About this journal

German Law Journal

ISSN: 2071-8322 (Online)
Frequency: 9 issues per year

The *German Law Journal* is a pioneering open-access forum for the publication of scholarship and commentary on comparative, European, and international law. It has been online and freely-available since 1999. Founded as a transatlantic newsletter on developments in German law, the Journal has secured a place among the world's leading law reviews disseminating scholarship across borders. The Journal combines high-quality theoretical research with reports on current developments and thematic special issues. Pursuing this agenda, the Journal has gained a reputation for innovative publishing - linking cutting-edge, border-crossing scholarship with open access and speed to publication.

Content preservation

Cambridge University Press publications are deposited in the following digital archives to guarantee long-term digital preservation:

- CLOCKSS (journals)
- Portico (journals and books)

This journal is published by Cambridge University Press on behalf of its managers and owners, German Law Journal e. V.

German Law Journal (2022), **23**, pp. 559–596
doi:10.1017/glj.2022.30

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think

Giovanni Comandè[1] and Giulia Schneider[2]

[1]Full Professor of Private Comparative Law at the Lider Lab of Sant'Anna School of Advanced Studies, Pisa, Italy and [2]Researcher in Economic Law at Catholic University, Milan, Italy
Corresponding author: giulia.schneider@unicatt.it

(Received 19 April 2021; accepted 23 July 2021)

Abstract
Against the backdrop of an evolving landscape describing data driven research, this article discusses the role of data protection laws in shaping a free flow of research data. In particular, the analysis inquires whether European data protection law hampers or encourages data-driven research. The analysis critically challenges the shared belief that the more severe data protection regime laid down by the European legislator adversely affects data flows and with that data-driven research. This is contrary to what occurs in the United States, where the more fragmented and less developed data protection framework facilitates data flows and related innovation patterns. We show how research objectives through data re-usability have been very recently given primary importance in the GDPR, where they find a formidable ally enabling the re-usability of public data by businesses and of private data by public institutions, for either public interest-related research purposes or commercially oriented innovation purposes. We argue that the GDPR differently promotes research-valuable data flows in consistency with an emerging principle of free movement of personal data. In order to ground this statement, our analysis links to this principle three-directional research regimes emerging from the GDPR.

Keywords: GDPR; Data Privacy; European Data Protection Law; Data Sharing; Consent of Data Sharing

A. Introduction and Scope of the Analysis

Data sharing practices imply access to data among contracting parties and the processing of it by involved subjects.[1] Even when data are shared merely for research purposes a legal framework is

Although the study has been conceived jointly, paras. A–E are to be attributed to Giulia Schneider and paras. F–H to Giovanni Comandè.

[1]*See* 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, and repealing Directive 95/46/EC, 2016 O.J. (L 119) art. 4(2) [hereinafter Council Regulation 2016/679] (clarifying that processing means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, *disclosure by transmission, dissemination or otherwise making available*, alignment or combination, restriction, erasure or destruction.") (emphasis added). *See also* Arye Schreiber, *Mere Access to Personal Data: Is It Processing?*, 10 INT'L DATA PRIV. L. 269 (2020) (assessing the relevance of access to data for the purposes of the General Data Protection Regulation).

needed[2] and implied in all the terms of service and licenses agreements. Access is generally meant to maximize the scientific and technological value of aggregated datasets, as processed for research and development purposes.[3] Several sets of legal rules have been issued with the specific aim of incentivizing data exchanges among different stakeholders for research and innovation purposes.

In the United States,[4] for example, the policy stance of enhancing the free flow of information has triggered recent reforms, especially in the health sector, that we choose as a test bed for our analysis. With the aim of promoting the flow of patients' personal health information, the 21st Century Cures Act[5] has established a framework to advance "interoperability and support the access, exchange and use of electronic health information."[6] For these purposes the Act creates a Trusted Exchange Framework and Common Agreement (TECFA), creating a network among authorized participants facilitating data exchanges to overcome existing barriers and to mitigate information blocking and withdrawal by relevant parties.[7] The Cure Act targets these objectives by setting shared standards establishing principles of transparency and non-discrimination specifically devoted to access to and research activities over electronic health information.[8]

In the EU, data sharing has lately become a key concern with the objective of boosting data availability within the European digital single market.[9] The European Commission has highlighted the importance of access to health data in its "European strategy for data."[10] Here, the creation of a "Common European health data space"[11] has been considered among the nine European data spaces the European Commission intends to encourage in the coming years.

Under the EU strategy for data, data pools shall be as "open as possible" and as "closed as necessary,"[12] so as to promote data re-usability and analysis across different sectors. The innovation principle, which, as the Commission underlines, ensures that "legislation is designed in a way that creates the best possible conditions for innovation to flourish,"[13] supports the sharing of data at regulatory level.

Accordingly, soft law tools have been used by the Commission in its Recommendation on access and preservation of scientific information[14] to directly target data-driven research objectives. Research

[2]In the European Union, there are experiences of integrated research platforms as the one developed within the SoBigData++ Horizon2020 project which delivers a distributed, Pan-European, multi-disciplinary research infrastructure for big social data analytics. One of the core objectives of the project is exactly that of mapping the ethico-legal concerns arising from collaborative data-driven innovation and operationalizing in the infrastructure the relevant principles and rules. *See* European Commission, *SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics*, Research Grant SoBigData-PlusPlus 871042, (Mar. 2, 2020), https://cordis.europa.eu/project/id/871042/it.

[3]Organization for Economic Cooperation and Development, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use Across Societies (2019).

[4]Michael J. Saks, Adela Grando, Chase Millea & Anita Murcko, *Advancing the Use of HIE Data for Research* 52 Ariz. State. L. J. 145, 176 (2020) [hereinafter Saks, Grando, Millea & Murcko].

[5]21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 45 C.F.R. § 170–71 (2020).

[6]*Id.* at para. 7424–01.

[7]Saks, Grando, Millea & Murcko, *supra* note 4, at 176.

[8]*See* Genevieve Morris & Elise Sweeny Anthony, *21st Century Cures Act Overview for States, The Office of the National Coordinator for Health Information Technology*, SIM State Educational Session 1 (Jan. 8, 2018), https://www.healthit.gov/sites/default/files/curesactlearningsession_1_v6_10818.pdf.

[9]European Commission Press Release IP/18/3364, Data in the EU: Commission Steps Up Efforts to Increase Availability and Boost Healthcare Data Sharing (Apr. 25, 2018).

[10]*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy for Data'*, at 7, COM (2020) 66 final (February 19, 2020) [hereinafter *European Strategy for Data*].

[11]European Data Protection Supervisor, Preliminary Opinion 8/2020 on the European Health Data Space (Nov. 17, 2020) [hereinafter Preliminary Opinion 8/2020].

[12]*European Strategy for Data*, *supra* note 10, at 15.

[13]*Ensuring EU Legislation Supports Innovation*, European Commission, https://ec.europa.eu/info/research-and-innovation/law-and-regulations/innovation-friendly-legislation_en.

[14]Commission Recommendation 2018/790 of Apr. 25, 2018, on Access to and Preservation of Scientific Information, 2018 O.J. (L 134/12) [hereinafter Recommendation 2018/790].

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

goals have been lately acknowledged by the Open Data Directive,[15] the Regulation regarding the free flow of non-personal information,[16] the Digital Single Market Directive,[17] as well as the proposed Data Governance Act.[18] All these set of rules are closely connected to the General Data Protection Regulation ("GDPR")[19] and help to unfold the pro-research potentials it has, especially with respect to datasets in which non-personal data and personal data are "inextricably linked."[20] Indeed, all these legislations expressly do not derogate the GDPR but build on it.

Against the backdrop of this evolving landscape, this article discusses the role of data protection laws in fostering a reliable and balanced framework for data sharing and related research objectives reaching conclusions opposite to mainstream literature.[21] In particular, it demonstrates that European data protection law does not hamper but rather encourages data-driven research.

For these purposes, the study critically challenges the shared belief that the apparently more severe and burdensome data protection regime laid down by the European legislator adversely affects data flows and with that data-driven research,[22] contrary to what occurs in the U.S., where the more fragmented and less developed data protection framework may facilitate data flows and related innovation patterns.[23]

As a disclaimer, we do not argue that the GDPR offers a perfect world; after all its wording is afflicted by many political compromises. However, we claim that its overall structure and content are naturally steered towards a balanced approach fostering research and research-based data sharing. In this approach, we move from the analysis of the GDPR's research goals and their specific rules. We thus explore how these rules enable suitable pathways for sharing research.

[15]Directive 2019/1024, of the European Parliament and of the Council of June 20, 2019 on Open Data and the Re-use of Public Sector Information, 2019 O.J. (L 172) 56 (June 26, 2019) [hereinafter Directive 2019/1024].

[16]Regulation 2018/1807, of the European Parliament and of the Council of Nov. 14, 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303) 59 [hereinafter Regulation 2018/1807].

[17]Directive 2019/790 of the European Parliament and of the Council of 17 Apr. 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/6/EC and 2001/29/EC, 2019 O.J. (L 130) 92.

[18]*Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020) [hereinafter *Proposal for Data Governance Act*].

[19]Council Regulation 2016/679, *supra* note 1. The European Commission has issued specific guidance regarding the interplay between the Regulation regarding the free flow of non-personal information and the General Data Protection Regulation. *See Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data*, COM (2019) 250 final (May 29, 2019) [hereinafter *Framework for the Free Flow of Non-Personal Data*].

[20]Council Regulation 2016/679, *supra* note 1, at art. 2(2); Regulation 2018/1807, *supra* note 16. The notion of 'inextricably linked' datasets has not been defined in the GDPR or in the Regulation on the free flow of non-personal information, but the European Commission has interpreted it as referring to datasets in which the separation between non-personal and personal data "would either be impossible or considered by the controller to be economically inefficient or not technically feasible." *Framework for the Free Flow of Non-Personal Data*, *supra* note 19, at 10.

[21]*See* David Peloquin, Michael DiMaio, Barbara Bierer & Mark Barnes, *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, 28 Eur. J. Hum. Genetics, 697, 697–705 (2020); Tania Rabesandratana, *European Data Law is Impeding Studies on Diabetes and Alzheimer's, Researchers Warn*, Sci. Mag., Nov. 20, 2019; Birgit Simell, Outi Törnwall, Iiro Hämäläinen, H-Erich Wichmann, Gabriele Anton, Paul Brennan, Laurene Bouvard, Nadia Slimani, Aurelie Moskal, Marc Gunter, Kurt Zatloukal, Joel Minion, Sirpa Soini, Michaela Mayrhofer, Madeleine Murtagh, Gert-Jan van Ommen, Mattias Johansson & Markus Perola, *Transnational Access to Large Prospective Cohorts in Europe: Current Trends and Unmet Needs*, 49 New Biotechnology 98–103 (Mar. 25, 2019); Andreas Wiebe & Nils Dietrich, Open Data Protection: Study on Legal Barriers to Open Data Sharing—Data Protection and PSI (2017); Lothar Determan, *Healthy Data Protection Law*, 26 Mich. Tech. L. Rev. 229–278 (2020).

