HINSHAW

Compliance Considerations for GDPR Consent in Biotech Clinical Research

How One EU Framework Can Lead to Divergent Data Strategies

Privacy, Cyber & AI Decoded Alert | 10+ min read

Mar 11, 2026

By: Jason J. Oliveri, Lily S. Elkwood, Caroline Poche*

Biotech and digital health teams working in Europe sometimes find that the hardest General Data Protection Regulation (GDPR)[1] question in clinical research is not whether the law applies (it does), but how the different views of countries on lawful bases and consent will complicate their carefully planned data strategy.[2]

Contemporary health research programs increasingly depend on re-analysis of trial data, secondary studies, and reuse of health and genetic data across projects and partners.[3] At the same time, many national regulatory regimes and review bodies still apply purpose limitation and consent concepts in ways that can be relatively narrow, which can create friction when sponsors aim to build multi-use, cross-border data assets.[4]

On its face, the GDPR gives research programs some room to operate. Consent is one lawful basis for processing personal data, but it is not the only one, and health data can also be processed for scientific research when specific legal conditions and safeguards are met.[5] In parallel, the European Union (EU) Clinical Trials Regulation (CTR) imposes informed consent requirements for participation in clinical trials, framed as ethical and participant-protection standards, not data-protection rules.[6]

In practice, this leaves every EU trial answering two distinct questions:

1. Can we ethically enroll this person in this study under the CTR and national research ethics rules, and
2. On what GDPR legal basis can we process their personal and health data?[7]

The GDPR does not require that these answers be identical - in fact, the European Data Protection Board (EDPB) has expressly warned against confusing informed consent under the CTR with consent as a GDPR legal basis.[8]

Member States have nevertheless implemented and interpreted the GDPR's research provisions – particularly Article 9(2)(j) and Article 89 – in different ways, and have added their own sector-specific rules and soft law.[9] For sponsors trying to build reusable, multi-country data resources, this divergence in lawful basis choices and

safeguards is not just a theoretical nuance; it materially complicates how they architect pipelines, contracts, and governance.[10]

Two Families of Approaches: Consent-Heavy vs. Research-Basis-Heavy

Observers of European health data governance often describe two broad patterns: one in which explicit consent remains the predominant lawful basis for processing special category data in research, and another in which controllers more often rely on public-interest or scientific research grounds together with statutory safeguards and governance mechanisms.[11]

The GDPR, for better or worse, supports both of these patterns: Article 6 provides a menu of lawful bases, and Articles 9(2)(j) and 89 offer a research pathway with safeguards that can operate without consent for every individual reuse.[12]

Consent-Heavy Member States

In a first set of Member States, consent still dominates in clinical study data processing, even though national law may allow research-based processing in some situations.[13] In Germany, for example, recent empirical work on clinical study data sharing concludes that "consent for study data is widely accepted, recommended, and in most cases mandatory," and that consent is currently seen as the only regularly feasible path to clinical study data sharing.[14]

Other countries, including some in central and eastern Europe, are reported as taking similarly cautious approaches, leaning heavily on consent and anonymization even where research exemptions exist.[15]

In such settings, sponsors and investigators are generally expected to obtain valid CTR consent to participate; where consent is chosen as the GDPR basis, to satisfy the usual GDPR standards (freely given, specific, informed, unambiguous); and to describe research purposes in a way that aligns with planned uses, without pretending they can predict every future analysis.[16] Recital 33 recognizes that scientific research cannot always be specified down to the last hypothesis at the outset, but still expects consent for "certain areas" of research, not a blanket authorization for unspecified future work.[17]

When purposes evolve – for example, to include new analyses, cross-study pooling, or model development – controllers in these environments must assess whether those uses remain compatible with the original purposes and consent, or whether further legal analysis, ethics review, or additional consent is required.[18] Academic literature on bio banks and data-intensive research notes that frequent re-consent or ethics committee review for each new use can be burdensome and may hinder reuse at scale, which is one reason many authors argue for robust safeguards and governance as alternatives.[19]

Research-Basis-Heavy Member States

In a second set of Member States, laws and regulatory frameworks place greater emphasis on research and public interest bases, combined with detailed safeguards, and treat consent as one part of the ethical picture rather than the cornerstone of every GDPR analysis.[20]

