MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Response to Public Consultation on EDPB Guidelines 1/2026

On the Processing of Personal Data for Scientific Research Purposes

Submitted by: MDT (Multidisciplinary Team) Date: June 2026

Section 1 — Executive Summary

My Data-Trust ('MDT') welcomes the publication of EDPB Guidelines 1/2026 on the processing of personal data for scientific research purposes. Our response focuses on practical considerations relating to clarity, operational feasibility, and implementation in the clinical research context. This executive summary highlights our key recommendations, while the detailed comments provide further analysis, practical examples, and proposed drafting improvements to enhance the clarity and usability of the Guidelines.

Each comment identifies the relevant paragraph number(s) of the Guidelines and, where helpful, quotes the EDPB text under review. Each comment contains an MDT Opinion sub-section and an MDT Suggestion sub-section.

Key Recommendations

- **DPO and DPIA as safeguards (paras. 49, 81, 149, 151 and 160):** We welcome the recognition of DPO and DPIA as additional safeguards under Art. 89. We suggest extending the recognition of the Data Protection Officer (DPO) as a safeguard in paragraph 49 throughout the Guidelines and explicitly encourage its voluntary appointment as a safeguard under Article 89(1) GDPR, even where not legally required. The limitation of data subject's rights and freedoms, balancing interests of controllers and data subjects, the assessment of applicability of exemptions, such as the one of the art. 4.5.b shall be conditioned by the DPO review and positive advice. The same approach should be adopted for Data Protection Impact Assessments (DPIAs), which conclusions shall receive a DPO dice. The Guidelines should emphasise the value of both measures in ensuring accountability and protecting data subjects' rights in the research context. Accordingly, paragraphs 81, 149, 151 and 160 should expressly refer to the appointment of a DPO and the conduct of a DPIA as recommended safeguards and good practices, rather than presenting them merely as optional compliance measures. Moreover, the guideline shall point to the DPO not only as a safeguard, but as essential part of the data protection governance in the sector.
- **Scientific Research definition:** MDT suggests adopting or more explicitly referencing the OECD's definition contained in Frascati Manual 2015 as the definitional baseline for scientific research, eventually to be supplemented by the six factors (paras. 6, 9, 11). Regarding the factors, we encourage the following modifications: Factor (i) prioritise 'defined objective and methodology' over hypothesis testing (para. 11(i)); clarify that adherence to ethical standards does not necessarily require ethics committee approval in all cases (para. 11(ii)).
- **Broad consent:** We welcome the approach in para. 39 which is greatly needed and invite EDPB to further encourage the use of such broad upfront information which in the context of research increases the overall transparency. The notion of broad consent shall not be hindered by other remarks, such as the suggestion to limit purposes (with the expectation to achieve the minimisation of data). In case of broad consent, the limitation of purposes takes a different meaning and such a statement introduces an uncertainty insofar the use of broad consent is concerned.
- **Adopt a multi-dimensional definition of 'large scale' processing (paras. 65, 149):** Clarify that "large scale" is not determined solely by the number of data subjects, but also by factors such as the volume, variety and sensitivity of the data processed. This would ensure that research involving

few individuals but extensive datasets, such as whole-genome sequencing, qualify without any doubt as large-scale processing.

- **Interpretation of Art. 11(1) GDPR applied to research** (linked to para. 112). MDT suggests that these guidelines should include a section dedicated to providing clarification on the interpretation of this article applied to scientific research. While some input is provided in relation to the exercise of data subjects rights Art.11(2), the lack of clarity on the expectations of paragraph (1) created legal uncertainty. The thorough analysis of the article 11.1 without prejudice to existing national requirements consequent to the application of the article 9.4 or 89 by, for example a DPO, shall be acknowledged in the guideline.
- **Collection of additional (directly identifying) information** to enable exercise of data subject's rights. MDT strongly opposes the requirement to collect additional information to enable exercise of data subject's rights in case of pseudonymised data by the data controller not holding the pseudonymisation key. This would expose the data to unwanted risks and in some instances, it would not even provide sufficient guarantees about the identity of the data subject. Moreover, in our view, it goes against the Art. 11 of GDPR.
- **Right to erasure (para.120):** Include an example addressing the safety and integrity implications of erasure in regulatory research Where erasure would distort a product's safety profile by removing adverse-event data, this should be recognised as a compelling reason to reject the request under Article 17(3)(d).
- **Ethics Committees and patients' representatives' organizations involvement:** We strongly advocate for the involvement of these bodies in the assessment of privacy-related decisions where ethical considerations are relevant (paras. 39, 46, 48, 98, 99, 101 and 111). Ethical and clinical standards such as the ICH GCP guidelines already assign specific responsibilities to Ethics Committees, and in practice they routinely review aspects of data protection insofar as these are linked to participant rights, safety, and welfare. Processors and controllers shall first consult their DPO (where internal or external). The Ethics Committee can further validate eventual exemptions taking into consideration applicable ethical standards. This is particularly valuable given the substantial alignment between ICH GCP principles and key data protection requirements.
- **Transparency and additional information (paras. 48, 86, 106, 108):** The Guidelines should acknowledge that transparency remains a cross-sector challenge and should not become a barrier to research where reasonable measures have been implemented. They should also encourage Member States to develop patient portals and similar tools to facilitate transparency and the exercise of data subject rights and recognize the right not to know as a legitimate limitation on transparency obligations in the context of health research.

  In relation to changes to processing operations (para. 108), clarification is necessary regarding when a new actor or a change of method materially affects the risk profile or data subjects' reasonable expectations such that additional information is required.

- **DPIA and LIA:** We suggest clarifying the relationship between risk assessment, DPIA, Article 89(1) safeguards and the LIA. Safeguards identified through the DPIA should inform the LIA assessment, without requiring a separate safeguards analysis where those measures already ensure an appropriate balance. Indeed, in the opposite, there can be a duplication or, eventually an request for contradictory safeguards that would weaken the level of overall protection. A thorough, DPO reviewed quality DPIA shall be able to identify all the safeguards that make the legitimate balance right.
- **Data collection in clinical trials:** Correct Example 11 to reflect that clinical-trial data collection is often composed of both direct and indirect collection and eliminate the current contradiction between paras. 82, 90-91.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

- **Data Protection roles allocation in research consortia** (Example 25; para. 145): MDT believes the Joint Controllership approach for large consortiums is detrimental to protection of personal data. Instead, the project shall be analysed and split in distinct sub-activities with more lean distribution of responsibilities. We recommend providing dedicated guidance and additional examples on the allocation of data protection roles in large research consortia, reflecting the variety and complexity of governance structures, work package arrangements, and data-sharing models commonly found in collaborative research projects.
- **Roles and controllership:** Clarify the factors determining joint controllership and provide further guidance, including practical examples, on when involvement in research protocol development amounts to joint determination of purposes and essential means (paras. 134, 141–142), particularly in light of upcoming regulatory developments such as the Biotech Act. The Guidelines should distinguish between partners actively involved in defining the protocol and those merely consulted or providing input without influencing key decisions. They should further clarify that the ability to make decisive choices over the purposes and essential means of processing — including through veto powers — is a key indicator of controllership and provide additional examples on role allocation in health data access infrastructures, including federated databases, trusted research environments and national health data access bodies (paras. 134–136, Example 22).
- **Anonymization and pseudonymization (paras. 94, 163, 161):** Clarify that, where personal data are genuinely anonymised in the hands of the recipient, the obligations in paragraphs 94 and 163 concerning the exercise of rights through pseudonyms and re-identification do not apply to that recipient, and should specify what residual obligations, if any, remain.

  Additionally, operational guidance would be useful on the expected level and frequency of de-identification measures using a risk-based approach over long retention periods such as in clinical research, where data may be retained for 15, 25 or more years (para. 161).
- **Information campaigns in genetic research (para. 169):** Provide more detailed guidance on the design and implementation of information campaigns in genetic research. The Guidelines should also clarify the concept of group-level risks and whether the recommendation applies only to isolated population groups or also to rare-disease communities, genetically identifiable families, disease-specific registries, and biobanks involving inherited conditions.**References to non-final or not-yet-applicable instruments (footnotes 11, 29, 138, 140):** The guidelines should use references to Digital Omnibus and other non-adopted instruments with caution, clarifying that they are as provisional.

About us:

MyData-TRUST is registered under Belgian Laws, active since 2017 in the data protection area and dedicated exclusively to the health and life science. Our multi-disciplinary team includes Data Privacy Lawyers, IT Security Specialists and Health data/Clinical Experts providing GDPR related services (such as privacy risk assessments, external DPO as a service, etc.). Our clients include among others Pharmaceutical, Biotech and Medical Devices companies, Contract Research Organisations (CROs), Healthcare providers and Health associations.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Section 2 — Detailed comments

MDT provides below its observations and suggestions, organised by section of the Guidelines. Each comment identifies the relevant paragraph number(s) of the Guidelines and, where helpful, quotes the EDPB text under review. Each comment contains an MDT Opinion sub-section and an MDT Suggestion sub-section.