[22]Mark Philipps & Bartha M. Knoppers, *Whose Commons? Data Protection as a Legal Limit of Open Science*, 47 J.L., Med. & Ethics, 106 106 (2019); Robert Eiss, *Confusion Over Data Privacy Law Stalls Scientific Progress*, 584 Nature 498 (2020).

[23]*See* Mike Hintze, *Science and Privacy: Data Privacy Laws and their Impact on Research*, 14 Wash. J.L. Tech. & Arts 103 (2019) [hereinafter Hintze]. *See also* Samantha Gilbert, *Is a Federal US Data Protection Regime Closer Than we Thought?*, Lexology (June 30, 2020) (reflecting on the innovation-friendly character of US fragmented data protection laws landscape), https://www.lexology.com/library/detail.aspx?g=21821e38-0a05-4ca5-8d69-3ba2a34ab6f1.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

B. Setting the Landscape

As recital 159 of the GDPR clarifies, the research objectives pursued by the Regulation are directly linked to the objectives set under Article 179(1) of the Treaty on the Functioning of the European Union, which encourages "the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely."[24] In light of these statements, data sharing is a "quasi-constitutional" mandate. These free circulation goals are directly connected with the market-integration objectives resulting from the free flow of personal data, the GDPR expressly pursues under Article 1(1) of the GDPR.[25]

Recital 2 of the GDPR states that the GDPR intends to contribute "to the economic and social progress" and "to the strengthening and the convergence of the economies within the internal market."[26] Accordingly, also recital 5 GDPR acknowledges that the "economic and social integration resulting from the functioning of the internal market" have facilitated the "exchange of personal data between public and private actors."[27] This market-based foundation of the GDPR stands directly behind the fundamental rights dimension of European data protection law, expressed under recital 1 and directly rooted in Article 8(1) ECFR and in Article 16 TFUE(1).[28]

In consistency with the set goals, the GDPR offers a specific framework regarding the processing of personal data for research purposes, primarily found under Articles 6(4); 5(1)(b); 9(2)(j) and 89 GDPR. Considering this research-based set of provisions, various scholars[29] have commented that the greater consideration of free flow of information and research objectives within the GDPR with respect to the previous Data Protection Directive, highlighting the occurrence of a "regime change" in European data protection law;[30] has led to a research facilitating regime[31] and the establishment of an outright research efficiency defense under data protection law.[32]

Building on this literature, this study moves from the acknowledgment of an existing gap in the literature as to how the GDPR can facilitate data-driven research in practice. It thus intends to answer largely unaddressed questions regarding where and how to draw the boundaries of openness allowed by the GDPR with respect to data sharing, and, in particular, the boundaries of openness for data sharing established and alimented for research purposes.

The analysis thus shows that there are many answers to the set questions, arguing that the two recalled European data protection law's regulatory pillars—fostering free flow of data while protecting fundamental rights—create an architecture of layered data protection regimes, which come to tighten data subjects' rights *vis à vis* massive data collection and processing activities on the one hand, and establish fruitful "enabling regulatory spots" for the processing of personal data on the other.

These differential data protection regimes applicable to data-driven research are not static and should be dynamically interpreted considering the flexibilities the GDPR provides. These flexibilities are leveraged taking the protection of fundamental rights with respect to the sharing of research-precious data—as health data—as a major concern and operationalizing it as an internal parameter of any sharing practice, also for research purposes.

[24]Treaty on the Functioning of the European Union art. 179(1), Dec. 13, 2007, 2012 O.J. (C 326) 47.

[25]Ionnanis Lianos, *Updating the EU Internal Market Concept*, *in* Fabian Amtenbrink, Gareth Davies, Dimitry Kochenov & Justin Lindenboom, The Internal Market and the Future of European Integration 495–548 (2019).

[26]Council Regulation 2016/679, *supra* note 1, at recital 2.

[27]*Id.* at recital 5.

[28]For a comment on these two pillars of the GDPR, see Giulia Schneider, *Health Data Pools under European Policy and Data Protection: Research as a New Efficiency Defense?*, 11 J. Intell. Prop., Info. Tech. & E-Commerce L. 1 (2020).

[29]Viktor Mayer-Schonberger & Yann Padova, *Regime Change: Enabling Big Data Through Europe's New Data Protection Regulation*, 17 Colum. Sci. & Tech. L. Rev. 315 (2016); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 Columbia Business Law Review 494 (2019).

[30]Schonberger & Padova, *supra* note 29.

[31]Wachter & Mittelstadt, *supra* note 29, at 102.

[32]Schneider, *supra* note 28, at paras. 86–98.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

This study proposes a "differential" interpretation of the GDPR's flexibilities based primarily on the different adherence of these differential data protection regimes to the parameters related to individual control objectives—data subjects in charge—and the free flow of information objectives—more extensive maneuvering ability for data controllers, or data controllers in charge. These different data protection regimes are first identified within the listed legitimate bases for data processing activities and further analyzed to describe how they balance the role and powers of the relevant stakeholders involved in the processing of personal data for research purposes.

The identified regimes differently address data subjects' control prerogatives and free flow of research data objectives by differentiating the safeguards requested and thus the standard of data protection required for private data pools, public data pools, and mixed private-public data pools.

Although we discuss health data pools, their regulatory framework as a case-study for their incredible research value,[33] and special consideration offered in any given jurisdiction, for example under Article 9 GDPR, our analysis has general relevance for any personal data sharing. The enquiry ultimately demonstrates that differential data protection regimes have a varied affect on the contractual freedom to share and aggregate personal data, which is the primary pillar of the creation of "common data spaces" envisaged under the latest European strategy for data. With respect to the case of health data, it shows how the GDPR offers specific data protection tools, capable of maximizing the research value embedded in health datasets, without unduly undermining patients' or data subjects' fundamental rights in the emerging "health data space."[34]

By unveiling the sophisticated nature of European data protection law with respect to data-driven research objectives, this study finally underlines the paradigmatic relevance of the resulting European regulatory model for both the interpretation of U.S. data protection regulations as well as their much-advocated reforms. Moreover it lays the basis for a possible alignment between the U.S. and European data protection regimes regarding research-oriented processing activities, which may be relevant especially with respect to EU-U.S. data transfers after the falling of the Privacy Shield.[35]

Under these general premises, the analysis requires a clear setting of the "legal" notion of research and of its scope across the ocean.

C. The Notion of Research Under Data Protection Laws: A Comparative Perspective

Big Data is deeply changing research methodology, and with it the range of public and private applications of the new insights collected through their use.[36] The sources of Big Data potentially valuable to medical researchers include electronic medical records and electronic health records,[37]

[33]Preliminary Opinion 8/2020, *supra* note 11, at 2. On Health Data Sharing, see Brígida Riso, Aaro Tupasela, Danya Vears, Heike Felzmann, Julian Cockbain, Michele Loi, Nana C. H. Kongsholm, Silvia Zullo & Vojin Rakic, *Ethical Health Data Sharing in Online Platforms—Which Values Should Be Considered?*, 13 LIFE SCI., SOC'Y & POL'Y 1–27 (2017).

[34]Preliminary Opinion 8/2020, *supra* note 11, at 7–14.

[35]Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems, ECLI:EU:C:2020:559, para. 201 (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404. For a comment on this case, see Christopher Kuner, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUR. L. BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

[36]Giulia Schneider, *Disentangling Health Data Networks: a Critical Analysis of Articles 9.2 and 89 GDPR,* 9 INT'L DATA PRIV. L. 253 (2019); Giovanni Comandè, *Ricerca in Sanità e Data Protection … Un Puzzle Risolvibile,* 41 RIVISTA ITALIANA DI MEDICINA LEGALE E DEL DIRITTO IN CAMPO SANITARIO 187, 189 (2019).

[37]Peter B. Jensen, Lars J. Jensen & Søren Brunak, *Mining Electronic Health Records: Towards Better Research Applications and Clinical Care*, 13 NATURE REVS. GENETICS 395–405 (2012).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

aggregate clinical trial data, administrative health care data,[38] genomic, and other -omics data,[39] along with health data collected using other means, and granular environmental data.[40] It is the case of health data collected by recording of online and physical activities of individuals, such as on mobile phones or wearable devices,[41] that are not labelled as medical devices.[42] This causes the same notion of "health data" to become increasingly diaphanous[43] and problematic in the data driven society.

As a result, research is evolving with a profound differentiation between data-driven and conventional approaches to research. First, researchers capture more comprehensively the data related to the phenomenon of their interest with all the environmental correlations, for example, being forced to assess trade-offs outside their normal range: Between data quality and quantity—for example—which are dimensions that are not in conflict in traditional research. Second, new methods of data analysis emerge to extract valuable information from more comprehensive data. For example, there are the various forms of machine learning put in place to detect patterns and correlations from data, as hypotheses to work on, rather than starting from a hypothesis and looking for data to work on.[44]

The ongoing changes in the ways research is conducted, the increasing relevance of data, and the involvement of both public and private stakeholders in research projects that are of an increasingly complex nature[45] render the legal notion of research a highly challenging interpretative battlefield at both the international[46] and supra-national level.

At a supra-national level, the definitions given to research and the rules provided with respect to processing operations of personal data conducted for research purposes greatly vary across jurisdictions. These differences are important to take into account because the legal uncertainties they engender may hamper the conduction of transnational collaborative research projects.

The following paragraphs will account for the differences in the definition of research between U.S. data protection laws and the European GDPR, setting the ground for a deeper analysis of the differential data protection regimes for research in the EU. The "differential" data protection regimes for research emerging from our analysis will provide relevant interpretative criteria for addressing legal uncertainties in minimizing these differences, favoring trans-oceanic data flows for research purposes.

[38]Janet Currie. '*Big Data' Versus 'Big Brother': On the Appropriate Use of Large-Scale Data Collections in Pediatrics*, 131 Pediatrics 127–132 (2013); Giovanni Comandè, Luca Nocco & Violette Peigné, *Il Fascicolo Sanitario Elettronico: Uno Studio Multidisciplinare*, 1 Rivista Italiana Di Medicina Legale e Del Diritto In Campo Sanitario 105–121 (2012).

[39]Vievien Marx, *Biology: the Big Challenges of Big Data*, 498 Nature 255–60 (2013); Fabricio F. Costa, *Big Data in biomedicine*, 19 Drug Discovery Today 433–440 (2014).

[40]Giovanni Comandé & Giulia Schneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-Ending Lifecycles of 'Health Data'*, 25 Eur. Jour. Health L. 284–307 (2018); Comandè, *supra* note 36 at 189.

[41]*Apple's Research, Kit frees medical research*, 33 Nature Biotechnology 322 (2015).

[42]Fabrico F. Costa, *Social Networks, Web-Based Tools and Diseases: Implications for Biomedical Research*, 18 Drug Discovery Today 272–81 (2013).

