3 Special Categories of Personal Data (Guidelines Section 4.4)

4.3.1 Personal Data Manifestly Made Public (Article 9(2)(e) GDPR)

We acknowledge the importance of the safeguards surrounding the processing of special categories of personal data. The draft Guidelines' requirement that the controller ascertain whether the data subject intended, "explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public" reflects the high threshold applied to this derogation, beyond the letter of the GDPR.

Digital contexts: The draft Guidelines' examples of "clear affirmative action" focus primarily on physical-world scenarios (e.g., participating in a publicly broadcast event). Additional guidance addressing digital contexts would support implementation. In particular, where an individual is posting content publicly in a digital service (including but not limited to platforms requiring users to actively configure audience settings and e.g., selecting a "public" setting, before content is shared, and where users are informed of the public nature of service or their posts, such user actions constitute clear affirmative actions within the meaning of Article 9(2)(e). We encourage the EDPB to consider including examples that reflect these common digital interaction patterns.

Self-posted vs. third-party data: We note the distinction drawn in paragraphs 71-72 between special category data actively posted by data subjects themselves and data posted by third parties. We also note the temporal limitation in paragraph 72 — that making certain data public does not extend to other data within the same category. However, the draft guidance cannot remain at the level of theoretical distinction; it must also address how this distinction is to be operationalised in practice.

The practical application of this framework at scale — particularly for scientific research relying on large volumes of publicly available content — may present implementation challenges. In many cases, the distinction between personal data about the individual himself or herself or referring to a third-party (individual) cannot reasonably be determined for each data point. Moreover, regulators cannot simply assume that posted *content* equates to *personal data*, in particular, when entities conducting research cannot reasonably — or have taken measures to prove that they do not intend to — identify the individuals mentioned in the content at hand. This is precisely the point of the *relative* concept of personal data that is missed in the draft guidelines: regulators should not presume that identification is possible merely because of the volume of “data” processed.

Inferred data: The Guidelines indicate that special categories of data include "personal data that can be used to collate or deduce such information, and sensitive information inferred from the data processed. There are serious concerns about the breadth of this formulation and its compatibility with general principles of EU law:

- The mere theoretical possibility of inference cannot suffice to trigger Article 9 obligations; such an approach would effectively transform any dataset into a repository of special category data. Instead, Article 9 should require an active intent to derive insights relating to the special category, not the incidental and hypothetical possibility to derive sensitive insights, and alongside a clear capacity to do so. This is supported by the CJEU case law. In *OT* (C-184/20), the Court stated that processing liable to *indirectly* reveal sensitive information is "not excluded" from the strengthened protection regime, but this does not create an automatic or systematic trigger or mean "is always included." Similarly, in *Lindenapotheke* (C-21/23), the inference of health data was far from hypothetical: purchasing medication in a pharmacy inherently entails a concrete link to a health condition. This fundamentally differs from large-scale research datasets where, through multi-step aggregation and speculation, one might theoretically yield inferences about sensitive attributes, particularly where researchers lack both the intent and the means to make such inferences about identified individuals.
- Several general principles of EU law militate against an expansive reading:
    - **Legal certainty:** If any dataset becomes subject to Article 9 merely because an inference is *theoretically possible*, controllers cannot ascertain their legal position, rendering the law unforeseeable and inapplicable.
    - **Non-impossibility of obligations:** As confirmed in *Montessori*, C-622/16 P, no one is obliged to do the impossible. Compliance becomes practically impossible if the controller must anticipate every conceivable inference from general-purpose research data.
    - **Intent and negligence as preconditions for liability:** *Deutsche Wohnen* (C-807/21) confirms that only infringements committed *"intentionally or negligently"* can result in fines under Article 83 GDPR. This confirms that the GDPR presupposes a degree of foreseeability and culpability. A framework imposing obligations for unforeseeable inferences — which the controller had no intent to make and took no steps toward — is incompatible with this liability structure.
    - **The relative concept of personal data:** Under *SRB* (C-413/23 P) and *Breyer* (C-582/14), identifiability must be assessed contextually, from the perspective of the specific controller, based on means *"reasonably likely to be used."* In the context of large-scale scientific research using publicly available content, researchers typically lack the intent or the practical means to identify individuals or derive sensitive inferences. The draft Guidelines cannot presume that processing volume equates to processing of personal — let alone special category — data.