France is a prominent example: Commission nationale de l'informatique et des libertés (CNIL's) méthodologies de référence – MR-001 for many interventional studies and MR-003 for certain non-interventional studies – set out standardized conditions for health-data research, including minimization, pseudonymization, retention limits, and security.[21]

If a project fits one of these frameworks and complies, the formalities are simplified; otherwise, a specific authorization process applies.[22] French Comités de Protection des Personnes (CPPs) review ethical and data-protection aspects together, including alignment with these CNIL frameworks.[23]

Historically, the UK Information Commissioner's Office has also warned that consent is often not the most appropriate or reliable legal basis for health research, and has pointed controllers instead toward public task and research conditions for special category data.[24]

Belgium has implemented the GDPR's public-interest and research provisions in its national law and requires appropriate safeguards when health data is processed on these bases.[25] In these research-basis-heavy models, consent remains crucial for ethics and transparency, but regulators and scholars focus more on whether the overall research framework is justified, proportionate, and well-governed than on whether every new use can be matched word for word to a consent clause drafted years earlier.[26]

Country Snapshots: Where the Law Meets the Site Initiation Visit

Germany

In Germany, empirical work on clinical study data sharing portrays a system where consent is presently treated as the default – and often the only practical – basis for sharing clinical study data with third parties, notwithstanding the existence of research provisions in national law.[27]

The same work notes considerable uncertainty around alternative lawful bases and points out that upcoming instruments - including a research data act and the European Health Data Space (EHDS) - may shift this balance.[28] Other German scholarship examines consent-free research under strict safeguards, but treats it as an evolving, contested space rather than a settled norm.[29]

Italy

In Italy, Article 110 of its national Privacy Code (as amended) and subsequent guidance from the Garante allow for health data research without consent in some cases, particularly retrospective research where obtaining consent

is impracticable, grounded in Article 9(2)(j) GDPR and conditioned on safeguards and impact assessments.[30] At the same time, Italian practice has long relied on explicit consent for many forms of biomedical research, with the Garante providing additional guarantees where consent cannot be obtained.[31]

Hungary

In Hungary, the Act XLVII of 1997 on the processing and protection of health and related personal data regulates access to health data for research and generally expects either anonymization or strict conditions for identifiable data use.[32] A recent overview outlines strict rules for the reuse of healthcare data, emphasizing security, privacy, and compliance with GDPR standards.[33]

Spain

Spain offers a more mixed picture. The Spanish Organic Law 3/2018 includes provisions on the processing of health data for research and allows certain uses in the public interest or for scientific purposes without consent under defined conditions.[34]

Work commissioned by the EDPB reflects examples from the AEPD in which patients who consent to one cancer research project can have their data used in other cancer projects within a defined framework, illustrating both the use of broad consent and the importance of context and safeguards.[35]

Across these examples, comparative studies, and the EDPB's own research on secondary use show that some Member States are more comfortable with explicit consent or anonymization, while others are cautiously operationalizing research-based processing without consent under Article 9(2)(j) and Article 89(1), often with ethics committee or oversight committee review.[36] The "two families" framing is therefore a simplification, but a useful one, provided we remember that the details vary significantly by jurisdiction.

Children, Imaging, and Data Minimization

Pediatric research and imaging turn these abstract models into concrete design choices. Under the GDPR, children merit specific protection, and controllers must implement appropriate measures to protect them, including in digital and research contexts.[37] The regulation also makes it clear that images and videos showing identifiable individuals, especially where they reveal health information or biometric traits, are special category data requiring heightened protection.[38]

European data protection law leans heavily on data minimization and proportionality: personal data should be adequate, relevant, and limited to what is necessary for the purposes, and controllers should implement technical and organizational measures to mitigate risk.[39] CNIL's recommendations on protecting children online exemplify this approach: they stress minimization, careful justification before collecting sensitive data, and robust safeguards.[40]

In a pediatric motor assessment trial where children are video recorded, these principles imply that, even when parents or guardians have consented to recording and research use, sponsors should still assess whether full face video is necessary for the endpoints or tools at issue, or whether pseudonymization, partial masking, restricted access, or shorter retention could achieve the same scientific purpose with less risk.[41] Parental consent is important, but GDPR does not treat it as exhaustive: controllers remain responsible for necessity, proportionality, and risk reduction.[42]

Academic and policy discussions on health data research consistently emphasize that, particularly where consent is limited or absent, appropriate safeguards – governance structures, oversight committees, minimization, and access controls – are central to legitimizing data-intensive research.[43] That logic is increasingly evident in European discussions about children, imaging, and digital health tools, even if national documents do not always explicitly spell out pediatric video scenarios.