[43]Comandé & Schneider, *supra* note 40, at 286; Giovanni Comandè & Gianclaudio Malgieri, *Sensitive By Distance: Quasi-Health Data in the Algorithmic Era*, 26 Info. & Commc'ns Tech. L. 229–49 (2017).

[44]Giovanni Comandé, *The Rotting Meat Error: From Galileo to Aristotle in Data Mining*?, 4 Eur. Data Prot. L. R. 270–277 (2018).

[45]*See* Schneider, *supra* note 36, at 253–255.

[46]At international level, it is interesting to note that the UN Committee on Economic, Social and Cultural Rights issued a Draft General Comment on Science on January 2, 2020, which re-defines research from a human rights law perspective exactly in light of the "risks and promises of the so-called 4th industrial revolution." Committee on Economic, Social and Cultural Rights, Draft General Comment on Science, U.N. Doc. E/C.12/GC/25 (2020).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

I. Research under US Data Protection Laws

In the U.S., the Health Insurance Portability and Accountability Act (HIPAA), lays down rules for the protection of health information, specifically addressing the use and disclosure of such information for research purposes.[47] It lays down only a very general framework for the protection of patients' personal data, however, deferring to State laws for the definition of more specific standards. This creates a mosaic of privacy regulations disparately addressing privacy concerns and creating a substantial regulatory hurdle to data sharing among relevant stakeholders.[48]

HIPAA defines research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[49] It provides that health information can be processed for research purposes without the data subject's authorization only when there is a documented waiver approved by an Institutional Review Board (IRB) or Privacy Board[50] of the covered entity making the disclosure, the receiving entity, or an independent board.[51]

Under HIPAA, in the absence of the institutional waiver, the processing of data for research purposes requires data subjects' authorization.[52] In this case, HIPAA encourages the adoption of "data use agreements" on the processing of certain kinds of health information, which although not fully de-identified has been subject to the removal of certain direct identifiers.[53] Ultimately, HIPAA establishes a data subjects' right to receive an accounting for personal information that has been disclosed by covered entities for research purposes over the last six years.[54] This obliges the same covered entities to accurately document disclosures for research purposes in a way not dissimilar to what requires the accountability principle under the GDPR but in a more burdensome way because it is operated in a less structured environment to gather evidence and keep track of the various data flows.

Additional restrictions to the processing of personal data for research purposes, specifically regarding personal data regarding children, are provided by the U.S. Children's Online Privacy Protection Act (COPPA), which establishes the requirement of consent from the parents of the interested children limited to the collection and use of children's personal information for research purposes, but excludes the possibility of consent for the disclosure to third parties of such information for the same purposes.[55]

The recently enacted California Consumer Privacy Act,[56] although only binding at the State level, is important for its intended natural leading role across the country and globally. The

[47]For a general overview, see HHS Research, 45 C.F.R. §§ 164.501, 164.508, 164.512(i).

[48]*See* Michelle Mello, Julia Adler-Milstein, Karen Ding, Lucia Savage, *Legal Barriers to the Growth of Health Information Exchange: Boulders or Pebbles?*, 96 MILBANK Q. 110 (2018); Saks, Grando, Millea & Murcko, *supra* note 4.

[49]Health Insurance Portability and Accountability Act of 1996, Pub. L. no. 104-191, 76 [HIPAA].

[50]45 C.F.R. § 164.512(i)(1).

[51]Hintze, *supra* note 23, at 123. Similar conditions for the processing of personal data for research purposes are provided by the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), which permits "disclosures of personal information" for "scholarly study or research without notice or consent" when (i) the information to be processed is needed for the achievement of the set research objectives, (ii) it is impracticable to obtain consent; and (iii) the research organization "provides prior notice to the Privacy Commissioner of Canada." Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.) § 7(3)(f). The specificity of Canadian data protection law exactly lies in the requirement of prior notice to the data protection authority, which is very unique to the PIPEDA. *See* Hintze, *supra* note 23, at 122. However, it can be only related under the GDPR to the eventual prior consultation of the relevant Data Protection Autorithy in case a DPIA "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk" requiring a consultation only in these extreme cases.

[52]Saks, Grando, Millea & Murcko, *supra* note 4, at 166.

[53]HIPAA § 164.514(e).

[54]HIPAA § 164.528.

[55]Children's Online Privacy Protection Act, 16 C.F.R. § 312.5(a)(2) [COPPA].

[56]California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 [CCPA]. *See* Lothat Determann, *New California Law against Data Sharing*, 35, 10 COMPUT. & INTERNET L. 1–10 (2018).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

CCPA narrowly defines and circumscribes the notion of research only to public-interest oriented research activities, that is "scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health . . . ."[57] The Act further states that "personal information that may have been collected from a consumer in the course of a consumer's interaction with a business's service or device for other purposes" can be processed for research purposes, provided certain conditions are met. These conditions include the required compatibility of the research purposes with the business purposes for which the information was collected, the implementation of technical safeguards obstructing the reidentification of consumers, and the pseudonymization or deidentification of such information are envisaged.[58]

The CCPA excludes from the scope of research-oriented processing those activities serving commercial purposes,[59] defined as "the use of personal information for the business's or a service provider's operational purposes, or other notified purposes"[60] in order "to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction."[61] The California data protection law thus provides an objective-based definition of commercial-oriented research, which is based on the nature of the satisfied interest, rather than on the nature of the involved research entities. This objective interpretation of the notion of research under the CCPA helps clarify why the Act still considers as research those activities that are conducted in the realm of the "business purpose," defined as the use of personal information "for certain operational purposes or other notified purposes" including "undertaking internal research for technological development and demonstration."[62] In this way the CCPA still allows for non-commercial oriented research conducted by businesses.

When it comes to the processing of personal data for research purposes, the CCPA allows for a derogation to data subjects' right to have their personal information deleted.[63] The same regulation nonetheless envisages additional obligations onto controllers when it comes to the "sale" of personal information for research purposes.[64]

Against the backdrop of this brief overview of U.S. data protection provisions about research, it emerges that HIPAA does not appear to take into consideration the distinction between different types of research, such as for profit and public interest-oriented research. A different approach in this perspective has been conversely adopted by the California Consumer Privacy Act, which cuts off from the notion of research those processing activities that directly target a commercial interest. As has been observed in the literature,[65] however, by including in the business purpose research activities for internal "development and demonstration," the Act opens up to substantial ambiguities regarding what is to be considered research conducted for "business purposes," and research which serves a purely commercial and economic interest and cannot, according to the cited provisions, be included within the CCPA's notion of research and corresponding data protection rules. Although more privacy preserving, this regulatory option may block potentially innovative research projects, as the ones involving private players and thus commercial research.

[57]CCPA § 1798.140(s).

[58]*Id.*

[59]William Nicholson Price, Margot E. Kaminski, Timo Minssen & Kayte Spector-Bagdady, *Shadow Health Records Meet New Privacy Laws-How Will Research Respond to a Changing Regulatory Space?,* 363 SCIENCE 448, 450 (2019).

[60]This is the definition of "business purpose" under CCPA § 1798.140(d).

[61]CCPA § 1798.140(f).

[62]CCPA § 1798.140(d)(6).

[63]*Id.*

[64]The sale is defined as any transfer of data for "monetary or other valuable consideration." CCPA § 1798.140(t). For a comment on this, see Hintze, *supra* note 23, at 129.

[65]Hintze, *supra* note 23, at 131–32.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

Overall, although the analyzed regulations provide some allowances to processing activities for research purposes, as it occurs with the derogation to data subjects' right to deletion provided by the CCPA, they nonetheless establish significant burdens onto controllers engaging in research endeavors, such as the need to have a waiver approved by an institutional board under HIPAA or the requirement of technical safeguards and the enactment of pseudonymization techniques under the CCPA. These considerations suggest that while being subject to an alternative set of data protection rules, processing activities conducted for research purposes do not enjoy a much more favorable data protection regime under US data protection laws especially when compared to the differential regimes emerging in the GDPR.

II. Research under EU Laws and the General Data Protection Regulation

Research objectives through data re-usability have been very recently given primary importance within the European Commission's Strategy for data, which in the aim of creating and consolidating a single market for data, stresses the need to enhance the re-usability of public data also by businesses[66] and of private data by public institutions, for either public interest related research purposes and commercially-oriented innovation purposes.[67] In particular, the Strategy acknowledges the relevance of the use of private data for the public good, thus also for public-interest related purposes.[68]

It thus appears that at European policy level, a new principle of free movement of research data is emerging, encompassing 1) public data employed for public interest-related research purposes, 2) public data employed for commercial-related research purposes, 3) private data employed for public-interest related research purposes, and ultimately, 4) private data employed for commercial-related research and innovation purposes.

This principle is differently substantiated at the European regulatory level. For example, in the Recommendation on access to and preservation of scientific research and in the Open Data Directive research and scientific innovation objectives are directly promoted through the establishment of facilitated accessibility regimes regarding public data. The notion of research as shaped by these two frameworks resides on the paradigms of open science and open access.[69] It is restricted to publicly-funded research,[70] and is primarily linked to public interest purposes. Nonetheless, under both frameworks the re-usability of research data is envisaged also for research carried out for commercial purposes.[71] As we shall see, this policy baseline is fully coherent with the differential regimes provided for by the GDPR which the Open Data Directive expressly declares to abide to under Article 1(4).

Similarly focusing on publicly funded research, also in the Copyright Directive, recital 12 excludes from the notion of "research organizations" and thus from the correspondent research-enabling regime "organizations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, such as through their quality of shareholder or member, which could result in preferential access to the results of the research."[72] Based on such subjective definition, however, contrary to the Recommendation or the Open Data Directive, the Copyright Directive appears to implicitly draw a distinction between not-for-profit and public interest-oriented research entities, on the one hand, and organizations operating for commercial purposes on the other.

[66]Specifically referring to the re-usability of publicly-generated health data by businesses, see *European Strategy for Data*, *supra* note 10, at 7.

[67]*Id.*

[68]*Id.* at 6.

[69]*See* Directive 2019/1024, *supra* note 15, at recitals 27, 28, 31; Recommendation 2018/790, *supra* note 14, at recitals 11, 12, 13.

[70]*See* Directive 2019/1024, *supra* note 15, at art. 10; Recommendation 2018/790, *supra* note 14, at recital 6.

[71]*See* Directive 2019/1024, *supra* note 15, at art. 10; Recommendation 2018/790, *supra* note 14, at recital 4.