2.1 — Definition of Scientific Research and Key-Indicative Factors

Paragraph 4 — Complementary Member State Law

MDT Opinion:

> **Para. 4:** *"the EDPB underlines that there is ample room left to, and consequently a need for, complementary Union and Member State (MS) law."*

In practice, many Member States lack provisions specifically governing scientific research data processing outside of clinical trials. While paragraph 4 is an accurate legal observation, it risks normalising fragmentation at the expense of enabling EU-wide research. Recent Union instruments (EHDS, the proposed European Biotech Act) will unfortunately not suffice by themselves to harmonise or stimulate research across the EU.

MDT Suggestion:

MDT calls for a unified Union-level scientific research data framework. EDPB could further build on this guidance to clarify and thus create a more harmonized environment to foster scientific and more specifically health research in EU.

Paragraph 6 — Absence of a Universally Agreed Definition

MDT Opinion:

> **Para. 6:** *"While the EDPB is aware that no universally agreed definition of scientific research exists, it is nonetheless necessary to clarify the concept ..."*

A widely accepted definition does exist in the OECD Frascati Manual 2015, which defines R&D as "creative and systematic work undertaken in order to increase the stock of knowledge" and lists five criteria: novel, creative, uncertain, systematic, and transferable/reproducible. The Frascati Manual is already cited in the Guidelines' own footnotes (footnote 11) but is not applied in the document, creating other (more subjective) factors instead.

MDT Suggestion:

The EDPB should adopt or explicitly reference the OECD Frascati Manual 2015 definition as the primary basis for the concept of scientific research, supplemented by the six key-indicative factors in paragraph 11. This would provide greater legal certainty and align GDPR interpretation with established international norms.

Paragraph 9 — The Term 'Genuinely Scientific'

MDT Opinion:

> **Para. 9:** *"the concept of scientific research purposes in the GDPR covers processing of personal data in research activities that are genuinely scientific."*

The qualifier "genuinely", while intended to prevent misuse, is subjective and susceptible to inconsistent interpretation across Member States and supervisory authorities. It introduces a value judgement that is not grounded in the text of the GDPR itself.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

MDT Suggestion:

The word “genuinely” should be deleted or replaced by a reference to the key-indicative factors set out in paragraph 11. Compliance with those factors is a sufficiently robust and objective test; the additional qualifier adds uncertainty without adding substance.

Paragraphs 10, 19, 88, 89 — Footnotes 11, 29, 138 and 140 — References to Non-Final or Not-Yet-Applicable Instruments

MDT Opinion:

> **Footnotes 11, 29, 138, 140:** *references to Recital 37 of the Digital Omnibus.*

Footnotes 138 and 140 refer to Recital 37 of the Digital Omnibus, and similar references to non-final or not-yet-applicable instruments appear elsewhere in the Guidelines. MDT raises this as a general, horizontal concern affecting the Guidelines as a whole, not only the individual paragraphs in which such references appear. Where the interpretation offered in the Guidelines depends on the wording of an instrument that is still in the legislative process, that interpretation is exposed to change: if the instrument is amended, delayed, rejected, or ultimately adopted with different wording, the corresponding guidance may become inaccurate, internally inconsistent, or misleading. Because controllers rely on the Guidelines for long-term scientific research compliance – often over retention periods of many years – guidance anchored to a moving target creates a real risk of legal uncertainty and of controllers building compliance frameworks on a basis that no longer holds.

MDT Suggestion:

As a general drafting principle, the EDPB should avoid making the interpretation of the GDPR dependent on instruments that are not yet adopted and applicable. Where such references are retained for context, they should be clearly marked as provisional and accompanied by an express statement that they do not affect the interpretation of the GDPR unless and until the relevant instrument is formally adopted and in force. MDT suggests that the EDPB review the Guidelines as a whole to identify all such references and apply this principle consistently, so that the validity of the guidance does not depend on the outcome of separate, ongoing legislative processes.

Paragraph 11, Factor (i) — Methodical and Systematic Approach (Hypothesis vs. Objective)

MDT Opinion:

> **Para. 11(i):** *“The research activities, including formulation and testing of a hypothesis, are conducted following a methodical and systematic approach ... If the research is exploratory or in a preliminary stage, the research may have a stated objective as opposed to a hypothesis.”*

Many valid research designs — including qualitative, descriptive, ethnographic and exploratory studies — are guided by research questions rather than hypotheses. Foregrounding hypothesis formulation as the primary criterion risks excluding legitimate scientific enquiry, even though factor (i) does acknowledge stated objectives for exploratory work.

In addition, where hypotheses are used, the wording could be more precise. In statistical research, it is important to distinguish between the *null hypothesis* and the *alternative hypothesis*, rather than referring generically to “a hypothesis,” as hypothesis testing is based on assessing evidence against the null hypothesis and, where appropriate, rejecting it in favor of the alternative.

MDT Suggestion:

Factor (i) should be revised to reference “a defined objective and methodology” as the primary requirement, with hypothesis testing as one exemplary approach rather than the default expectation. This aligns with the Frascati Manual's broader framing.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Paragraph 11, Factor (iv) — Autonomy and Independence in Commercial Research

MDT Opinion:

> **Para. 11(iv):** *"The research activities are conducted autonomously and independently in relation to the prejudices of the scientific community and other external parties, as well as the researcher's own prejudices, in an environment free from undue pressures."*

MDT does not put this principle in question, but it is harder to demonstrate in commercial research, which is frequently — and by definition — seen as not independent. Concrete examples of how independence can be evidenced in a commercial context are needed.

MDT Suggestion:

The EDPB should provide examples of how independence can be demonstrated in commercial research, such as: use of independent data monitoring committees (IDMCs, as in clinical research), pre-registration of protocols, publication in peer-reviewed journals, and separation of research and commercial functions within an organisation.

Paragraph 11, Factor (v) — Contribution to Society's Knowledge and Wellbeing

MDT Opinion:

> **Para. 11(v):** *"The research activities are carried out with the aim of contributing to the growth of society´s general knowledge and wellbeing. This does not exclude that the research may also aim to further commercial interests."*

In a commercial context, research results may remain confidential for a period of time for legitimate reasons, including the protection of intellectual property, competitive interests, or ongoing product development. This can make it difficult to reconcile this factor with an expectation that research should immediately contribute to society's knowledge. In MDT's view, this criterion risks conflating the nature of the research activity with the timing and manner in which its benefits become publicly accessible. Practical examples would be helpful, such as future publication of results, submission of evidence to regulatory authorities, or the development of products, treatments, or services intended to improve the wellbeing of individuals or populations. In the clinical trial context, it should also be recognised that results are subject to mandatory transparency requirements, including publication through the Clinical Trials Information System (CTIS), ensuring that study outcomes ultimately become publicly available even where certain information remains commercially confidential during the conduct of the research.

MDT Suggestion:

This factor should be decoupled from the immediate public availability of research results. A commitment to eventual dissemination—through scientific publication, submission in a regulatory dossier, disclosure under applicable transparency requirements (such as publication of clinical trial results in CTIS), or deposit in a public repository—should be sufficient to satisfy this criterion. The Guidelines should expressly acknowledge that commercially confidential research may meet this factor where it is reasonably expected to contribute to general knowledge, public health, innovation, or societal wellbeing over time.

Paragraph 11, Factor (vi) — Examples of Contribution to Existing Knowledge

MDT Opinion:

> **Para. 11(vi):** *"The research activities are merited, as they have the potential to contribute to existing scientific knowledge or apply existing knowledge in novel ways."*

There are multiple ways research can contribute beyond those alluded to; the examples given are sparse.

MDT Suggestion:

Additional examples should be provided, including developing or validating biomarkers, applying established statistical methods to new datasets, generating real-world evidence to complement trial data,

applying new techniques to existing datasets, and developing new measurement instruments. MDT recommends overall sticking closer to the OECD definition.

Paragraph 12 (Example 1) — Clinical Trial: Meaning of 'Hires'

MDT Opinion:

> **Example 1 (after para. 12):** *"The pharmaceutical company hires a team of academically qualified and vetted researchers to carry out the scientific research activities necessary to conduct the trial. This corresponds to factor iv (independence and autonomy)."*

In practice, commercial sponsors often use their own internal staff, including employees with academic qualifications. The framing of "hires" implies an external engagement and raises the question of whether internal research teams satisfy the independence criterion, and what "hires" is intended to mean.

MDT Suggestion:

The Example should clarify that qualified researchers may be employees of the sponsor. The independence and autonomy criterion should be met where the team has functional independence in the conduct of the science, regardless of internal/external status, supported by structural safeguards (e.g. IDMC oversight).

2.2 — Research Data Infrastructures

Paragraph 13 — Nature of Infrastructure Operators

MDT Opinion:

> **Para. 13:** *"Personal data may be processed in a research data infrastructure ... for the purposes of making the data available for future research projects within a specific area of research."*

Infrastructure operators are frequently intermediaries rather than data controllers. Established providers such as the European Genome-phenome Archive (EGA) or the IDDI often function as access facilitators or processors, not controllers. The example should be adjusted accordingly.