Attribution of Article 9 obligations for inferred data: The Guidelines are unclear regarding which controller bears Article 9 obligations where special categories of data are *inferred* from data that do not, on its face, constitute special category data. Where a platform provides access to publicly available posts and metadata, with direct identifiers redacted and no data export permitted, the platform itself does not infer any special categories. Any inference of special category data would be performed by the researcher, using the researcher's own analytical methods, within the research environment. If the platform providing access were held responsible under Article 9 for special categories that researchers might infer from the data made accessible, the platform would need to either pre-screen all publicly available content for potential special category inferences, which is impractical at scale, or restrict access to any content from which

special categories could theoretically be inferred, which would undermine the objectives of DSA Article 40. We would encourage the EDPB to clarify that where a platform provides access to data that does not on its face constitute special category data, and any special category inference is performed by an independent researcher-controller, the Article 9 obligations attach to the researcher's processing rather than to the platform's provision of access.

Proportionality at scale: The requirement that controllers verify platform settings and assess individual data points may present challenges for research involving large datasets (potentially millions of data points and not necessarily personal data). Where a platform's architecture *systematically* requires active configuration of public settings before content is visible to the general public, and this is documented and verifiable at the system level, guidance on whether system-level verification can constitute a proportionate compliance approach (rather than individual post-level assessment) would be of significant practical value.

Recommendations:

- Include examples of "clear affirmative action" in digital contexts, such as actively selecting public audience settings on platforms that require such selection.
- Provide guidance on proportionate approaches to verifying the "manifestly made public" requirement at scale, including the role of system-level governance and platform design documentation.
- **Incorporate an intent-derived foreseeability test** for the application of Article 9 GDPR to inferred data: the heightened obligations of Article 9 should apply only where a controller *actively pursues* the derivation of sensitive insights about individuals identifiable by the controller through reasonable means, or where such derivation is a *foreseeable and inherent* consequence of the processing design. Without such a threshold, the draft Guidelines would render the GDPR unworkable for legitimate scientific research, contradicting Article 13 (freedom of the arts and sciences) and Article 52(1) (proportionality) of the EU Charter, as well as Recital 4 of the GDPR.
- Within the DSA context, clarify that where a platform provides access to data that does not on its face constitute special category data, and any special category inference is performed by an independent researcher-controller, the Article 9 obligations for inferred data attach to the researcher's processing rather than to the platform's provision of access.

5. Obligations to Inform (Guidelines Section 5)

We note the helpful clarifications regarding exceptions from information obligations under Article 14(5) GDPR, particularly where provision of information proves impossible or would require disproportionate effort. These exceptions are of practical importance for research using large volumes of data not collected directly from data subjects.

Transparency cooperation at scale: Paragraphs 92-93 of the draft Guidelines encourage cooperation between controllers, and between intermediaries and researchers, to support compliance with transparency obligations. While this is indeed a helpful principle, we would encourage the EDPB to provide further guidance on how it applies at scale, for example, where a platform provides structured access to multiple vetted researchers within a controlled environment from which data cannot be exported. In such circumstances, one-to-one transparency coordination for each researcher, project, and data subject may not be practicable. We would encourage the EDPB to clarify whether system-level transparency measures, such as platform privacy notices, research environment disclosures, and public documentation of the access programme, can constitute adequate cooperation for the purposes of paragraphs 92-93.

Recommendation:

- Provide guidance on how the transparency cooperation envisaged in paragraphs 92-93 operates at scale, including for entities providing structured data access to multiple researchers.