[72]Recommendation 2018/790, *supra* note 14, at recital 12.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

The Copyright Directive example illustrates that the categorizations and definitions of research at European level are far from being settled or harmonized as well.[73] However, in this context, European data protection law takes a distinctive position.[74] Research has a particularly important role within the General Data Protection Regulation, which overtly aims to facilitate research carried out over personal data.[75]

At a general level, recital 159 GDPR suggests that scientific research "should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and *privately funded research*."[76] Under the interpretation suggested by the cited recital, scientific research for the purposes of European data protection law encompasses research activities conducted by both public and private stakeholders, or more generally funded by public or private resources.[77] This multifaceted definition of scientific research has recently been welcomed by the German Data Ethics Commission, which includes both publicly and privately funded research, as well as commercially-oriented research such as product development and enhancement, in its definition of "research."[78]

A wide notion of research, similar to the one provided by the GDPR, encompassing both privately and publicly funded investigations has also been adopted by the recently issued proposal for a Data Governance Act, which stated that "scientific research, including for example technological development and demonstration, fundamental research, applied research and *privately-funded research,* should be considered as well purposes of general interest."[79]

In this perspective, the GDPR leads an approach different from the one taken by the described US data protection regulations, which have equally provided research-enabling data protection regimes.

The GDPR welcomes a more inclusive notion of research and the scope of applicability of the correspondent data protection regime is thus of broader reach. To this end, the German Data Ethics Commission has underlined the opportunity to exploit to the maximum the research privileges existing under European data protection law, as well as the need to consider research as a "particularly valuable good" when compared with other competing interests.[80]

1. The Tiziana Life Science Case

The challenges of distinguishing "qualified" processing activities carried out for research purposes from other processing activities mainly conducted to pursue an economic interest are well mirrored by the Italian rulings by the Tribunal of Cagliari[81] and the Italian Data

[73]*See also* Heiko Richter, *Open Science and Public Sector Information, Reconsidering the Exemption for Educational and Research Establishments under the Directive on Re-Use of Public Sector Information*, 9 J. INTELL. PROP., INFO. TECH. & E-COM. L. 51, 53 (2018).

[74]For instance, data protection law considers the relevance of coupling information from registries for the purposes of scientific research and in particular of health research, for the purposes of the generation of "new knowledge of great value with regard to widespread medical conditions, such as cardiovascular disease, cancer and depression." Council Regulation 2016/679, *supra* note 1, at Recital 157.

[75]GDPR Recital 157 expressly refers to the goal of facilitation scientific research, by stating that "in order to *facilitate* scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law." *Id.*

[76]Emphasis added.

[77]Schneider, *supra* note 36, at 253.

[78]*Id.*

[79]*Proposal for Data Governance Act*, *supra* note 18, at recital 35.

[80]Bundesministerium für Justiz und Verbraucherschutz, Opinion of the Data Ethics Commission, Jan. 22, 2020, no. 124, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.html;jsessionid=776E9EC21856B458D8F4D1927D7705C5.1_cid324?nn=11678512.

[81]Tribunal of Cagliari, Sentenza n. 1569 (June 6, 2017).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

Protection Authority[82] in the Tiziana Life Science Case. The controversy involved the transfer of genetic data from an Italian genomic biobank named Shard. Na, storing genetic and health data of Sardinian data subjects to the U.K.-based for-profit corporation Tiziana Life Science plc.[83]

The Italian Data Protection Authority[84] had blocked the transfer with an interim injunction, ordering the company Tiziana to inform the data subjects of the change of data controller and of the new research purposes for which the transferred genetic data would have been processed for. In addition to this, the DPA required the company to recollect consent from all the data subjects whose data was transferred.[85] Overturning this decision, the Tribunal of Cagliari ruled for the lawfulness of the processing of the genetic and health data acquired by the English company in view of the common research purpose shared by it with the genomic biobank.[86] The ruling was, however, soon followed by a subsequent decision of the Italian Data Protection Authority, again ordering the English company to block the processing of health data referring to the data subjects that had withdrawn their consent as a result of the occurred data transfer to the for-profit company.[87]

In these two decisions, the Italian Data Protection Authority signals the opportunity to distinguish between the diverse types of research—that is the public interest-oriented research carried out by Shard. Na and the profit-based research conducted by Tiziana Life Science Corporation—with the resulting need to apply to them different data protection regimes.

As the Authority has underlined, in the notice given to data subjects the purposes to which consent was linked were specifically related to the research activities of the Sardinian genetic bank.[88] Accordingly, it was stressed that many Sardinians had volunteered their genetic data to a public not-for profit research project and might have objected the swift change in controllership—public vs. private— and of purpose, from basic research to profit research.[89]

Despite referring to the Italian data protection framework before the General Data Protection Regulation, the case triggers many questions, which are of great interest also for the purposes of the implementation of current EU data protection law. These questions mainly regard the interaction and application of different data protection rules with respect to research projects based on the processing of personal data: can different research projects be treated alike under the General Data Protection Regulation? Is a one-size-fits-it-all model of data-driven research desirable with respect to the two data protection law's policy objectives of promoting the flow of personal information and of protecting data subjects' fundamental rights? Or should exactly the consideration of such rationales suggest the adoption of a diversified approach? Speaking in more technical terms, should a further processing operation carried out for research purposes be subject to a presumption of compatibility with the first processing operation likewise conducted for research purposes, as Article 6 (4) (a) and Article 5 (1) (b), along with referral 40 GDPR, seem to suggest? Should those secondary processing activities be considered lawful in case of data subjects' consent withdrawal? Under which legal basis?

[82]Italian Data Protection Authority, *Provvedimento di blocco del trattamento dei dati personali contenuti in una biobanca*, n. 389 (Oct. 6, 2016), https://www.garanteprivacy.it/pdf?p_p_id=PdfUtil&p_p_lifecycle=2&p_p_state=normal&p_p_mode=view&p_p_resource_id=%2Foffering%2FprintPDF&p_p_cacheability=cacheLevelPage&_PdfUtil_articleId=5508051

[83]For commentary on this case, see Luca Marelli & Giuseppe Testa, *Scrutinizing the EU General Data Protection Regulation—How Will New Decentralized Governance Impact Research?*, 360 SCIENCE 496, 498 (May 4, 2018).

[84]Italian Data Protection Authority, *supra* note 82.

[85]*Id.*

[86]Tribunal of Cagliari, *supra* note 81.

[87]Italian Data Protection Authority, *Provvedimento 21 dicembre 2017,* n. 561 (Dec. 21, 2017) https://www.garanteprivacy.it/pdf?p_p_id=PdfUtil&p_p_lifecycle=2&p_p_state=normal&p_p_mode=view&p_p_resource_id=%2Foffering%2FprintPDF&p_p_cacheability=cacheLevelPage&_PdfUtil_articleId=7465896.

[88]Italian Data Protection Authority, *supra* note 82, at 2.

[89]*Id.* The not-for-profit nature of the project was reflected by the collaboration between the genetic biobank Shard. Na and the CNR, which is the Italian national research center.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

The analysis that follows aims at providing clearer answers to these questions suggesting the existence of differential regimes under EU data protection law and showing how these are generally more favorable to research than the ones found in the U.S. data protection framework.

D. Health Data as a Case Study: The Legitimate Bases under Article 9 GDPR

To define the differential research data regimes under the GDPR we need to briefly describe the relevant legal bases for data processing. The GDPR provides a complex regulatory framework regarding health data. First, it provides specific definitions of different types of health data, such as genetic data or biometric data under Article 4(13)–(15) GDPR. Moreover, health data are considered as a "special category of data" and is subject to a specific regulatory regime under Article 9 GDPR. In line with the previous Data Protection Directive,[90] the GDPR conditions the processing of such special category of personal data to stricter data protection rules.

This stricter regime is directly substantiated in the prohibition of processing special categories of data under Article 9(1) GDPR, for simplicity we will use the "old" expression" sensitive data. The prohibition to process sensitive data under Article 9(1) GDPR is one of the most apparent expressions of the fundamental rights foundation of the General Data Protection Regulation.[91] This prohibition, however, is mitigated by the legitimacy of the processing of health data under specific and rather broad legal bases and in case certain conditions are met. These conditions are listed under Article 9(2) GDPR.

If one of the general legal bases for processing under Article 6 GDPR is met,[92] the legitimate bases for the processing of special categories of data, including health data under Article 9(2) GDPR, build up a mosaic of processing possibilities of sensitive data, health data in our use case, which need to be carefully interpreted with respect to the general prohibition regarding its processing.

By establishing a general prohibition of health data processing and some grounds of exceptions to that prohibition, the regulatory status of health data processing appears to be shaped by a

[90] *See* Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free movement of Such Data O.J. (L 281/31) art. 8 (Nov. 23, 1995); Art. 29 Data Protection Working Party, *Annex-Health Data in Apps and Devices* 1 (Feb. 5, 2015), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [hereinafter *Annex-Health Data*]; European Data Protection Supervisor, *Opinion on the Communication from the Commission on 'eHealth Action Plan 2012–2020—Innovative Healthcare for the 21st Century'*, 3 (Mar. 27, 2013), https://edps.europa.eu/sites/edp/files/publication/13-03-27_ehealth_action_en.pdf; *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records* 8 (Art. 29 Data Protection Working Party, Working Paper No. 131, 2007), https://www.dataprotection.ro/servlet/ViewDocument?id=228.

[91] In these regards, the Council of Europe has recently welcomed the higher threshold of protection regarding data concerning health, in view of the need to regulate its use so as to "guarantee due regard for the rights and fundamental freedom of every individual, in particular the right to protection of privacy and data protection," EUR. PARL. ASS., *Recommendation CM/Rec(2019) 2 of the Committee of Ministers to Member States on the Protection of Health-Related Data* 2 (Mar. 27, 2019), https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html. Along the same lines, the prohibition at stake is also consistent with the statements by the European Court of Human Rights, which has underlined the importance of protecting health data in the context of article 8 of the European Convention on Human Rights, stressing that "the protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Art. 8 of the Convention." *I v. Finland*, App. No. 20511/03, para. 38 (July 17, 2008), https://www.5rb.com/wp-content/uploads/2013/10/I-v-Finland-ECHR-17-July-2008.pdf; *Armonienė v. Lithuania*, App. No 36919/02, para. 40 (Nov. 25, 2008), https://en.efhr.eu/download/ecohr/CASE_OF_ARMONIENE_v._LITHUANIA_15.07.2014_en.pdf.

[92] The majority of the scholarship interprets GDPR article 9(2) not as a *lex specialis* of the *lex generalis* under GDPR Article 6, but as a complementary legal basis with respect to the ones listed under Article 6. This interpretation is more coherent with the stricter data protection regime regarding special categories of data under Article 9. *See* Edward S. Dove, *The EU General Data Protection Regulation*: *Implications for International Scientific Research in the Digital Era,* 46 J.L., MED. & ETHICS 1013, 1024 (2018) [hereinafter Dove].

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

layered regime, which triggers some challenging interpretative efforts. The different nature of the various legitimate bases under Article 9(2) GDPR has both theoretical and practical relevance, given that, as will be shown below, the choice of the applicable legal basis influences the scope of data subjects' applicable rights and has an affect on the developed data pools and derived products. For instance, without a legal basis different from consent, any withdrawal of consent would affect both the available data pool and the developed models.[93] Hence, a correct interpretation of the scope of these legal bases is of crucial importance to determine the closeness/openness of the data protection regime to be applied, and thus the reaction capabilities of involved data subjects. It is also crucial to design clear guidance for researchers both in the public and private domains.