Multi-Country Reality and Program-Level Design

When sponsors run trials or data platforms across several EU countries, differences in lawful bases, safeguards, and expectations converge into a single operational challenge. Comparative analyses and stakeholder reports highlight how divergent implementations of GDPR research provisions and national health data rules complicate secondary use and cross-border data-intensive research.[44]

In response, many organizations appear to adopt cautious "highest common denominator" strategies: designing governance and technical controls to satisfy the strictest applicable requirements, so they are not forced to manage multiple subtly different regimes for similar processing.[45] This approach is not mandated by the GDPR, but it is a recognizable pattern in practice.

Regulators and oversight bodies may also vary in their stance on higher-risk processing, such as imaging, AI training, or large-scale pooling, especially where children or vulnerable groups are involved.[46] Controllers then face a design choice: maintain distinct data pipelines and governance regimes by jurisdiction, or harmonize to a more restrictive standard to simplify operations. The GDPR's accountability, privacy by design, and data protection impact assessments (DPIA) duties do not dictate which option to choose; they simply ensure that controllers remain responsible for their choices.[47]

For biotech companies, this makes program-level design – legal, ethical, and technical – central rather than peripheral. GDPR requires appropriate technical and organizational measures and expects controllers to integrate data protection considerations into processing from the outset, including through DPIAs.[48] Academic work on secondary use, bio banks, and the EHDS proposal reinforces that lawful bases, reuse pathways, and safeguards are architectural choices, not details to be patched in after the protocol is finalized.[49]

Practical Considerations for Biotech Teams

For clinical operations, site and country strategy matter. Because Member States differ in how heavily they rely on explicit consent or on research/public-interest bases for health data processing, and in how they treat secondary use, it can be prudent to factor these differences into site selection, timelines, and resource planning.[50]

Transparency obligations under GDPR also mean that consent and information materials should, as far as reasonably possible, explain foreseeable secondary uses, data sharing, and potential model development to align participant expectations with likely future research uses.[51]

For data science and AI teams, GDPR's principles of purpose limitation, minimization, and privacy by design support building data pipelines that can accommodate different permissions, constraints, and levels of identifiability for different cohorts or jurisdictions, including the possibility that some data may be used only for more limited purposes or must be pseudonymized or anonymized more aggressively.[52] EDPB and academic work on secondary use indicate that, in practice, controllers often end up with core datasets usable for a range of purposes and more constrained subsets where lawful bases, consent scopes, or safeguards differ, which must be factored into model design, validation, and documentation.[53]

For in-house counsel and compliance teams, GDPR's accountability, contract, and DPIA requirements point to the need for a coherent legal and technical architecture rather than improvising on a form-by-form basis.

Organizations need to determine, for each program, whether to rely primarily on consent, on research/public-interest bases with safeguards, or on a combination, and then reflect that architecture consistently in DPIAs, contracts, policies, and governance structures.[54] EDPB and Commission guidance on the CTR-GDPR interplay confirm that CTR informed consent and GDPR lawful bases must be kept analytically distinct, even if participants see a single information sheet, and that this distinction should be clear in internal analyses and documentation.[55]

A Simple Playbook for a Not-So-Simple Regulatory Landscape

For teams planning EU-facing trials or data platforms, a straightforward playbook – grounded in the law and soft law sources discussed above – can help:

- **Decide your tolerance for variation.** Given the documented heterogeneity in Member State research rules and practices, choose whether you will run different lawful bases and consent scopes by country, or design around a single, relatively strict standard that works across your key jurisdictions.[56]
- **Segment and document from day one.** Accountability and record-keeping duties make it sensible to tag data by site, country, lawful basis, consent scope (where relevant), and intended uses, so you can later see which datasets can be used for which projects without reconstructing every prior decision.[57]
- **Standardize building blocks, not every outcome.** Develop model consent and information language and standard contractual clauses with sites and partners that acknowledge both primary trial uses and reasonably foreseeable secondary uses, within the limits of each jurisdiction and Recital 33's cautiously flexible approach to research consent.[58]