MDT Suggestion:

The Guidelines should include an example illustrating an infrastructure provider acting as an intermediary or processor, with the controller being the entity that determines the research purposes for which access is sought. Guidance on role allocation along the access pathway (provider, access committee, researcher) would clarify accountability and align with the EHDS.

2.3 — Ancillary Processing Operations

Paragraph 15 — Framing of Ancillary Operations

MDT Opinion:

> **Para. 15:** *"Ancillary processing operations should have a clear scientific research objective, which must be assessed on a case-to-case basis in light of the factors listed at para. 11 ..."*

This should be rephrased. Preparatory activities — cohort identification, data extraction, transfer to a research controller — are destined to support a project with a scientific research objective, but as such they do not themselves have that objective, since the key-indicative factors will not directly apply to them. This is different from side projects of sub-studies, which in addition to the main research purpose aim to ask more research questions.

MDT Suggestion:

Paragraph 15 should clarify that ancillary operations must be clearly and demonstrably in service of a principal activity that satisfies the scientific research criteria, rather than themselves satisfying all six factors. Transfer of personal data to another controller for research purposes should be added as an example of an ancillary operation.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Section 3 — Data Protection Principles

3.1 — Purpose Limitation

Paragraphs 17, 24 and 26 — Further Processing and Indirect Collection

MDT Opinion:

> **Para. 17:** *"If a controller initially collects and processes personal data for non-scientific purposes, but later on decides to process the personal data for scientific research purposes, this is considered further processing for scientific research purposes."*
>
> **Para. 26:** *"the provision of personal data by controller A will be considered further processing if it was not one of the primary processing purposes when the personal data was collected."*

The GDPR already structures this scenario: for Controller A the transfer is a secondary purpose, while for Controller B the receipt from Controller A is indirect collection (Article 14) for its own primary purpose. This structure should not be altered. The current framing introduces terms do not present in the GDPR and risks confusion between secondary use and indirect collection. Paragraph 24 should clarify that, for Controller B, this is not a further purpose but indirect collection.

MDT Suggestion:

The Guidelines should expressly acknowledge that Controller B's processing constitutes indirect collection under Article 14, not a further processing, and should add an example of the full flow (Controller A direct collection/transfer → Controller B indirect collection for research use). Both, Controller A & B can thereafter do their own further use (yet for another research project for example). The difference between further us (also called secondary use) and indirect collection should be explained, as it is poorly understood in practice.

Paragraphs 18, 22 and 23 — Welcome Clarifications

MDT Opinion:

> **Para. 18:** *"Personal data can also be collected for several purposes, amongst which one of the purposes can be scientific research. In such situations, the scientific research purpose is also considered to be a primary purpose of processing."*

Paragraph 18 is a perfect and very welcome clarification, as are paragraphs 22 and 23 on the ability to rely on the same legal basis and the weight of the societal interest in the legitimate-interest balancing test.

MDT Suggestion:

No change recommended. MDT supports these paragraphs and encourages the EDPB to retain them in the final text.

3.2 — Storage Limitation

Paragraph 29 — Specification of Future Research Area

MDT Opinion:

> **Para. 29:** *"If it is not possible to specify the purposes of a future research project at the time of storage, specifying potential research in a certain area of research can suffice."*

This is very welcome and provides the practical flexibility needed for longitudinal and translational research.

MDT Suggestion:

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

No specific change recommended. The link between “area of research” for storage purposes (para. 29) and “area of research” for broad consent (section 4.1.2.1) should be made explicit and carried through consistently.

Section 4 — Lawfulness

4.1.1 — Freely Given Consent

Paragraph 38 (Example 7) — Exclusion of Vulnerable Data Subjects

MDT Opinion:

> **Example 7 (after para. 38):** *“On the basis of this advice, the institute conducting the study decides to proceed on the basis of consent but will exclude data subjects that it determines are not in a position to give free consent.”*

While logical from a GDPR consent perspective, excluding the participants who cannot give free consent will likely introduce a non-negligible bias in the research, since the population most affected by the disease would be underrepresented.

MDT Suggestion:

Rather than recommending exclusion, the Guidelines should indicate that for the sub-population that cannot provide free consent, controllers should explore an alternative legal basis (e.g. Article 6(1)(e) public interest, or Article 6(1)(f) legitimate interest together with the applicable Article 9(2), derogation for special categories). The example should be revised to present reliance on a different legal basis for that sub-set of participants as the preferable option to preserve research integrity and inclusivity.

Furthermore, as proposed elsewhere in the Guidelines, the involvement of patient representatives would help ensure that appropriate safeguards are developed and implemented, while ensuring that the interests, perspectives, and specific needs of these populations are adequately taken into account.

Paragraph 39 — Remuneration and Freely Given Consent

MDT Opinion:

> **Para. 39:** *“if the remuneration would constitute a significant part of the data subject’s regular income, it is more likely that it would affect whether consent was freely given or not.”*

First, the word remuneration is not accurate and should be compensation to align with ICH GCP guidelines. Further, for those cases where ethics committees already review the level of remuneration, and judges it acceptable, this should suffice. As formulated, the criterion may lead controllers to collect the data subject's income (data not otherwise required) to validate the acceptability of consent going against the principle of data minimisation and would render a duplication of assessment over the same subject.

Please note that as per ICH GCP: 1.2.8, if the trial participants are compensated for their participation in the trial, the IRB/IEC should review both the amount and method of payment to participants to assure that neither presents problems of coercion or undue influence on the trial participants. There are already other mechanisms aimed to protect trial participants as, those stating that payments to a participant should be timely, prorated and not wholly contingent on completion of the trial by the participant; that reasonable reimbursement of expenses incurred by participants, such as for travel and lodging, is not coercive; and that the IRB/IEC should ensure that information regarding payment to participants, including the methods, amounts and schedule of payment to trial participants, is set forth in the informed consent materials and any other information to be provided to participants.

MDT Suggestion:

The Guidelines should state that ethics committee approval of the remuneration level is a sufficient safeguard for assessing whether consent is freely given. Controllers should not be required to assess

individual participants' financial situations. The formulation in paragraph 39 should be amended to avoid creating an implicit conflict with data minimisation.

4.1.2 — Specificity of Consent (Broad and Dynamic)

Paragraph 42 — Specificity of Purposes in Research

MDT Opinion:

> **Para. 42:** *"Controllers should opt for a mechanism of obtaining consent that provides data subjects with sufficient specificity of the purposes of processing and a high level of data protection over time ..."*

In research, the notion of "sufficient specificity" is far more granular than in other fields and risks being confused with ethical requirements and the need to know exactly what research is being done.

MDT Suggestion:

The Guidelines should distinguish the GDPR's purpose-specificity requirement from ethical or protocol-level specificity, and confirm that, for the purposes of consent under the GDPR, delimitation to an area of research (with appropriate safeguards) provides sufficient specificity.

Paragraph 44 — What Is 'Already Known' in Broad Consent

MDT Opinion:

> **Para. 44:** *"controllers intending to process personal data for scientific research purposes on the basis of broad consent should define the purposes of future research as clearly as possible."*

The concept of what is "*already known*" at the time of collection is not explained and should be clarified.

MDT Suggestion:

The Guidelines should add that controllers should provide information of "what is already known" regarding the research at the time of the collection. The notion of "what is already known" refers to information on the research for which a protocol or plan is already finalised or at an advanced stage at the time consent is sought, whereas research areas or objectives that are defined but lack detailed protocols may appropriately remain the subject of broad consent.

Paragraph 45 — Purpose Delimitation and Data Minimisation

MDT Opinion:

> **Para. 45:** *"The delimitation of the purpose should enable controllers to determine what personal data are necessary to process ..."*

This is not always correct. Some specified purposes result in a collection sufficiently large to enable a very broad panel of later purposes; others do not. The statement of a direct relation between data minimisation and purpose limitation is therefore incorrect as a general proposition. (The accompanying recognition that purpose can be delimited by expected outcomes is very welcome.)

At the same time, in clinical research, a clearly defined purpose remains important for assessing the necessity and proportionality of data collection. This is reflected in ICH E6(R3) and ICH E8(R1), which promotes a Quality by Design approach whereby each data element collected should be justified by the study objectives, participant safety, regulatory requirements, protocol compliance, or planned statistical analyses, thereby avoiding unnecessary data collection.

MDT Suggestion:

Paragraph 45 should acknowledge that the relationship between purpose limitation and data minimisation is not necessarily linear. Broad consent purposes may justify broader data collection where scientifically motivated, provided data minimisation is applied within each individual research project using the data.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Paragraph 46 — Transition from Broad to Dynamic Consent

MDT Opinion:

> **Para. 46:** *"then it should ask the data subjects to consent to that individual research project (or stage thereof) – i.e. rely on dynamic consent."*

This is correct, unless an exemption applies (notably Article 14(5)(b)), which the text does not acknowledge at this point.