Under these premises, the following paragraphs will identify the different data protection regimes that are associated to the legitimate bases applicable to data-driven research activities over special categories of data as health data under the GDPR. They will give account of the state of the art in the literature regarding the interpretation of these different regimes, which we will subgroup into three main categories. The first category relates to the fundamental rights-based pillar of the General Data Protection Regulation, directly based upon the protection of data subjects' right to informational self-determination through consent. Conversely, the second and third categories rely on some specific purposes to which data controllers' processing activities are bound, namely public interest or "purely" research-related purposes.

The mentioned legal bases describe a scale of different data protection regimes ranging from data subject-controlled to data controller-oriented ones.

These data protection regimes are given by the combination between the lawful bases under Article 9(2) GDPR and the specific rules the GDPR sets for research, namely the default compatibility with the purpose limitation principle under Articles 5(1)(b) and 6(4) GDPR on further processing for research purposes; and the provision under Article 89(1) GDPR requiring controllers to enact appropriate measures to safeguard data subjects' fundamental rights and freedoms that may be impaired in the course of research investigations. The framework resulting from the combined reading of these provisions is applicable whenever the processing over personal data is carried out for research purposes, irrespective of the legitimate basis on which the processing relies on. Accordingly, we assess the different interaction between the mentioned legal bases for the processing of personal data for research and Articles 5(1)(b); 6(4), and 89 GDPR along the lines of a dynamic spectrum ranging from data subjects' full control—consent with all its characteristics—for private data pools processed for profit purposes, to release and consequent loss of control with the exceptions to rights provided for by Chapter III GDPR for private or public data pools employed for non-profit, non-public interest research-oriented purposes.

In this perspective, we identify below a data subject-based, a public interest-based and a general research-based regime. This categorization is the result of the application to the legitimate bases under Article 9(2) GDPR of the two parameters of data subjects' control and free flow of personal information as defined in the scope of Article 1 GDPR. As will be highlighted, under the first data protection regime the data subjects' rights provided by Chapter III GDPR are fully actionable; under the public interest-based regime some derogations to ordinary data subjects' rights may be established by Union or national laws in accordance with Article 23 GDPR;[94] conversely, under the research-based regime, substantial derogations to those rights are envisaged directly in the GDPR and further ones can be introduced by state and Union law. However, in order to counterbalance the weakening of actionable data subjects' rights, the GDPR shifts the burden of care onto data controllers, which are required to enact adequate safeguards for the protection of data subjects' rights and freedoms: With greater powers come greater responsibilities.

[93] *See* 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) (art. 70.1.b)) (Jan. 23, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

[94] *See* Council Regulation 2016/679, *supra* note 1, at art. 23(1)(e).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

E. The Data Protection Regimes for Research

I. The Data Subject-Oriented Regimes: Consent under Article 9(2)(a) and 9(2)(e) GDPR

Just as the prohibition of processing under Article 9(1) GDPR, the first category of data protection regimes for the processing of special categories of data under Article 9(2) GDPR is to be directly contextualized in the individual fundamental rights' dimension of the General Data Protection Regulation. It comprises legitimate bases for processing, which are directly based upon the protection of data subjects' fundamental rights as the right to informational self-determination through consent.

Article 9(2)(a) and 9(2)(e) GDPR respectively allow the processing of special categories of data, provided data subject's consent is given and in case the data are made "manifestly public" by the data subject. In both cases the data subject is given the autonomy of choice over the processing of their sensitive personal data, thus directly exercising their right to informational self-determination.

Under Article 9(2)(a) GDPR, the given consent[95] needs to be explicit and must relate to one or more specified purposes in accordance with the principle of purpose limitation.[96] As newly required by the GDPR, consent must be "freely given" in a contractual relationship where there is no "significant imbalance" between the data subject and the controller.[97] The performance of the contract must not be "conditional on consent to the processing of personal data that is not necessary for the performance of a contract."[98]

Through the reference to explicit consent needed for the processing of data concerning health, the Regulation reaffirms the role of data subject's consent as a fundamental condition for the processing of sensitive data, as variously established in international declarations and guidelines regarding medical research.[99] Explicit consent was considered as the default regime for the processing of health data in

[95]*See* Council Regulation 2016/679, *supra* note 1, at art. 4 (defining consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."). For an overview of the notion of consent, see Art. 29 Data Protection Working Party, *Opinion 5/2011 on Consent* (July 13, 2011) [hereinafter *Opinion 5/2011*]; Art. 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (Apr. 10, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [hereinafter *Guidelines on Consent*]. Article 7 GDPR outlines some additional organizational and procedural requirements the data controller shall comply with with respect to the consent. *See* Council Regulation 2016/679, *supra* note 1, at art. 7 (stating that the controller shall request the consent "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language," and thus shall be able, through adequate measures of data governance, to "demonstrate that the data subject has consented to processing of his or her personal data." *See also* Comandè, *supra* note 33, at 189.

[96]*Accord* Council Regulation 2016/679, *supra* note 1, at art. 4.

[97]*Id.* at Recital 43.

[98]*Id.* at art. 7(4).

[99]The World Medical Association's Declaration of Helsinki calls for "informed consent, preferably in writing" and establishes the right of the data subject "to refuse to participate in the study or to withdraw consent to participate at any time without reprisal." *See* World Med. Ass'n., *Declaration of Helsinki*: *Ethical principles for Medical Research Involving Human Beings* paras. 25–32 (July 9, 2013), https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/. For a critical assessment on the Helsinki Declaration, see Christine Aicardi, Lorenzo Del Savio, Edward S. Dove, Federica Lucivero, Brent Mittelstadt, Maartje Niezen, Barbara Prainsack, Michael Reinsborough & Tamar Sharon, *Shortcomings of the revised 'Helsinki Declaration' on Ethical Use of Databases*, *in* Clinical Trials and Human Subjects Research (2016), https://www.thehastingscenter.org/shortcomings-world-medical-associations-revised-declaration-ethical-use-health-databases/. *See also* Convention on Human Rights and Biomedicine art. 5, Apr. 4. 1997, ETS No. 164 ("an intervention in the health field may only be carried out after the person concerned has given free and informed consent to it," provided appropriated information to the purpose and nature of the intervention, consequence and risks, and with the right to freely withdraw consent "at any time."); Convention on Human Rights and Biomedicine arts. 6–9, Apr. 4. 1997, ETS No. 164; International Organizations of Medical Sciences, International Ethical Guidelines for Biomedical Research Involving Human Subjects (2002) (establishing that for the processing of health data, voluntary informed consent of the prospective subject must be obtained and that waiver of informed consent is to be regarded as uncommon and exceptional, and must in all cases be approved by an ethical review committee). For a comment on these guideliness, see Dove, *supra* note 92, at 1021–1022.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

the context of scientific research[100] and is additionally required for the processing of personal data in case of automated individual decision making, such as profiling.[101] Yet, in several medical research contexts it is not advised to use consent as a legal basis for personal data processing.[102]

Already under the Data Protection Directive, the Article 29 Data Protection Working Party has specified that explicit consent must be given through an "express statement," such as a written statement signed by the data subject "in order to remove all possible doubt and potential lack of evidence in the future."[103]

As widely stressed by scholars, in the traditional data protection law architecture, consent is the fundamental means of control over the course of data processing activities.[104] It is strictly related to the individual values of autonomy and dignity,[105] which are structural elements of the individual fundamental right to data protection. It is thus a means for data subject's self-determination and self-empowerment. To these purposes, consent is associated with the reaction means newly provided by the General Data Protection strengthening data subjects' control over personal data.[106]

Note, however, that the notion and limits of consent under the GDPR are more stringent. Pursuant to Article 7 GDPR, "the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[107] Any violation of these requirements or more generally of the GDPR makes consent not "binding" and not valid. Moreover, consent should be withdrawable as easily as it was to give it.

The suitability of the legal basis of consent has been much debated both at general level and with specific regards to health research. From the first standpoint, the adequacy of using consent as a legal basis for data processing in the digital age has been widely questioned both in the literature and in policymaking processes. Consent's "pathologies" have been brought into the spotlight, especially in terms of unwitting consent, coerced consent, and incapacitated consent.[108] The shortcomings of consent models permeating the digital consumer landscape appear to sharpen what has been traditionally known as the "privacy paradox," given by the existing gap between what privacy—and consent—is theoretically meant for and what consumers actually do in practice.[109] As increasingly demonstrated also at empirical level, the understanding of the privacy policies is often quite weak, if not completely null.[110] As a result, consent has become a "free pass" for

[100]Paul Quinn & Liam Quinn, *Big Genetic Data and Its Big Data Protection Challenges,* 34 COMPUT. L. & SEC. REV. 1000, 1011 (2018); Secretary's Advisory Committee on Human Research Protections (SACHRP), Attachment B: European Union's General Data Protection Regulations (Mar. 13, 2018) ("[C]onsent is the basis most typically relied upon for processing personal data in research."), https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-b-implementation-of-the-european-unions-general-data-protection-regulation-and-its-impact-on-human-subjects-research/index.html.

[101]Council Regulation 2016/679, *supra* note 1, at 2 para. c.

[102]*See* European Data Protection Board, supra note 93.

[103]See *Opinion 5/2011*, *supra* note 95, at 18–19 ("In the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.").

[104]*See* Council Regulation 2016/679, *supra* note 1, at recital 7 ("[N]atural persons should have control over their personal data."). The perspective of consent as a means of control well suits the "will theory" of rights. *See* Yvone McDermott, *Conceptualising the Right to Data Protection in an Era of Big Data*, BIG DATA & SOC'Y 1, 3 (2017) (recalling the reconstruction of Herbert L.A. Hart, *Are There Any Natural Rights?*, 64 PHIL. REV. 175–91 (1955)).

[105]McDermott, *supra* note 104, at 3.

[106]Giulia Schneider, *European Intellectual Property and Data Protection in the Digital-Algorithmic Economy*, 13 J. INTELL. PROP. L. & PRAC. 229, 230–231 (2018); Orla Lynskey, *Deconstructing Data Protection: The Added Value of a Right to Data Protection in the EU Legal Order*, 63 INT'L & COMPAR. L. Q. 569–97 (2014).

[107]Council Regulation 2016/679, *supra* note 1, at art. 7.

[108]Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U L. REV. 1461 (2019).

[109]Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, (Nat'l Bureau of Econ. Rsch., Working Paper No. 23488, 2017).