- **Invest in governance when you rely on Article 9(2)(j).** Where you rely on research or public interest grounds rather than consent, Article 89(1) and the Article 89 literature stress that appropriate safeguards–including minimization, pseudonymization, risk assessments, oversight committees, and robust documentation–are essential.[59]
- **Watch the EHDS and national developments.** The EHDS proposal and associated commentary make clear that secondary use of health data is a major policy focus, and that Member States will continue to refine how research/public interest bases are applied.[60] Building flexibility into your governance and technical design now can make adaptation easier as these frameworks evolve.[60]

Biotech innovation now depends as much on what you can do with data as what you can do with molecules. In Europe, the question is not just whether an activity is "GDPR-compliant" in the abstract, but whether the chosen combination of consent strategy, lawful bases, and safeguards can sustain the ways you actually need to use your data over time and across borders. Getting that architecture right will not make the regulatory landscape simple, but it can make it more navigable and more workable for those willing to engage with its details.

**Caroline Poche is a law clerk and is not admitted to practice law.*

---

[1] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://data.europa.eu/eli/reg/2016/679/oj.

[2] European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (adopted Jan. 23, 2019). https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

[3] Regina Becker & Edward S. Dove, The EU GDPR and Secondary Use of Health and Genetic Data for Research Support Purposes, Int'l Data Priv. L(published Jan. 27, 2026),https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipag001/8443007.

[4] Julie-Anne R. Smit *et al.*, Specific Measures for Data-Intensive Health Research Without Consent: A Systematic Review of Soft Law Instruments and Academic Literature, 32 Eur. J. Hum. Genetics 21, 22-25 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10772063/

[5] GDPR arts. 6(1), 9(2)(j), 89(1); GDPR recital 33.

[6] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on Clinical Trials on Medicinal Products for Human Use, 2014 O.J. (L 158) 1, arts. 28-29. https://eurlex.europa.eu/eli/reg/2014/536/oj.

[7] *See* EDPB, Opinion 3/2019, supra note 2.

[8] *Id*.

[9] Global All. for Genomics & HealthGDPR Brief: How Is Article 89 Implemented Across the EU/EEA? (June 3, 2019). https://www.ga4gh.org/news_item/how-is-article-89-implemented-across-the-eu-eea/

[10] Ciara Staunton *et al*., Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research, 13 Frontiers in Genetics 719317 (2022). https://pmc.ncbi.nlm.nih.gov/articles/PMC8896881/.

[11] Global All. for Genomics & Health (GA4GH), *supra* note 9; Smit *et al.*, *supra* note 4.

[12] GDPR arts. 6, 9, 89.

[13] European Data Protection Board, Study on the Secondary Use of Personal Data in the Context of Scientific Research (Mar. 31, 2025). https://www.edpb.europa.eu/our-work-tools/our-documents/other/study-secondary-use-personal-data-context-scientific-research_en.

[14] Evgeny Bobrov *et al.*, Six Solutions for Clinical Study Data Sharing in Germany, 23 BMC Med. Ethics 1 (2025) https://pmc.ncbi.nlm.nih.gov/articles/PMC12103796/.

[15] *See* Dalibor et al., *supra* note 14. https://pmc.ncbi.nlm.nih.gov/articles/PMC12103796/. *See also* Smit *et al.*, *supra* note 11. https://pmc.ncbi.nlm.nih.gov/articles/PMC10772063/.

[16] GDPR art. 5(1)(b), arts. 6(1)(a), 7; recital 33.

[17] GDPR recital 33; Global All. for Genomics & Health, *Policy Brief: When Can I Rely on Broad Consent for Research?* (Apr. 1, 2019), https://www.ga4gh.org/news_item/when-can-i-rely-on-broad-consent-for-research/.https://data.europa.eu/eli/reg/2016/679/oj.

[18] GDPR arts. 5(1)(b), 6(4), recital 50.

[19] Smit *et al.*, *supra* note 11. https://pmc.ncbi.nlm.nih.gov/articles/PMC10772063; Staunton *et al., supra* note 10.

[20] Commission Nationale de l'Informatique et des Libertés (CNIL), MR-001, https://www.cnil.fr/sites/cnil/files/atoms/files/mr-001.pdf.

[21] Commission Nationale de l'Informatique et des Libertés (CNIL), Méthodologie de référence MR-003, https://www.cnil.fr/sites/cnil/files/atoms/files/mr-003.pdf.