MDT Suggestion:

A cross-reference to the exceptions under Article 14(5)(b) — in particular where informing data subjects would seriously impair the research objectives — should be added to paragraph 46, so controllers are aware of the full range of options before defaulting to individual consent requests. The use of the article shall be subject to the prior DPO review.

In addition, ethics committees may be well placed to assess whether the scope of broad consent remains appropriate in the specific research context and whether a future research project remains within that scope. The EDPB could expressly mention, in paragraph 46 or in the related safeguards section, that ethics committee review (or equivalent research oversight) may be considered a relevant Article 89 safeguard when assessing the appropriateness of the scope of broad consent and the reasonable expectations of data subjects in health and clinical research.

Paragraph 48 — Broad Consent Safeguards: DPO advice, Ethics Oversight and Patient Portal

MDT Opinion:

> **Para. 48:** *"controllers should adopt measures that enable data subjects to receive information about the processing of their personal data, for example by subscribing to a newsletter."*

In clinical research, any communication to patients normally, besides being eventually reviewed by the DPO, needs to pass through an ethics committee, and there is no one-stop-shop for this in the EU. A newsletter issued without EC review may itself breach ethical standards.

MDT also notes a structural tension specific to pseudonymised research: a newsletter-based approach generally requires the controller to maintain contact details linked to participants over time, which is difficult where the research dataset is intended to remain pseudonymised and where a clear separation should exist between contact information and research data. Pull-based mechanisms such as participant portals reduce the need for continuous processing of contact details and better preserve that separation.

MDT Suggestion:

The Guidelines should add that, in clinical and medical research, participant communications should be reviewed by the DPO and then submitted to (or at least noted by) the relevant ethics committee. A patient-facing web portal — accessed by participants at their own initiative — is generally preferable, as it reduces unsolicited contact while meeting transparency obligations and allowing patients to have more control over their data. In some cases, a page on the publicly available webpage is enough. The link can be provided in the information. In some contexts, where a more direct contact is necessary, it would be technically possible to provide access without collection or use of the full name or even an e-mail.

In the long term, the real solution for this dilemma lies in the opportunities offered by e-health and EHDS. For instance, there are two complementary implementation layers that could be envisaged.

1) **Member State–level infrastructure:** The EDPB could encourage Member States to develop national patient or participant portals which provide citizens with a secure, state-operated digital environment for managing and accessing their health data. In France, Mon espace santé is a government-run platform enabling individuals to store, access, and share their health documents (such as prescriptions, test results, and medical reports) with healthcare professionals. It is built

around strong authentication and user control, allowing patients to manage access permissions and track data usage. A similar model extended to clinical research would allow participants to centralise study-related information and exercise GDPR rights in a trusted, public infrastructure rather than through fragmented sponsor systems.

2) **Sponsor-level implementation:** Sponsors could additionally operate study-specific participant portals aligned with the same principles, using a pseudonymised-by-design approach in which only study identifiers are processed, and no direct identifiers are visible to the sponsor.

Core features would include:

- participant access to study information and updates
- structured GDPR rights requests (access, rectification, withdrawal, consents)
- secure messaging via study identifiers
- communication of safety updates and results
- preference management for future research involvement

Requests would be routed to the appropriate controller via the investigator site, which retains the link to participant identity.

Paragraph 49 — DPO as Safeguard

MDT Opinion:

> **Para. 49:** *"An oversight body may include a representative of the research participants, experts in the respective scientific research field, experts in data protection, as well as the data protection officer (DPO) ..."*

The recognition of the DPO as a safeguard is welcome. A further option would be to always designate a DPO, at least where Article 9 (special categories) is concerned.

MDT Suggestion:

The Guidelines should encourage voluntary DPO designation as a safeguard whenever special categories of personal data are processed for research, even where appointment is not legally mandatory.

Paragraph 53 — Research Consent as an Additional Safeguard

MDT Opinion:

> **Para. 53:** *"Such consent is not required by the GDPR but may be considered as an additional safeguard according to Article 89 GDPR."*

Treating ethical/legal research consent as an additional Article 89 safeguard is an excellent clarification.

MDT Suggestion:

No change recommended. MDT strongly supports this clarification and encourages its retention.

4.4 — Special Categories of Personal Data

Paragraph 63 — Sequencing of DPIA, Article 89(1) Safeguards and the LIA

MDT Opinion:

> **Para. 63:** *"the controller should take the Article 89(1) safeguards into account in the balancing test."*

The concern is not the need to implement safeguards, which MDT supports, but the structure of the reasoning. As drafted, paragraph 63 may give the impression that controllers must conduct a second, separate risk assessment inside the legitimate interest assessment (LIA), in addition to the DPIA or risk

analysis already carried out for the research. This creates uncertainty, because the DPIA and the LIA serve different purposes: the DPIA identifies risks and the appropriate safeguards, whereas the LIA assesses whether, after those safeguards are taken into account, the controller's legitimate interest is overridden by the rights and freedoms of data subjects.

MDT Suggestion:

The EDPB should clarify the expected sequence. For scientific research, controllers should first conduct the risk analysis or DPIA where required, identify the necessary Article 89(1) safeguards, and then reflect those safeguards in the LIA when assessing the balance. If the balance already stands once the safeguards identified through the DPIA or risk analysis are taken into account, no additional, separate "LIA-specific" safeguards assessment should be required.

Paragraph 65 — Definition of 'Large Scale' for Special Categories

MDT Opinion:

> **Para. 65:** *"If controllers process special categories of personal data on a large scale, they must assess and mitigate the risks associated with such processing through a DPIA."*

This is a very welcome clarification. However, "large scale" is undefined and risks being read solely in terms of the number of data subjects. This would exclude scenarios involving few individuals but very large volumes of sensitive data (e.g. whole-genome sequencing of ten people).

MDT Suggestion:

The EDPB should add to the document a multi-dimensional definition of "large scale" for research, taking into account the volume, variety and sensitivity of data in addition to the number of data subjects, so that even data on ten people may amount to large-scale processing.

Section 5 — Obligations to Inform

5.1 — General Transparency Obligations

Paragraphs 77–79 — Contact Details, Portals and the Clinical Research Context

MDT Opinion:

> **Para. 77:** *"it should give data subjects an opportunity to voluntarily provide contact details ... even if the purposes for processing personal data do not require the processing of contact details."*

In medical research, voluntary provision of contact details harms pseudonymisation, infringes ICH-GCP, and increases privacy risk by making confidentiality harder to ensure outside the therapeutic relationship. It also sits in tension with Article 11. A portal that does not require provision of contact details (the patient receiving a connection code) is preferable. Contact by mail or telephone (para. 78) should be reserved to hospitals or structures naturally in direct contact with patients, and any portal (para. 79) should sit at the clinical trial site, not the sponsor.

MDT Suggestion:

The Guidelines should distinguish obligations by controller type. For sponsors of clinical trials and research conducted through healthcare facilities, transparency should be discharged primarily through the treating institution rather than direct sponsor-to-patient contact. Patient portals linked to existing health e-infrastructure (including national e-health applications) should be expressly recommended as a privacy-by-design solution; direct collection of contact details by sponsors should be flagged as a last resort.

Paragraph 80 — Privacy Dashboard and the EHDS

MDT Opinion:

> **Para. 80:** *"Controllers should also consider providing a privacy dashboard, as described in the Guidelines on transparency ..."*

It is a pity that the EHDS is not cited for medical research here; it would be an appropriate way to ensure privacy with a secure connection and without providing patient contact details to the sponsor.

MDT Suggestion:

Paragraph 80 should reference the EHDS as an appropriate infrastructure for privacy dashboards and secure participant information in medical research, avoiding the transfer of patient contact details to the sponsor.

Paragraph 81 — Contact Point and DPO

MDT Opinion:

> **Para. 81:** *"controllers should consider setting up a contact point, either digital or analogue – but preferably both – through which data subjects can pose questions, get information or exercise their data protection rights."*

It is unclear how this differs from the DPO. The GDPR requires a means of contacting the controller, but this can be simplified: the DPO should be sufficient, and a DPO should be mandatory for scientific research.

MDT Suggestion:

The Guidelines should clarify that the DPO, where designated, is a sufficient contact point for data subject requests in research and should encourage voluntary DPO appointment — treated as an Article 89(1) safeguard — for all research involving special categories of personal data.

5.2 — Direct Collection

Paragraph 82 (Example 11) — Clinical Trial as 'Direct' Collection

MDT Opinion:

> **Example 11 (after para. 82):** *"Information to data subjects whose personal data is directly collected from the data subject through a clinical trial."*
>
> **Para. 91:** *"New personal data generated in the course of a research project will fall within the scope of Article 14 of the GDPR and are not considered as collected directly from data subjects."*

Clinical trials involve a mixture of direct and indirect collection: much research data is extracted from samples or complex examinations or derived through calculation by site staff. Direct contact is not the same as direct collection. Example 11 is mis-titled, as paragraph 91 itself confirms. The interview example (Example 12) is, by contrast, an appropriate illustration of direct collection.