6. Data Subjects' Rights (Guidelines Section 6)

6.1 Right to Erasure (Guidelines Section 6.2)

We welcome the acknowledgment that data subjects' rights, including the right to erasure, may be subject to exceptions where the processing is necessary for scientific research purposes and where erasure would render impossible or seriously impair the achievement of those purposes.
The Guidelines state that where a controller processes data from "a large number of data subjects, requests of data subjects for erasure of their personal data may not make it impossible or seriously impair the achievement of the scientific research purposes." This formulation may create interpretive uncertainty. Read literally, it could suggest that the larger the research dataset, the less likely individual erasure requests would "seriously impair" the research — and therefore the less likely the controller could rely on the research exception. This would produce a counterintuitive outcome where controllers conducting large-scale, comprehensive research have fewer opportunities to rely on the exception than those working with smaller datasets.

Recommendations:

- Clarify that the assessment of whether erasure would "seriously impair" scientific research should consider the cumulative impact of potential erasure requests (not only individual requests in isolation), the methodological requirements of the research (including completeness, representativeness, and statistical validity), and the nature of the research design.
- Confirm that the scale of a dataset does not, in itself, diminish the applicability of the research exception under Article 17(3)(d) GDPR.

7. Attribution of Responsibility (Guidelines Section 7)

Clear guidance on role attribution is important for collaborative research arrangements and for entities that provide data access to external researchers. The draft Guidelines must approach joint controllership determinations with great care. As scholars including Kuner and Millard have observed, an expansive interpretation of Article 26 GDPR severs the foundational link between **liability and risk-creation**–a principle central to civil and commercial law across EU Member States. As Advocate General Bobek cautioned in *Fashion ID* (C-40/17), disconnecting legal responsibility from factual control renders the concept of joint controllership devoid of meaningful content. While the CJEU acknowledged in *Wirtschaftsakademie* (C-210/16) that joint responsibility does not imply *equal* responsibility, regulatory practice often fails to differentiate, holding entities accountable for processing they cannot influence.
The EDPB should reaffirm that responsibility must remain proportionate to the actual determination of purposes and means. This is particularly critical regarding the DSA. Platforms and researchers should not be considered joint controllers under Article 40 DSA. These arrangements involve independent actors: the researcher independently defines the research

purpose and methodology, while the platform maintains a distinct role. Treating these as joint controllers imposes legal duties on parties who lack the decisional power to discharge them.

The draft Guidelines provide detailed examples of controller and processor determinations in traditional research settings, such as clinical trials, CROs and research consortia. These environments are heavily regulated, and their complexity has historically led to divergent and disharmonized positions among DPAs. The Guidelines would benefit from specific guidance addressing role attribution in contexts subject to different regulatory frameworks. For instance, where an entity provides structured data access to external researchers under a legal obligation like DSA Article 40, the platform and the researcher typically determine their respective purposes and means independently: the platform determines the mechanisms of access, the safeguards applied, and the categories of data made available, while the researcher independently determines their own research objectives and methodology.

Recommendation:

- Clarify that collaborative research arrangements typically give rise to separate, independent controllership, rather than joint controllership or a controller-processor relationship, would be of practical value.

8. Appropriate Safeguards (Guidelines Section 8)

We welcome the guidance on appropriate safeguards under Article 89(1) GDPR, including the emphasis on risk analysis, DPIA requirements, and anonymisation/pseudonymisation. The safeguards framework is essential to ensure that the GDPR's research provisions operate within a framework of robust data protection governance.
While the guidance on appropriate safeguards is helpful, we would encourage the EDPB to clarify that, for entities providing structured research access, architectural and system-level safeguards may constitute appropriate safeguards at the infrastructure level. Safeguards may include, for example, secure processing environments, restrictions on data export, redaction of direct identifiers, and contractual prohibitions on re-identification and onward sharing.

Recommendation:

- Confirm that architectural and system-level safeguards implemented by entities providing research access infrastructure may constitute appropriate safeguards under Article 89(1) GDPR.