[22] CNIL, MR-001, *supra* note 20; (CNIL, MR-003, *supra* note 21.

[23] Code de la santé publique, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072665.

[24] Info. Comm'r's Off., What Are the Rules on Special Category Data? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-rules-on-special-category-data/.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-rules-on-special-category-data/.

[25] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Belg.,), https://etaamb.openjustice.be/fr/loi-du-30-07-2018_n2018040581.html.

[26] Smit *et al.*, *supra* note 4; Staunton *et al.*, *supra* note 10.

[27] Evgeny Bobrov *et al.*, Six Solutions for Clinical Study Data Sharing in Germany, 25 BMC Med. Res. Methodol.:140 (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12103796/.

[28] *Id*.

[29] Gesine Richter *et al.*, How to Elucidate Consent-Free Research Use of Medical Data, 2 26: J. Med. Internet Rsch. 351350 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11196244/.

[30] Garante per la Protezione dei Dati Personali, Sanità e Ricerca scientifica, https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica.

[31] *Id*.

[32] Évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, https://njt.hu/jogszabaly/1997-47-00-00.

[33] International Bar Association, The Intersection of Big Data and healthcare: Legal developments in Hungary (Apr. 28, 2024), https://www.ibanet.org/big-data-healthcare-hungary.

[34] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (Spain) https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673.

[35] European Data Protection Board, Study on the Secondary Use of Personal Data in the Context of Scientific Research (Mar. 31, 2025),https://www.edpb.europa.eu/our-work-tools/our-documents/other/study-secondary-use-personal-data-context-scientific-research_en).

[36] European Data Protection Board, Study on the Secondary Use of Personal Data in the Context of Scientific Research (Mar. 31, 2025), https://www.edpb.europa.eu/our-work-tools/our-documents/other/study-secondary-use-personal-data-context-scientific-research_en); Smit *et al*., *supra* note 10.

[37] GDPR recital 38.

[38] GDPR arts. 4(1), 4(14), 4(15), 9(1).

[39] GDPR arts. 5(1)(c), 24, 25, recital 39.

[40] Commission Nationale de l'Informatique et des Libertés (CNIL) (Aug 9, 2021). https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online.

[41] See Id.; GDPR art. 32.

[42] GDPR arts. 5, 24, 25.

[43] Smit *et al.*, *supra* note 4; Staunton *et al.*, *supra* note 10.

[44] Global All for Genomics & Health, *supra* note 9; EDPB, Study on the Secondary Use of Personal Data, *supra* note 13.

[45] DIGITALEUROPE, Making the Most of the GDPR to Advance Health Research (June 11, 2021), https://cdn.digitaleurope.org/uploads/2021/06/Making-the-most-of-the-GDPR-to-advance-health-research_DIGITALEUROPE.pdf; Becker & Dove, *supra* note 3.

[46] EDPB, Study on the Secondary Use of Personal Data, *supra* note 9.

[47] GDPR arts. 24, 25, 35.

[48] *Id*.

[49] Won Bok Lee *et al*., Secondary Use Provisions in the European Health Data Space Proposal, Eur. J. Pub. Health (2023), https://pmc.ncbi.nlm.nih.gov/articles/PMC10440198/.

[50] EDPB, Study on the Secondary Use of Personal Data, *supra* note 13.

[51] GDPR arts. 12-14.

[52] GDPR arts. 5(1)(b)-(c), 25, 32.

[53] EDPB, *Study on the Secondary Use of Personal Data*, *supra* note 13; Smit et al., *supra* note 4, at 22–25.

[54] GDPR arts. 24–28, 35.

[55] EDPB, *Opinion 3/2019*, *supra* note 2.

[56] Global All. for Genomics & Health, *supra* note 9; DIGITALEUROPE, *supra* note 45.

[57] GDPR art. 30.

[58] GDPR art. 89(1); European Data Protection Board, Study on the Appropriate Safeguards under Article 89(1) GDPR for the processing of personal data for scientific research (Jan. 13, 2022), https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf.

[59] GDPR art. 89(1); European Data Protection Board, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research (Jan. 13, 2022) https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf.

[60] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final (May 3, 2022), https://health.ec.europa.eu/system/files/2022-05/com_2022-197_en.pdf; Lee *et al.*, *supra* note 49.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Lily S. Elkwood

Associate

212-655-3898

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity

Healthcare