MDT Suggestion:

The title and framing of Example 11 should be corrected to state that the data are partly directly collected, reflecting that clinical trial data collection is a mixture of direct (interviews, questionnaires) and indirect (clinical observations, sample analyses, derived endpoints) collection, consistent with paragraph 91.

5.3 — Further Processing for Scientific Purposes

Paragraphs 86 and 106 — The Right Not to Know

MDT Opinion:

> **Para. 86:** *"the controller should make sure that data subjects can stay informed, in accordance with Articles 12 and 13 GDPR."*

Information is treated as near-absolute. This does not adequately address the right not to know, nor the reality that patients may leave the centre where they are followed without notice. A pull-based portal, ideally

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

part of the e-health ecosystem rather than private portals, is more appropriate in health research. Paragraph 106 touches on this, but the right is broader and can extend to “push”-type of information which may be perceived as too invasive in medical context.

MDT Suggestion:

The Guidelines should explicitly acknowledge the right not to know as a potential limitation on the obligation to inform in health research, cross-reference paragraph 106, and develop how this right modifies transparency obligations, distinguishing “push” (controller-initiated) from “pull” (participant-initiated) information models. An encouragement of implementation (by Member States) of a more appropriate model, such as a possibility for sponsors to provide an EC-approved summary to a central location securely accessible through national e-health applications to research participants should be described.

Paragraphs 87–88 — Deletion of Contact Details and Site vs. Sponsor Role

MDT Opinion:

> **Para. 87:** *“Controllers should not knowingly delete contact details if they intend to or anticipate that they will further process personal data for scientific research purposes.”*
>
> **Para. 88:** *“If the controller has identifiers ... it should make reasonable efforts to acquire contact details if they are readily available and acquisition would not require a disproportionate effort.”*

In clinical research, this obligation properly belongs to the treating institution (hospital/trial site), not the sponsor — it is the site's mission. For the sponsor, holding direct identifiers is not possible and would undermine pseudonymisation. Even for the hospital, not everything that is possible is appropriate, as re-acquiring contact details may be invasive.

MDT Suggestion:

Paragraphs 87–88 should attribute the obligation to the healthcare institution or trial site that holds direct contact information, not to the sponsor or secondary research controller. Guidance for the sponsor should be framed around working through the institution, without the sponsor itself holding direct identifiers.

MDT therefore suggests that the EDPB add a clarification, disclaimer or footnote stating that paragraphs 86–87 should be applied in a context-specific manner: feasible in some models, such as registries, cohorts or research infrastructures where participant contact is already part of the governance model, but not necessarily appropriate or feasible in clinical trials and certain health research projects, particularly where private sponsors intentionally do not hold contact details. The paragraphs should not be understood as requiring controllers to retain or create contact datasets where this would conflict with data minimisation, pseudonymisation safeguards, or established sponsor–site separation models.

Paragraph 89 — Indirect Information Channels

MDT Opinion:

> **Para. 89:** *“Advertising in public spaces, on the television or radio, in newspapers – in particular local media or online ...”*

Advertising in public spaces and mass media would not be appropriate for the private sector in many contexts. Reliance on patient organisations, by contrast, is a good suggestion.

MDT Suggestion:

The Guidelines should temper the public-advertising channels for sensitive or private-sector research and give greater prominence to information provided through associations representing research subjects (patient organisations, trade unions, non-profits).

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

5.4 — Indirect Collection

Paragraph 90 — Indirect Collection Beyond Controller-to-Controller Transfers

MDT Opinion:

> **Para. 90:** *"When a controller receives personal data from another controller and intends to process it for scientific research purposes, the obligation to inform pursuant to Article 14 GDPR applies."*

Indirect collection is not only from another controller — a key example is data derived from biological samples. If trials are treated as direct collection, it is inconsistent that we inform patients about data to be collected; that is an Article 14, not Article 13, requirement.

MDT Suggestion:

Paragraph 90 should acknowledge that indirect collection in research may arise from the analysis of biological samples or from derived data generated by site staff, not only from receipt of data from another controller, and should set out appropriate transparency approaches for each scenario.

Paragraph 94 (Example 14) — Pseudonym as Identifier; Length of the Chain

MDT Opinion:

> **Para. 94:** *"the data subjects should be informed about how they can exercise their rights, for example by providing the pseudonym relating to their personal data."*

This is not enough — a pseudonym can be known to the family and is not safe enough to protect confidentiality; the role of a second pseudonymisation is unclear. Moreover, paragraph 83 and Example 14 assume a short (two-node) chain, but in further use by third parties the chain may be much longer and the requester's identity hard to prove after several cycles of pseudonymisation, while the data remains non-anonymous; fulfilling the request might require an attempt to re-identify, endangering the data.

MDT Suggestion:

The Guidelines should explore privacy-preserving mechanisms for identity verification that do not compromise confidentiality, such as second-level pseudonymisation, verification through the treating institution, or secure e-health identity tokens. They should also acknowledge that real-world data-sharing chains may be considerably longer than the two-node example, and address how rights are exercised in those longer chains.

In addition, the handling of such requests could be managed through a clearly separated function or body, such as the DPO, to preserve the separation between identifiable data and research data. The EDPB could clarify how the mechanism in paragraph 94 can be implemented safely without weakening pseudonymisation, confidentiality or organisational firewalls.

Paragraphs 98–99 and 101 — DPO and Ethics Committee Role in Exemption Assessment

MDT Opinion:

> **Para. 98:** *"There will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects."*
>
> **Para. 101:** *"the controller should consider the safeguards that it has adopted pursuant to Article 89(1) of the GDPR, as well as measures to provide information indirectly."*

These paragraphs do not reference the role of a DPO nor of the ethics committees in confirming the non-feasibility of information or whether patients are already sufficiently informed. First, the DPO shall give the opinion and advice with regards to the eventual limitation of data subject rights. This advice and the final decision of the controller can be further assessed by the EC. ECs are institutionally well placed to make this assessment. The specific examples in paragraph 101 are very welcome.

MDT Suggestion:

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

The Guidelines should state that the fact that individual information is not feasible (or would endanger the research or participants) shall be reviewed by the DPO and further confirmed by an ethics committee, providing is strong evidence supporting reliance on Article 14(5)(b). A reference to the Helsinki Declaration 2013 (Article 32) and relevant ICH-GCP provisions should be added at paragraph 101.

MDT further notes that the distinction between impossibility and disproportionate effort is itself unclear. Paragraph 98 states it may be impossible to provide information where the controller cannot obtain contact details despite reasonable efforts – but this could equally be classified as disproportionate effort. The Guidelines should clarify whether the controller must actually try and fail despite reasonable efforts, or whether it may justify on paper that such efforts would not be reasonable. This matters in scientific research: attempting to obtain contact details may itself amount to an attempt to re-identify data subjects, thereby weakening protection. Either obtaining contact details is simple and straightforward, in which case the controller should do it, or the steps required would weaken protection to an unreasonable extent, in which case the matter should fall within the justification of impossibility or disproportionate-effort assessment. MDT therefore suggests that controllers should conduct and document the impossibility to contact and/or make a disproportionate-effort assessment, with the Guidelines presenting the relevant elements as factors to weigh for and against rather than as fixed examples, given that the same example may be acceptable in one type of research but not another. Such justification or assessment could be submitted to an , after having been reviewed by a DPO to an Ethics Committee (or equivalent research oversight) for independent review. This shall release the Controller from the obligation to (try to) contact data subjects.

Paragraph 104 — Disclosure 'Required by Law' and Regulatory Bodies

MDT Opinion:

> **Para. 104:** *"If, pursuant to Union or MS law, a controller must obtain or disclose personal data for scientific research purposes ..."*

In clinical trials, disclosure is technically required not by the law itself but by drug agencies or HTA bodies. It is unclear whether this is assimilated to "required by law" given their executive power under specific legislation.

MDT Suggestion:

The Guidelines should clarify that obligations imposed by regulatory authorities (medicines agencies, HTA bodies) acting under specific legislation shall be treated as disclosure "expressly laid down by Union or MS law" for the purposes of Article 14(5)(c).

Example 16 — Informing Children

MDT Opinion:

> **Example 16 (after para. 103):** *"the researchers would normally be obliged to inform both the children and parents or guardians of the processing of personal data."*

More guidance on informing children — including very young children or babies — would be welcome from the EDPB.

MDT Suggestion:

The EDPB should provide dedicated guidance on how transparency obligations apply where the data subjects are children, including very young children, and how the role of parents or guardians interacts with those obligations in a research context.

Paragraph 106 — Right Not to Know (Welcome)

MDT Opinion:

> **Para. 106:** *"a data subject has provided personal data for medical research and has requested, in line with national law, to not be informed about discoveries about their health or wellbeing."*

This paragraph is very welcome.

MDT Suggestion:
No change recommended, save that (as noted at paragraphs 86 above) the right not to know should be treated more broadly and connected to the general transparency obligations, not only the confidentiality exception.