[110]Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and the Terms of Service Policies of Social Netwoeking Services,* 23 INFO., COMMUC'N & SOC'Y 128 (2020).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

big businesses' data gathering practices.[111] With respect to possible remedies to these failures, there have been discussions about how to render privacy policies more effective.[112] Accordingly, new personalization and visualization schemes are being proposed by DPAs.[113]

These general considerations also apply in the context of data-driven health research, which increasingly relies on the sharing, aggregation and repurposing of data processing activities.[114] Nonetheless, the specificities of digital health research raise some additional, sector-specific concerns. For example, although voluntary participation in research might not be considered a contract in many jurisdictions, in those countries that acknowledge the possibility of a fee for participation or even a form of incentive might cast doubts on the freedom of consent, especially in case of economic or other vulnerabilities. Moreover, data-intensive health research has widely expanded the borders of research projects, which have become ever more interconnected and open-ended,[115] and is thus becoming structurally unsuitable with respect to the consent paradigm, designed for specific and "closed" research projects.[116]

As a result, alternative forms of informed consent, of more open and dynamic nature are considered more appropriate for the governance of the uncertainty and unpredictability of data-driven health research.[117] This opportunity has been concretely acknowledged within the General Data Protection Regulation, which under recital 33 GDPR admits consent given for "certain areas of scientific research"[118] under the condition that these areas of research respect the "recognized ethical standards for scientific research."[119] It is worth noting from the outset that these broad terms could unveil a Pandora's box notion of "research." It can remain questionable if recital 33 GDPR, having no binding force, is able to justify a reading of Article 9(2)a GDPR, which requires "explicit" consent for specific purposes, compatible with forms of wide-ranging consent, open to further use. This is likely to be the case, at least if the architecture used follows the parameters of recital 33 GDPR: broad consensus limited to specific areas of scientific research and accompanied by "recognized ethical standards for scientific research."[120]

[111]Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn,* 40 PACE L. REV. 307 (2020).

[112]*See, e.g.*, Zohar Efroni, Jacob Metzger, Lena Mischau & Marie Schirmbeck, *A Risk-Based Approach to Visualisation of Data Processing,* 5 EURO. DATA PROT. L. 352 (2019).

[113]*"Easy Privacy Information via Icons? Yes, You Can!" The Italian DPA Launches a Contest Calling for Creative Ideas from All Quarters*, EUR. DATA PROT. BD. (Apr. 14, 2021), https://edpb.europa.eu/news/national-news/2021/easy-privacy-information-icons-yes-you-can-italian-dpa-launches-contest_en.

[114]Brent Mittelstadt & Luciano Floridi, *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, 22 SCI. & ENG'G ETHICS 303 (2016); Comandè, *supra* note 36, at 189.

[115]Comandé & Schneider, *supra* note 40, at 286; Schneider, *supra* note 36, at 255.

[116]Jacob Metcalf & Kate Crawford, *Where are Human Subjects in Big Data Research? The Emerging Ethics Divide,* 3 BIG DATA & SOC'Y 1 (2016).

[117]Anne S.Y. Cheung, *Moving Beyond Consent for Citizen Science in Big Data Health and Medical Research*, 16 NORTHWESTERN J. TECH. & INTELL. PROP. 15, 25 (2018); Dara Hallinan & Michael Friedewald, *Open Consent, Biobanking and Data Protection Law: Can Open Consent Be 'Informed' Under the New General Data Protection Regulation,* 11 LIFE SCI. SOC'Y POL'Y, 1 (2015). In the context of bio-banking, forms of broad consent have already become the norm under the so-called FAIR (findable, acceptable, interoperable and reusable) principles. *See The FAIR Data Principles Explained,* DUTCH TECHCENTRE FOR LIFE SCIS., https://www.dtls.nl/fair-data/fair-principles-explained/.

[118]Chih-hsing Ho, *Challenges of the EU General Data Protection Regulation for Biobanking and Scientific Research*, 25 J.L., INFO. & SCI. 84, 93–94 (2017).

[119]Council Regulation 2016/679, *supra* note 1, at recital 33 ("It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."). For a comment on this, see Comandè, *supra* note 36, at 189. According to the literature, the reference to ethical standards imply approval by ethics committees and compliance with codes of conduct. *See* Quinn & Quinn, *supra* note 100, at 94.

[120]Council Regulation 2016/679, *supra* note 1, at recital 33.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

The possibility of a broad consensus for research purposes has been confirmed and further developed in the proposed Data Governance Act, in the form of a new notion of "data altruism," relating to "consent by data subjects to process personal data pertaining to them ... without seeking a reward, for purposes of general interest, such as scientific research purposes ...."[121]

Nevertheless, with respect to consent as a legal basis, there are still problems, mainly related to its revocability, which raise significant uncertainties in the research practice.[122]

In this respect, Article 29 Data Protection Working Party[123] has clarified that research purposes as well as relevant research areas need to be "well-described," nonetheless admitting the possibility that they are not "fully specified."[124] The legitimacy of consent for broad research purposes implies a partial derogation of the principle of purpose limitation. Nonetheless, in case of a lack of a specified purpose, the same Working Party mitigates this derogation, by advising data controllers to implement additional safeguards as the provision of a comprehensive research plan before the commencement of the project, as well as the implementation of adequate transparency measures enabling data subjects also to withdraw consent.[125]

In addition to this, the GDPR directly sets a derogation to the purpose limitation principle with respect to further processing for research purposes of personal data initially collected through consent. In this respect, the default compatibility rule under Article 6(4) GDPR and Article 5(1)(b) GDPR suggests that the processing of personal data for secondary purposes "in the public interest, scientific or historical research purposes or statistical purposes shall in accordance with Article 89(1), not be considered incompatible with the initial purposes"[126] and thus it is considered lawful under Article 6(4) GDPR, even if such further processing is not based upon the data subject's consent.[127]

The joint consideration of the possibility of a broad consent for the initial processing of health data for research purposes under Article 9(2)(a) GDPR, as interpreted in light of recital 33 GDPR and the recalled Working Party's guidelines on consent, as well as the mentioned default presumption of compatibility regarding secondary processing for research purposes, show how a very weak impulse by the data subject through a broad consent could apparently legitimize potentially infinite cycles of processing activities for various, different research purposes. In this respect, it is important to observe that the derogation of the purpose limitation rule for research would enable not only the sharing of sensitive health data among different businesses, but also the re-use of data by different research teams within broader corporate teams. For example, this is the case within big tech companies where there are often no separate research departments. Nonetheless, since the derogation to the purpose limitation principle is limited to research, the data should not be further used within a same corporate team for purely commercial, non-research-driven purposes. Here, the principle of segregation of

[121] *Proposal for Data Governance Act*, *supra* note 18, at art. 2 para. 10; *see also* Council Regulation 2016/679, *supra* note 1, at recital 38.

[122] David Townend, *Conclusion: Harmonization in Genomic and Health Data Sharing for Research: An Impossible Dream?*, 137 Human Genetics 657 (2018).

[123] *Guidelines on Consent*, *supra* note 95, at 27–30.

[124] *Id.* at 28.

[125] *Id.*

[126] Council Regulation 2016/679, *supra* note 1, at art. 5(1)(b).

[127] Emphasis added. The rule is further confirmed by Council Regulation 2016/679, *supra* note 1, at recital 50. Article 6(4) GDPR introduces criteria for the compatibility test, which the data controller has to carry out on a case-by-case basis, taking into account, amongst other factors, "any link between the purposes for which the personal data have been collected and the purposes of the intended further processing," "the context in which the personal data have been collected," and "the nature of the personal data, in particular whether special categories of personal data are processed." Council Regulation 2016/679, *supra* note 1, at art. 6(4)(a)–(c). As expressed by recital 50 GDPR also "the reasonable expectations of data subjects on the basis of their relationship with the controller as to their further use." *See* Council Regulation 2016/679, *supra* note 1, at recital 50. *See also* Marelli & Testa, *supra* note 83, at 496–97.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

personal data processing,[128] similar to what is clearly set out in the Data Governance Act for data sharing entities,[129] would be paramount in guaranteeing a clear respect of the purpose limitation principle. However, the borders between research-based and commercial-based data processing activities conducted within a same corporate unit could be quite difficult to draw, even if their corresponding personal data processing are correctly mapped in the records. In this specific case, when data is used for commercial purposes by a corporate unit, no default compatibility rule can apply and the relevant data should be processed in accordance with a full application of the purpose limitation principle demanding that datasets are processed in consistency with the "specified, explicit and legitimate" purposes for which the data has been originally collected. Accordingly, a proper respect of this principle requires to use the data only for the specific project for which they have been collected and not for other projects/purposes.

Yet, there is an inherent tension between recital 33 GDPR, not binding by definition, and the mentioned Working Paper 29 guidelines under the regime of the Data Protection Directive on the one hand and the recalled notion of consent under the GDPR –that need to be specific pursuant to Article 7 GDPR.

A way forward putting at ease those tension might emerge from the systemic interpretation we envisage. For instance, blanket consent might be more welcome if and when it is related to public interest research or in favor of public good institutions. Furthermore, blanket consent might be "more" acceptable when the same data processing is assisted by another suitable legal basis.

In any event, it is possible to sustain the general stricter scrutiny for the validity of consent in the research domain needs to be read in connection with recital 33 GDPR and that the formula clearly uses the language of the protection of the fundamental right to data protection but actually opens the way to both 1) blanket consent, as long as it unfolds "with recognized ethical standards for scientific research", and 2) to select specific research projects' objective aim of consent, or entities-subjective criteria, as assumed in the Tiziana case by the DPA and confirmed by the proposed Data Governance Act.

Under these premises, the legal basis of the explicit consent is to be aligned to the legitimate basis under Article 9(2)(e) GDPR, regarding the processing of sensitive data that are "manifestly made public by the data subject", since it equally implies the release of personal data based on the data subject's will. However, it is particularly problematic, since it could be applied to all the data that is "made public" online, in social networks or in specific online communities, without the need of a consent, be it of specific or of broad nature, or the enactment of safeguards offering the outer limits of the perimeter of a lawful data processing of sensitive data. This basis could thus potentially legitimate free flows of sensitive data as a result of their publicity. Nonetheless, the applicability of general data subjects' rights under Chapter III GDPR still assures the preservation of a certain degree of individual control over such data flows and the ability to challenge the requirement of being "manifestly made public."

In line with the guidance provided by referral 33 GDPR, personal data can be "manifestly made public" by selecting, for instance, kinds of project or data controllers creating a very simple avenue for data subjects' contribution to research. In a sense, data subjects are enabled to directly express

[128]Council Regulation 2016/679, *supra* note 1, at art. 89(4).

[129]*See, e.g.*, *Proposal for Data Governance Act*, *supra* note 18, at ref. 26. ("A key element to bring trust and more control for data holder and data users in data sharing services is the neutrality of data sharing service providers as regards the data exchanged between data holders and data users. It is therefore necessary that data sharing service providers act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose. This will also require structural separation between the data sharing service and any other services provided, so as to avoid issues of conflict of interest. This means that the data sharing service should be provided through a legal entity that is separate from the other activities of that data sharing provider. Data sharing providers that intermediate the exchange of data between individuals as data holders and legal persons should, in addition, bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data holders."). *See also Proposal for Data Governance Act*, *supra* note 18, at art. 11.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

their consent to a given and known data controller or to express their will towards unidentified data controllers with the ability of setting the terms of this implied consent by publication. Note that, by managing their autonomy along the lines of Article 9(2)(e) GDPR, data subjects simplify data controllers' compliance without burdening them with further latches even when data subjects select projects or data controllers they want to contribute to.