5.5 — Changes to Processing Operations

Paragraph 108 — Changes Requiring Additional Information

MDT Opinion:
MDT welcomes the examples provided in paragraph 108. However, further practical clarification would be useful for clinical research.

MDT Suggestion:
First, the Guidelines should clarify when a new research partner remains within a category of recipients already described in the privacy notice, and when it becomes a new research partner that data subjects would not reasonably expect (point 4 of paragraph 108). Second, the Guidelines should clarify when a change to the scientific method or technology materially changes the risk profile (point 6 of paragraph 108). Not every scientific or technical change should require fresh information – a minor adjustment to a statistical analysis, for example, should not.

Finally, the Guidelines should clarify that additional information is required only where the change materially affects the risk profile or the reasonable expectations of data subjects.

Paragraph 110 — Delayed Execution of Announced Research

MDT Opinion:

> **Para. 110:** *"changes that would normally not require any additional information to the data subjects include: Regularly re-occurring studies that remain the same from time to time ..."*

The list of changes not requiring additional information should also include delayed execution of what was already announced — for example, where further research was described by disease area, there should be no need to inform about each individual sub-project within that larger, already-explained purpose (linking to the granularity of purpose under broad consent).

MDT Suggestion:
Add to the paragraph 110 list an example of delayed execution of previously announced research within an already-communicated research area, confirming no additional information is required for individual sub-projects falling within that purpose.

Section 6 — Data Subjects' Rights

6.1 — General

Section 6 (Entire) — Absence of Reference to DPO and Ethics Committee

MDT Opinion:

> **Para. 111:** *"Chapter III of the GDPR, on data subjects' rights, includes two specific provisions that are of particular importance when controllers process personal data for scientific research purposes ..."*

It is unfortunate that, throughout the rights section, the possibility to refer to the role of the DPO and an ethics committee ('ECs') at least in the medical research context is not mentioned even once, despite DPO sand ECs systematically reviewing how protocols handle erasure, objection and access.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

MDT Suggestion:

Throughout Section 6, where the medical research context arises, a cross-reference should be added to the involvement of the DPO and ethics committees in assessing the feasibility of exercising data subject rights, reflecting the integrated governance structure of medical research.

Paragraph 112 — Derogations and Article 11

MDT Opinion:

> **Para. 112:** *"Article 89(2) of the GDPR permits derogations – In Union or MS law – from the rights in Articles 15, 16, 18, 19 and 21 ..."*

Derogations from data subjects' rights are also linked to Article 11 (processing not requiring identification), which should be mentioned here. Article 11 GDPR clearly states additional data shall not be required to be collected for the only sake of compliance with this regulation and grants exemption from the rights described in the Articles 15 to 20. In MDT view Art 11 can be used to support the derogation cited in the Art. 89(2), including in the absence of any additional statement in any other Union or MS law, where the impossibility or disproportionate effort needed to contact data subjects have been documented.

MDT Suggestion:

Paragraph 112 should cross-reference Article 11 GDPR, explaining how the inability to identify data subjects interacts with the exercise and limitation of rights in the research context (granting the derogations of the Art 89(2).

Additional Point — Clarification on Article 11 GDPR in scientific research

MDT Opinion:

In many research projects, the controller processes pseudonymised (coded and key-separated) personal data. In line with established ethical standards, it is particularly important that trial sponsors do not hold the re-identification key. Although this setup is common in scientific and clinical research and may also result from the application of safeguards under Article 89(1) GDPR, it is noteworthy that the Guidelines do not explain the core meaning and implications of Article 11(1) GDPR in this context.

MDT Suggestion:

The Guidelines should clarify how Article 11(1) GDPR applies in scientific research. It would be useful to clarify that controllers should not be required to maintain, acquire or process additional identifying information solely to enable compliance with the GDPR where identification is not necessary for the research purposes. The Guidelines should also recommend that controllers document their assessment under Article 11 GDPR.

6.2 — Right to Erasure

Paragraph 115 — Withdrawal of Consent and Legal Obligation

MDT Opinion:

> **Para. 115:** *"Unless there is another legal basis that justifies continued retention of the data, personal data must be erased following withdrawal of consent."*

Where erasure does not apply because of a legal obligation to retain (e.g. statutory retention periods in clinical research), the relevant legal obligation should be cited expressly. Moreover, the right of erasure may also be limited through the application of exemptions of the Art. 11 or Art 89. This shall also be taken into account.

MDT Suggestion:

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Paragraph 115 should expressly reference the legal-obligation ground (and Article 17(3)(b)) as a situation where erasure does not apply notwithstanding withdrawal of consent, citing clinical-research retention obligations as an example. Moreover, the text shall be adjusted to: "*Unless there is another legal basis that justifies continued retention of the data or an exemption of Articles 11 or 89 applies, personal data must be erased following withdrawal of consent.*"

Paragraph 120 — Erasure, Number of Subjects and Bias/Safety

MDT Opinion:

> **Para. 120:** *"if a controller processes personal 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."*

It is important to note that the need to retain data it is not only about numbers. Erasure can induce bias even within a large cohort — for example, where a single participant experienced a very serious adverse effect. If such data is deleted, one would conclude the drug is safer than it is. The number-of-subjects framing is therefore incomplete in safety-critical research.

Further, for clinical trials subject to ICH-GCP, sponsors are required to retain essential study records to ensure data integrity, traceability, and verification of study results. Deletion of source records, informed consent documentation, laboratory results, adverse event records, or audit trails could prevent inspectors from reconstructing the study and verifying the reported outcomes, thereby compromising data integrity, safety assessments, and the reliability of the study conclusions.

For studies outside the scope of ICH-GCP, while specific record-retention requirements may differ, the same concerns generally apply. Deletion of key study documentation may impair the ability to verify findings and ensure the reliability of the research results.

MDT Suggestion:

Paragraph 120 should include an example addressing the safety and integrity implications of erasure in regulatory research (ICH-GCP obligations, pharmacovigilance, post-market surveillance). Where erasure would distort a product's safety profile by removing adverse-event data, this should be recognised as a compelling reason to reject the request under Article 17(3)(d), regardless of cohort size.

Section 7 — Attribution of Responsibility

7.1 — Controller

Paragraphs 134–135 — Welcome Clarifications

MDT Opinion:

> **Para. 134:** *"the fact that an organisation provides research funding or is consulted in the process of drafting a research protocol ... is not in itself sufficient to attribute the role of a controller (or joint controller)."*
>
> **Para. 135:** *"an entity or an individual may be qualified as a controller even though it does not process personal data at all, only process personal data to a limited extent, or only process pseudonymised data."*

These are very nice clarifications and are strongly supported.

MDT Suggestion:

No change recommended. MDT supports paragraphs 134–135 and encourages their retention.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

Paragraph 136 — Add a CRO to the Sponsor Example

MDT Opinion:

> **Para. 136:** *"The sponsor, which mainly process pseudonymised data, is nonetheless still regarded as a controller (or a joint-controller) because it determines purposes and means of processing personal data in a clinical trial ..."*

It would be better to add a CRO to this example, since the sponsor sometimes processes only limited amounts of personal data — doing so would make the example more robust.

MDT Suggestion:

Paragraph 136 (or a related example) should incorporate a CRO to illustrate the sponsor (controller, determining purposes and essential means) and CRO (processor, implementing the protocol under instruction) distinction in a multi-party clinical trial.

Paragraph 137 — Researchers as Controllers; 'De-badging' of Sites

MDT Opinion:

> **Para. 137:** *"individual researchers, such as researching healthcare staff, laboratory technicians or other persons involved in scientific research are generally not considered controllers, but rather acting under the authority of a controller."*

This is a good example. In practice we see hospitals seek to disclaim controllership for clinical trials while their entire infrastructure is used for the research. However, the way this part is currently phrased may be misleading, since it may be understood investigators are acting under the direct authority of the Sponsor, which in case of a clinical trial will not be accurate. An example would prevent such a misunderstanding from occurring.

MDT Suggestion:

> The Guidelines could note that an institution/hospital whose infrastructure and staff are integral to the conduct of the research cannot simply disclaim its data protection responsibilities (either, controller, joint controller, or processor as is the case in some countries), reinforcing the functional approach to role attribution. "…*, but rather acting under the authority of a controller. For example in a clinical trial, investigators would typically act under the authority of the clinical site."*

7.3 — Joint Controllers

Paragraphs 134–136 (Example 22) — Role Allocation in Health Data Access Infrastructures

MDT Opinion:

> **Example 22 (paras. 134–136):** *role allocation between a university operating a research database and a company accessing data for its own research purposes.*

MDT welcomes Example 22. However, additional practical guidance would be useful for newer health data access models, including federated databases, trusted research environments and health data access bodies. Increasingly, health data reuse does not operate through a simple model in which one controller transfers a dataset to another; instead, data may remain within a controlled infrastructure and researchers may access it only under strict conditions. In Belgium, for example, the Health Data Agency acts as a trusted intermediary between organisations that need health data (researchers, health authorities) and those that hold it (hospitals, care providers), supporting access requests and ensuring compliance with security, confidentiality and ethical requirements.