II. The Public Interest-Oriented Regime under Article 9(2)(i) and Article (9(2)(g)

Shifting from data subject-based regimes to controller-based legal bases for the processing of health data, the GDPR allows for many exceptions to the general prohibition of processing special categories of data, as health data.

For our purposes, however, we are interested in the notion of public interest directly concretized by Article 9(2)(i) GDPR referring to the purposes of "protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices."[130] The link between public interest and the protection of the right to health as enshrined in some Member States' constitutions has been assessed by the Article 29 Data Protection Working Party,[131] which has underlined how every processing activity that is functional to the protection "against serious cross-border threats to health" or the safeguard "of high standards of quality and safety of health care" are to be considered of public interest-oriented nature. In the absence of further indications, it has however left controllers to set the boundaries of what is necessary to safeguard "high standards of quality and safety of health care."

The public health interest exception offered by Article 9(2)(i) GDPR clearly encompasses, among others, post market studies, observational studies, and pharmacovigilance activities. Note, however, that these processing activities must be grounded in "Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."[132] The public interest clause is employed in many ways at both normative and policy level and is mostly defined on a case-by-case basis. In the absence of a determination by national legislators, the guidelines of data protection authorities are to be taken into consideration.[133] Here, what is relevant is that the GDPR qualifies in terms of public interest the research—post-market, observational studies, pharmacovigilance—ensuring "high standards of quality and safety of health care and of medicinal products or medical devices." In this way it appears to legitimize personal data processing for public interests that at the same time serve also private interests. Post market studies and product monitoring, although fulfilling legal duties, clearly serve legitimate and business interests of data controllers generating data that under the GDPR regime can more easily be further processed for

[130]The analysis applies also to art. 9(2)(g) GDPR.

[131]*Annex-Health Data*, *supra* note 90, at 13.

[132]*Id.* at 12–13 (recalling the European Court of Human Rights jurisprudence, defining the features of the law causing the interference with a fundamental right such as the one of to private and family life under art. 8 ECHR, and highlighting that the law "must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."); *Rotaru v. Romania*, App No. 28341/95, para. 55 (May 4, 2000) (expressing this principle), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}; *Hasan and Chaush v. Bulgaria*, App. No. 30985/96, para. 84 (Oct. 26, 2000), https://minorityrights.org/wp-content/uploads/old-site-downloads/download-382-Hasan-and-Chaush-v-Bulgaria.pdf; Council Regulation 2016/679, *supra* note 1, at art. 6 para 2–3; Council Regulation 2016/679, *supra* note 1, at recital 10, ("regarding the processing of personal data for compliance with a legal obligation, *for the performance of a task carried out in the public interest* or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation.") (emphasis added); Evert-Ben Van Veen, *Observational Health Research in Europe: Understanding the General Data Protection Regulation and Underlying Debate*, 104 Eur. J. Cancer 70, 76 (2018) (stressing that that the decision regarding what constitute a reason of public interest must be defined by a democratically accountable body).

[133]Giovanni M. Riccio, Guido Scorza & Ernesto Belisario, GDPR e Normativa Privacy-Commentario 101 (2018).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

secondary research using the presumptions of "non-incompatibility in Article 5(1)(b) GDPR, the compatibility test in Article 6(4) GDPR, and the general research regime in Article 89 GDPR.

Within the system of the General Data Protection Regulation, the public interest aim embedded in the legal basis under Article 9(2)(i) GDPR regarding sensitive data is to be aligned to the one generally envisaged under Article 6(1)(e) GDPR, regarding processing activities that are "necessary for the performance of a task carried out in the public interest."[134] The notion of "the task carried out in the public interest" has been interpreted by the U.K. Data Protection Authority in accordance with an objective criterion based on the nature of the purpose of the processing and not on the nature of the controller,[135] clarifying that any organization either private or public can rely on this basis.[136] This approach appears consistent with the one also upheld by the European Data Protection Board, which has specified that the processing of personal data for the purposes of clinical trials' procedures is to be considered as a task carried out in the public interest, when "the conduct of clinical trials directly falls within the mandate, missions and tasks vested *in a public or private body by national law*."[137]

As the Article 29 Data Protection Working Party had already outlined under the Data Protection Directive, the public interest clause is an expression of the flexibilities within data protection law, enabling to strike the appropriate balance between the protection of data subjects' rights and other collective interests.[138] It is worthwhile noticing that article 9(2)(i) GDPR does not expressly mention the need to "respect the essence of the right to data protection," as does, for instance, article 9(2)(g) GDPR. This because article 9(2)(j) GDPR assumes that the general framework for "medicinal products or medical devices" already "provides for suitable and specific measures to safeguard the rights and freedoms of the data subject" and thus already respects such an essence. Otherwise, the provision and the recalled rules would be in violation of the Treaties and subject to be struck down by the European Court of Justice (ECJ).

Overall, the notion of "the essence of the right to data protection" is recalled for instance also under Article 23(1) GDPR, allowing for Union or Member State laws' restrictions to the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34. Under EU law the elements constituting the essence of the fundamental rights to personal data protection are basically listed under Article 8(2) of the EU Charter of Fundamental Rights According to this provision the principles of purpose specification, fairness in processing on a legitimate basis laid down by law along with the right of access to one's own personal data and the right together with the control by an independent authority. Along these lines, the ECJ has concluded that legislation not providing for any possibility of pursuing legal remedies to access, rectify or erase their personal data "does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."[139]

The fact that Article 9(2)(i) GDPR does not recall the requirement to respect "the essence of the right to data protection" allows, with the mentioned caveats, higher pressure on the right to

[134]Dove, *supra* note 92, at 1023.

[135]*See* Lydia F. De La Torre, *What is 'Public Interest' Under EU Data Protection Law?*, MEDIUM (5 February 2019) https://medium.com/golden-data/what-is-public-interest-under-eu-data-protection-law-a8ef4637724a.

[136]Council Regulation 2016/679, *supra* note 1, at recital 45; INFORMATION COMMISSIONER'S OFFICE, PUBLIC TASK https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/lawful-basis-for-processing/public-task/; Comandè, *supra* note 36, at 193.

[137]European Data Protection Board, *supra* note 93, at 7 (emphasis added).

[138]*Annex-Health Data*, *supra* note 90, at 12.

[139]*See* Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, ECLI:EU:C:2014:2081 (July 17, 2014); Case C-615/13 ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority, ECLI:EU:C:2015:489 (July 16, 2015); *see also* Case C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], ECLI:EU:C:2015:650 (Oct. 6 2015) (concluding that legislation not providing for any possibility of pursuing legal remedies to access, rectify or erase their personal data "does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.").

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

personal data protection when public health or "quality and safety of health care and of medicinal products or medical devices" are at stake. This is well reflected by Article 23 GDPR, which explicitly allows EU or Member States laws to restrict the applicability of—and thus set derogations to—Articles 12–22 GDPR or Article 5 GDPR, establishing fundamental data protection principles such as, amongst others, the principle of data minimization and accuracy, when the processing serves "important objectives of general public interest of the Union or of a Member State," as public health.[140] Also Article 17(3)(c) GDPR, which directly refers to Article 9(2)(i) GDPR, admits derogation to data subjects' right to erasure when the derogation is needed for "reasons of public interest in the area of public health." Moreover, as will be better shown below other derogations under Article 14(5)(b) and Article 89(2) GDPR can be allowed for with respect to processing activities under Article 9(2)(i) GDPR.

However, as the GDPR clarifies, the balance between the competing interests of data subjects and data controllers always has to respect the "essence" of the right to data protection in accordance with the proportionality principle[141] and through the enactment of suitable and specific measures to safeguard data subjects' fundamental rights and interests.[142]

The importance of anchoring personal data processing activities carried out for public interest purposes to the parameters of proportionality and necessity has been underlined also by the ECJ,[143] which has affirmed that "the protection of the fundamental right to respect for private life at the European Union level requires that derogations from the protection of personal data and its limitations be carried out within the limits of what is strictly necessary."[144] This means, firstly, that if another legal basis more respectful of the data subjects' rights and interests, such as consent, can be relied upon by the controller for the achievement of the same purpose, then this must be chosen.[145] Yet, these clarifications were suggested under the previous data protection regime when the exception envisaged by Article 9(2)(i) GDPR did not exist. Secondly, exactly the principles of proportionality and necessity assure that the data subjects' rights as set by Chapter III GDPR are not undermined or somehow restricted in case of processing for public interest reasons. This means that the data subjects shall maintain control of such processing activities through their information rights and their corresponding reaction tools.

A further limit for the respect of the essence of the right to data protection is directly given by the principle of purpose limitation, which harshly cuts out from the realm of public interest-oriented processing activities those that serve different purposes, as commercial purposes. This is directly acknowledged by recital 54 GDPR, stating that the processing of personal data concerning health for public interest purposes shall not result in the same data being processed for other purposes by third parties, as employers or insurances and banking companies.[146] However, here the principle of purpose limitation finds a special discipline for research under Article 5(1)(b) GDPR, the presumption of compatibility if Article 89 GDPR is applied, and Article 6(4) GDPR, a test for further use.

[140]Council Regulation 2016/679, *supra* note 1, at art. 23(1)(e).

[141]*See* Council Regulation 2016/679, *supra* note 1, at art. 35(7)(e) (establishing data controllers' obligation to assess the "necessity and proportionality of the processing operations in relation to the purposes.").

[142]The essence of the right to personal data protection is directly connected to its nature of fundamental right under Article 8 paras. 2–3 of the European Charter of Fundamental rights. As a result, the infringement by any national or Union provision of the right to data protection, would also infringe the Treaties.

[143]Case C-73/16, Puskar v. Finance Directorate of the Slovak Republic, ECLI:EU:C:2017:725 (Sept. 27, 2017) (interpreting "task carried out in the public interest" as a legitimate basis for processing personal data under art. 7(e) of the previous Data Protection Directive).

[144]Case C-362/14, Schrems v. Data Protection Commissioner, at para 112.

[145]Quinn & Quinn, *supra* note 100, at 1013.

[146]*See* Council Regulation 2016/679, *supra* note 1, at recital 54; Price, Kaminski, Minssen & Spector-Bagdady, *supra* note 59, at 450.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

In short, the GDPR offers a different and more data-controller-oriented regime for the research aims mentioned under Article 9(2)(i) GDPR moving along the spectrum by authorizing data processing without consent and opening to further research uses, provided appropriate safeguards are offered. These are instances in which both public and private research aims are pursued and in which clearly research is mostly run by private—and for-profit entities.

The scaling of possibilities in our spectrum of data protection regimes for research finds another instance—reflecting the proportionality principle described above—in Article 9(2)(g). Contrary to Article 9(2)(i) which is specific for "public interest in the area of public health," Article 9(2)(g) is of general relevance and requires—in addition to the requirements provided by Article 9(2)(g)—that the public interest is "substantial" and that the legislation defining it along with the needed safeguards respects "the essence of the right to data protection."