In such models several actors may be involved: the healthcare provider or data holder; the health data access body or trusted intermediary organising access conditions; the secure environment or infrastructure

through which data are made available; and the researcher or company using the data for a specific project. The practical difficulty is that the researcher may determine the scientific purpose of its project but may not freely determine all essential means: access conditions, security measures, permitted outputs, data minimisation requirements and technical restrictions may be imposed by the access body, the infrastructure, or applicable law. This connects to MDT's observation at paragraph 13 that infrastructure operators frequently act as intermediaries or processors rather than controllers.

MDT Suggestion:

The EDPB should provide additional examples on role allocation in health data access infrastructures, including federated databases, trusted research environments and national health data access bodies.

Paragraphs 141–142 — Participation in Drafting a Research Protocol and Joint Controllership

MDT Opinion:

> **Paras. 141–142:** *"where several parties participate jointly in the drafting of a research protocol that determines the purposes and essential means of processing, this may suffice for those parties to be considered joint controllers."*

MDT welcomes paragraphs 141 and 142, including the clarification that agreeing to and adhering to an already established research protocol is not always sufficient to create joint controllership. However, further practical clarification would be useful on the level of participation in the drafting, review, amendment or approval of a protocol that suffices to amount to joint determination of purposes and essential means as opposed to 'being consulted' (as stated in paragraph 134). This is particularly relevant in clinical research, where parties are involved to differing degrees.

Scenario 1 – Joint protocol design: a sponsor, university hospital and research institute jointly define the study objectives, methodology, endpoints, data categories, inclusion and exclusion criteria, and future research uses. Joint controllership may be easier to identify here, as the parties jointly determine purposes and essential means.

Scenario 2 – Site adherence to an established protocol: a sponsor develops the protocol; a hospital site receives the final protocol, signs the clinical trial agreement, recruits participants and enters data in accordance with the sponsor-defined protocol. The site's agreement to follow the protocol should not automatically mean it participated in determining purposes and essential means.

Scenario 3 – Scientific or operational comments on a draft: a sponsor asks investigators or sites to comment on feasibility, recruitment criteria, visit schedules or patient burden, and accepts some comments before finalising. It may be unclear whether the site merely provided input or participated in determination.

Scenario 4 – Material influence: a hospital or investigator proposes substantial changes to objectives, endpoints, data categories, population criteria or future use, which are incorporated. Involvement may be closer to joint determination, but guidance is needed to distinguish material influence from consultation or expert input.

Clinical research often sits on a spectrum between simple adherence and true joint design. Without further clarification, there is uncertainty as to when participation in protocol development creates joint controllership.

MDT Suggestion:

The EDPB should provide additional examples (such as those above) clarifying how to assess different levels of involvement in the preparation of a research protocol.

Paragraph 143 — Different Legal Bases for Joint Controllers

MDT Opinion:

> **Para. 143:** *"the GDPR does not preclude that different joint controllers rely on different legal bases, depending on their applicability to a given processing operation."*

This important clarification merits an example: in a public-private partnership, a public controller may use a public-health legal basis while the private controller cannot and must instead rely on legitimate interest or consent.

MDT Suggestion:

Add a worked example for joint controllers with divergent legal bases in a public-private research partnership, showing how each independently establishes lawfulness, how the joint-controller agreement reflects this, and how data subjects are informed of the differing bases.

Example 25 — Large Research Consortia

MDT Opinion:

> **Example 25 (after para. 145):** *"A research consortium pursues a joint research project on the quality and efficacy of an oncological treatment scheme ... The research consortium involves a commercial pharmaceutical company, several university hospitals and a private research institute."*

The example can be explained better. Although it is one consortium project, it comprises a number of processing activities and responsibilities may vary across them; large consortium projects need a nuanced analysis, since different members may play different roles in different parts of the project. A project of 30 equal joint controllers is essentially uncontrolled, as clarity of responsibility becomes almost impossible; splitting it into sub-projects resolves this.

> **(Continuation of example):** *"The research activities also include several sub-projects to be undertaken following the conclusion of the observational study. The research protocol, which was drafted and approved jointly by all consortium partners, sets out the common purposes and methodology for the study, which research data (including personal data) that is to be collected and processed, criteria for inclusion/exclusion of research participants, permitted further use of the data for future research, etc".*

For instance, this example appears to assume that all parties within a research consortium participate in the drafting of the protocol. In practice, however, this is often not the case. Research consortia typically define work packages in the Grant Agreement, with responsibility for protocol development usually assigned to only one or a limited number of consortium partners. It would therefore be helpful to include an alternative example that better reflects consortium structures in which specific tasks are allocated through work packages, while not all partners are involved in determining the purposes and essential means of the processing. Such an example could provide greater clarity on the allocation of data protection roles where consortium agreements designate all partners as data owners, but only certain partners are responsible for activities that influence the purposes and means of the processing.

> **(Continuation of example):** *"Furthermore, because the processing of personal data in the database is decided on and operated jointly by all partners of the research consortium, and since all data retained in that database are inseparable for the purposes of conducting further research, all partners to the research consortium are joint controllers for the processing of personal in the federated database that is necessary to make personal data available to the consortium partners for future research activities".*

Similarly, this paragraph appears to assume that access to, and the sharing of, research data are inherently linked to the conduct of further research within the consortium. In practice, however, this is often not the case. Consortium partners are typically involved because of the specific expertise, resources, or data they can contribute, for example through previous studies they have conducted. Their primary interest may not necessarily be participation in all subsequent research activities carried out under the consortium, but rather obtaining access to the research results and, where permitted, the underlying data generated through the collaboration. This enables them to pursue their own independent research activities outside the scope of

the consortium. An example reflecting this common arrangement would provide a more realistic basis for assessing the allocation of data protection roles and responsibilities.

MDT Suggestion:

The Guidelines should acknowledge that large consortia may benefit from being structured as a series of discrete processing activities, each with a clear controller allocation, rather than a single monolithic joint-controller arrangement. The practice of appointing a lead controller for specific activities (data intake, database operation, sub-project access) should be endorsed, and Example 25 extended to illustrate this.

Further, alternative examples should cover those situations where the protocol development is attributed partially to some of the consortia partners; helping to interpret the allocation of roles for these complex infrastructures. A good solution could be to endorse the approach suggested in "Joint controllers in large research consortia: a funnel model to distinguish controllers in the sense of the GDPR from other partners in the consortium" by Veen, E.-B., Boeckhout, M., Schlünder, I., Boiten, J.W. & Dias, V. (2024) Open Research Europe: https://open-research-europe.ec.europa.eu/articles/2-80

Section 8 — Appropriate Safeguards

8.1 — General

Paragraph 149 — DPO as Safeguard

MDT Opinion:

> **Para. 149:** *"appointing a data protection officer (DPO) when required."*

Adding "when required" can be misleading, as mandatory appointment is already a GDPR obligation based on the interpretation of article 37(7) letters (b) and (c). The added value of this section would lie on suggesting a voluntary DPO appointment even where not legally required, which should be emphasised as a safeguard for the processing activities and an integral part of the data protection governance underpinning the organisation's accountability. (Paragraph 149 is also a good place to clarify the requirements for DPO appointment, for instance, stating as a reminder of the Annex 5.3 of the Guidelines on Data Protection Officers ('DPOs'), that data volume is defined not only by the number of data subjects, but also by the volume of data per person, variety and velocity.)

MDT Suggestion:

Remove "when required" and instead present voluntary DPO appointment as a recommended Article 89(1) safeguard, in particular where special categories of personal data are processed for research. Use paragraph 149 to clarify the multi-dimensional nature of "volume" (per-person volume, variety, velocity).

8.2 — Risk Analysis and DPIA

Paragraphs 151 and 160 — Internal Consistency on the DPIA as Starting Point

MDT Opinion:

> **Para. 151:** *"The starting point for adopting appropriate safeguards, pursuant to Article 89(1) GDPR, is conducting a risk analysis or – when required – a DPIA."*
>
> **Para. 160:** *"The assessment should be undertaken as part of a risk analysis or, where relevant, a DPIA."*

Paragraph 151's clarification that the starting point is a risk analysis/DPIA is very good (and the new reference to incidental findings is welcome). However, there reference "where relevant" in both paragraph 151 and 160 suggests the DPIA may be optional. In MDT's view, the DPIA should be encouraged as a safeguard, in line with the approach suggested in the previous point related to DPO appointment of this document response to the public consultation.

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

The clarification in paragraph 151 that a risk assessment/Data Protection Impact Assessment (DPIA) should serve as the starting point is particularly welcome, as is the new reference to incidental findings. However, the qualification "where relevant" in both paragraphs 151 and 160 appears to suggest that conducting a DPIA may be optional in certain circumstances. In MDT's view, the use of a DPIA should be more strongly encouraged as an important safeguard when processing personal data in the research context. This would be consistent with the approach advocated regarding the recommendation to appoint a Data Protection Officer (DPO), and would further support accountability and the protection of data subjects' rights.

MDT Suggestion:

Revise the wording in paragraphs 151 and 160 to avoid implying that a Data Protection Impact Assessment (DPIA) is merely optional. Instead, the guidance should present the conduct of a DPIA as a preferred safeguard and a recommended starting point for assessing and mitigating risks associated with research processing activities, even where a DPIA may not be strictly required under Article 35 GDPR. This would reinforce accountability, support a risk-based approach, and promote a consistent standard of data protection in research contexts.

Paragraph 153 — Effect on Related Persons (Genetic Data)

MDT Opinion:

> **Para. 153:** *"The controller should also consider if the processing of personal data may affect persons related to the data subject, such as family members or friends."*

This is particularly important in genetic research, where the data inherently concerns biological relatives.

MDT Suggestion:

Paragraph 153 should expressly highlight the genetic-data context, where processing affects family members by the nature of the data, and link this to the safeguards in section 8.4.

8.3 — Anonymisation and Pseudonymisation

Paragraph 156 — Anonymisation and Pseudonymisation over the Study Lifecycle

MDT Opinion:

> **Para. 156:** *"personal data processed for scientific research should, in the first place, be anonymised where the purposes of the processing can be fulfilled using anonymised data."*

MDT supports this principle, but further clarification would be useful on how it applies across the lifecycle of a clinical study. Anonymisation may not be appropriate or possible at the outset, because the research purpose may require individual-level follow-up, traceability or linkage over time, and because anonymisation procedures may in some cases reduce the utility of the data. In these situations, pseudonymisation may be the most appropriate safeguard during the active research phase, while anonymisation may become appropriate at a later stage, for example for publication, sharing of aggregated results, or where individual-level traceability is no longer required.

MDT Suggestion:

The Guidelines should clarify that anonymisation should be preferred where it is compatible with the research purpose, but that pseudonymisation will often remain necessary and proportionate in clinical research where individual-level traceability, safety follow-up, reproducibility or regulatory requirements must be preserved.

Paragraphs 159 and 164 — Contradiction with Paragraph 77 on Contact Details

MDT Opinion:

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

> **Para. 159:** *"the controller should always opt for using anonymised data or pseudonymised personal data if the purpose of the scientific research does not require the use of personal data that can be used to directly identify data subjects."*

Paragraph 159 (and the related transparency duty in paragraph 164) directly contradicts the earlier suggestion in paragraph 77 to collect contact details for the exercise of rights. In pseudonymised research, collecting direct contact data conflicts with data minimisation and pseudonymisation.

MDT Suggestion:

Resolve the contradiction explicitly: the contact-detail recommendation in paragraph 77 must yield to pseudonymisation requirements where they apply. In clinical trials, where Sponsors don't hold the key for reidentification, and similar pseudonymised research, transparency should be achieved through the treating institution or pull-based patient portals, not direct contact by the controller holding pseudonymised data.

Paragraph 160 — Timing of the Format Assessment

MDT Opinion:

> **Para. 160:** *"Consideration of which format of data is necessary and justifiable to process for scientific research purposes should take place when a controller draws up a plan for the processing of personal data ..."*

As noted above, paragraph 160's "where relevant, a DPIA" wording contradicts paragraph 151, which treats the DPIA as the starting point for safeguards.

MDT Suggestion:

Harmonise paragraph 160 with paragraph 151 so that the format assessment is consistently positioned within the baseline risk analysis, escalating to a full DPIA where high risk is likely.

Paragraph 161 — Effectiveness of Pseudonymisation

MDT Opinion:

> **Para. 161:** *"controllers must use state-of-the-art anonymisation or pseudonymisation methods, taking into account the most current assessment of effectiveness, risks of re-identification, threats to security, etc."*

Given the volume of data involved, the transferability/reproducibility-type criterion is difficult to meet in absolute terms, but pseudonymisation is not black or white. Where effectiveness cannot be fully achieved, additional security measures should mitigate the residual risk; pseudonymisation should be assessed together with other safeguards.

MDT Suggestion:

Paragraph 161 should acknowledge that pseudonymisation is a risk-mitigation measure on a spectrum, not an absolute protection. Where "state-of-the-art" pseudonymisation cannot fully eliminate re-identification risk given data volume and variety, the Guidelines should endorse a compensating-safeguards approach (access controls, secure processing environments, contractual prohibitions on re-identification).

Paragraph 162 — Effect of True Anonymisation for the Recipient

MDT Opinion:

Where data are transmitted under true anonymisation for the recipient, paragraphs 163 and 94 should not apply to that recipient, as there is no longer a data subject capable of being re-identified by it. MDT considers that the Guidelines would benefit from clarifying the recipient's obligations in cases of genuine anonymisation (where genuine anonymisation can in fact be achieved).

MDT Suggestion:

The EDPB should clarify that, where personal data are genuinely anonymised in the hands of the recipient, the obligations in paragraphs 94 and 163 concerning the exercise of rights through pseudonyms and re-identification do not apply to that recipient, and should specify what residual obligations, if any, remain.

Separately, paragraph 161 refers to an ongoing process of verification that the measures remain effective. Additional operational guidance would be useful on the expected level and frequency of such verification in long-term clinical research, where data may be retained for 15, 25 or more years. It is unclear whether "ongoing verification" requires continuous review, periodic reassessment, reassessment upon specific trigger events, or a risk-based combination. MDT suggests clarifying that verification of anonymisation and pseudonymisation measures may be conducted using a risk-based approach, enabling proportionate implementation while maintaining effective safeguards against re-identification.

Paragraph 163 — Identity Verification for Pseudonymised Data Subjects

MDT Opinion:

> **Para. 163:** *"contractual obligations should ensure that – following a request from a data subject that exercises his or her rights – the controller that pseudonymised the personal data can provide the information that is necessary to re-identify a data subject ..."*

Re-identifying a data subject to service a right may itself increase re-identification risk and may conflict with national DPA guidance (e.g. CNIL guidance discouraging the use of identity documents combined with medical data). It is unclear how a non-hospital controller can be certain of a requester's identity; if a request requires combining a direct identifier with medical data, would CNIL authorisation be needed? Offering the data subject a choice — a form of consent to the residual risk that providing more information may place data at risk — could be considered.

MDT Suggestion:

The Guidelines should provide concrete, privacy-preserving guidance on identity verification in pseudonymised research, including use of the participant's own pseudonym (where safely communicated at enrolment), verification through the treating institution, secure e-identity mechanisms, or a trusted data intermediary. Divergence from national DPA guidance (e.g. CNIL) should be flagged, and the EDPB should consider issuing supplementary guidance on identity verification in pseudonymised medical research by non-hospital controllers.

Paragraph 164 — Information on Limitations of Identification

MDT Opinion:

> **Para. 164:** *"data subjects should not be given the impression that their personal data will be anonymised if the data in fact will be processed in a pseudonymised form and the data subjects will still be identifiable, albeit indirectly."*

MDT welcomes the precision that information must include the limitation arising from advanced de-identification (and its impact on the exercise of rights).

MDT Suggestion:

No change recommended. MDT supports paragraph 164 and encourages its retention.

8.5 — Other Appropriate Safeguards

Paragraph 169 — Information Campaigns and Group-Level Risks in Genetic Research

MDT Opinion:

> **Para. 169:** *"information campaigns" for genetic research involving isolated population groups.*

MDT welcomes paragraph 169 and understands its objective as addressing risks beyond the individual participant: in genetic research, findings may affect relatives, families, communities or groups sharing

MyData-TRUST
18b av. Lavoisier
1300 Wavre
Belgium

genetic characteristics, creating risks of discrimination, stigmatisation, reputational harm or unexpected group-level findings. This connects to the genetic-data context highlighted at paragraph 153. However, paragraph 169 refers specifically to isolated population groups, and it may not always be clear whether similar measures should be considered in other genetic research contexts where group-level risks arise. For example, a genomic study of a small island population may clearly justify a community-level campaign; a rare-disease study of 100 patients across several countries is less clear; and a biobank studying inherited cancer mutations may also raise questions where findings affect relatives or identifiable families.

MDT Suggestion:

The EDPB should provide additional guidance on: when an information campaign should be considered; who should be responsible for conducting it; what information it should contain; how the affected group or community should be identified; whether a minimum size or level of identifiability is relevant; and whether the recommendation applies only to isolated population groups or also to rare-disease communities, genetically identifiable families, disease-specific registries or biobanks involving inherited conditions.

Paragraph 170 — Catalogue of Safeguards

MDT Opinion:

> **Para. 170:** *"when processing personal data for scientific research purposes, it may be necessary to adopt other types of safeguards beyond anonymisation or pseudonymisation."*

The detailed, non-exhaustive catalogue of safeguards in paragraph 170 is very welcome and provides practical, operable guidance.

MDT Suggestion:

No change recommended. MDT supports paragraph 170 and encourages its retention.

MDT remains available to provide further input or participate in stakeholder dialogue as the EDPB finalises these Guidelines.