III. The Research-Based Regime under Article 9(2)(j) GDPR

The third category of data protection regimes progressively offering a more liberal legal framework regards processing activities over special categories of data conducted for research purposes. Research is indeed an autonomous legal ground for the processing of special categories of data, as health data, under Article 9(2)(j) GDPR, which states the legitimacy of the processing when this is "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" if:

a) In accordance with Article 89(1);
b) is based in Union or Member State law, which will thus have to define the activities that fall under the scope of research as a legitimate basis for the processing of special categories of data;
c) it is proportionate to the aim pursued, consistently with the proportionality under art. 5(1)(b);
d) it respects the essence of the right to data protection;
e) it is subject to suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[147]

As can be derived, the legitimate basis under Article 9(2)(j) GDPR is shaped similarly with respect to the public interest-oriented ground for processing under Article 9(2)(g) GDPR. The major difference between the two legitimate bases is given by the explicit link of the former to Article 89(1) GDPR. Conversely, it is interesting to notice that both the considered provisions, unlike what occurs under Article 9(2)(i) GDPR, make reference to the respect of the essence of the fundamental rights to data protection. This is not surprising since the legitimate bases respectively regarding research under Article 9(2)(j) GDPR and the public interest 9(2)(g) GDPR are of very general scope and do not precisely list the sectors, respectively for research and the public interest, to which these legitimate bases apply, to the contrary of the provision under Article 9(2)(i) GDPR that makes a specific list of the cases relevant for "the public interest in the area of public health."

This regime requires the safeguards enacted by the controller to assure the respect of the principle of data minimization. The principle as generally expressed under Article 5(1)(b) GDPR is certainly applicable also to the processing for public interest purposes and to consent as a legitimizing basis for processing. Nonetheless, the explicit reference to the principle under Article 89(1) GDPR—recalled by Article 9(2)(j) GDPR—suggests that in case of processing activities for research purposes grounded in the legitimate basis of research there must be a strengthened compliance with data minimization goals: To the larger maneuvering room for data controllers

[147]Comandè, *supra* note 36.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

corresponds a smaller ability to contractually derogate exactly because data subjects have reduced avenues to monitor the actual enforcement of the data minimization principle. The legislator sets it as a driving principle to data controllers, calling to its strict adherence exactly because appropriate safeguards are established by data controllers themselves policed only by the principle of accountability but not, eventually, by the exercise of data subjects' rights.

Indeed, this stricter interpretation of the safeguards under Article 9(2)(j) GDPR with respect to the ones justified under Article 9(2)(g) GDPR is to be better understood considering the possibility to derogate to data protection principles and rights available to controllers undertaking research activities. This softening in the data protection system requires tighter data protection measures from the controllers' side to comply with the "essence of the right to data protection" recalled by Article 9(2)(j) GDPR. The switching of the power of setting the stage for data processing from data subjects—consent and manifestly public data—to data controllers—for research purposes without consent—signaled by the constraints to data subjects' rights revolves around more defined boundaries to set up appropriate safeguards, and above all the respect of the data minimization principle. When the general data protection principles as the one of purpose and storage limitation under Articles 5(1)(b) and 5(1)(e) GDPR and other data subjects' rights are derogated, then the protection of the "essence of the right to data protection" needs to be achieved by other means, and cannot suffer a compression also of the data minimization principle around which revolves the indications of Article 89 GDPR in term of safeguards.

Under these premises, the next sections will analyze the special data protection research regime as normatively shaped by the Regulation, identifying the derogations it sets in case of research activities for research purposes and providing some first interpretative guidance regarding the required safeguards on how GDPR opens the personal data flow.

IV. The EU Data Protection Rules for Research: The Derogations

On a general level, it can be outlined that the rules applicable to processing activities encourage on the one hand the processing of personal data for research purposes through significant derogations to ordinary data protection principles and rights. These derogations are nonetheless paired with the requirement of enacting appropriate measures to safeguard data subjects' fundamental rights and freedoms under Article 89(1) GDPR. The framework resulting from the combined reading of these provisions offers the parameters for the research exemption applicable whenever the processing over personal data is carried out for research purposes, irrespective of the legitimate basis on which the processing relies.

The derogations in case of processing for research purposes involve, first, important data protection law principles, as the principle of storage limitation under Article 5(1)(e) GDPR and the principle of purpose limitation under the above-recalled default compatibility rule under Article 6(4) and Article 5(1)(b) GDPR offering a presumption of compatibility. The mentioned provisions in turn derogate to the principle of data minimization established under Article 5(1)(c) GDPR. The default compatibility rule proves to be particularly difficult in the interplay of different legitimate bases and of data protection regimes for research, as will be assessed below.

Also, data subjects' rights as the right to be forgotten under Article 17(3)(c) and (d) GDPR can be derogated in case the enactment of the right impairs the achievement of the research objectives. Specific attention is to be given also to the possible derogation under Article 14(5)(b) GDPR to data subjects' right to be informed when the processed data is collected from third party sources and not directly from the data subjects, in case the "provision of such information proves impossible or would involve a disproportionate effort."[148] This last derogation is quite far-reaching since

[148] As observed by some scholars, compliance with the transparency requirements within long data-driven research projects could be disproportionate and substantially impair the objectives of the processing, especially when there are many data subjects involved and the data has been heavily pseudonymised. *See* Quinn & Quinn, *supra* note 100, at 1014.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

it allows controllers processing health data for research purposes to diminish the information they have to disclose to the data subjects in the privacy notice.

The two derogations to the right to erasure, under Article 17 (3)(c) and (d) GDPR, and the right to be informed, under Article 14(5)(b) GDPR, appear to be structurally incompatible with the legitimate basis of consent. In this respect indeed, the data subject has established a direct relationship with the data controller through its consent. The eventual withdrawal of consent would automatically block the processing activities of the data subject's personal information, with a *de facto* erasure of the relevant data from the controllers' databases, in consistency with the principle of storage limitation under Article 5(1)(e) GDPR. The provision indeed requires data controllers to store data as long as it is "necessary for the purposes for which the personal data are processed." In case of consent withdrawal this necessity to store the data would be radically voided, this leading to an automatic data erasure. Similarly, with respect to the data subject's right to receive information under Article 14 GDPR, the fact that the subject has given its consent first presupposes the release by the controller of the information needed to shape an informed consent. In second stance, the existence of a consent from the data subject itself eases the provision of information to the data subject by the data controller, thus excluding a situation in which the data controller faces an impossibility or a "disproportionate effort" to provide the relevant information, as required under Article 14(5)(b) GDPR.

On the contrary, the concerned derogations are highly relevant when the processing is based on the other legitimate bases not only under Article 9(2)(j), but also under Article 9(2)(i) GDPR, which is expressly recalled under Article 17(3)(c) GDPR. In this case, indeed the derogations directly facilitate the achievement of the particular objectives of the processing in the context of public health interventions and of research enquiries. Accordingly, the derogations can be relied on by data controllers also in case of secondary processing of datasets that were originally processed on the basis of the data subjects' consent and that are then grounded in the pursuing of a public health or pure research goals.

When the data are directly collected from the data subject, the controller still needs to comply with information duties under Article 13 GDPR, unless, as described by recital 62 GDPR, "the provision of information to the data subject proves to be impossible or would involve a disproportionate effort."

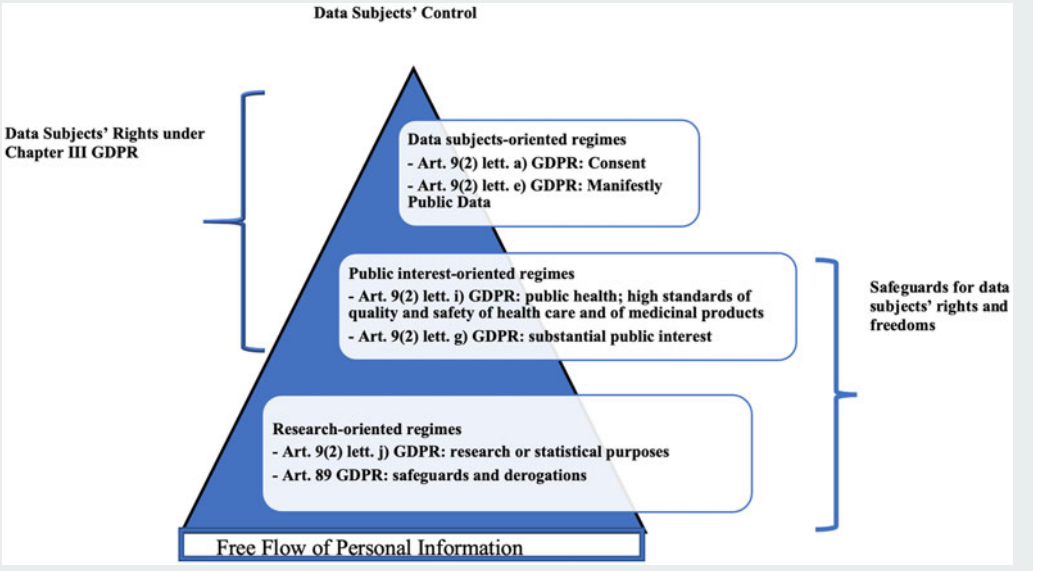
In addition to the derogations directly established by the Regulation, under Article 89(2) GDPR Member States can issue further derogations from data subjects' right to access under Article 15 GDPR; right to rectification under Article 16 GDPR; right to restriction of processing under Article 18 GDPR; and ultimately the right to object under Article 21 GDPR. These derogations can be provided only when the full enforcement of data subjects' rights "are likely to render impossible or seriously impair the achievement of the objectives of that processing" and these derogations are necessary for the fulfilment of the purpose.[149] Additional derogations by national laws to data subjects' rights under Articles 12–22 GDPR are permitted by the recalled provision under Article 23(1)(e) GDPR when the processing targets public health objectives.

These national-based derogations under Articles 89(2) and 23(1)(e) GDPR should be applicable only when the processing for research purposes is based on the legitimate grounds under Article 9(2)(i)–(j) GDPR, and not when these are based on consent under Article 9(2)(a) GDPR (Table 1): consent and the controller-data subject relationship directly activated by consent should indeed pose data controllers in the ease of protecting the mentioned data subjects' rights. Conversely, the specificities of processing operations for reasons of public interest in the area of public health, Article 9(2)(i) GDPR, or for research purposes, Article 9(2)(j) GDPR, may well justify the establishment of the mentioned derogations by national laws, in light of the excessive

[149]Council Regulation 2016/679, *supra* note 1, at art. 89. With regards to processing for scientific purposes, the English Data Protection Bill, approved in 2018, has established derogations with regard to the right to access under art. 15 GDPR; to rectification under Article 16 GDPR; to object under Article 21 GDPR.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

Table 1. Data Protection Regimes for Research under Article 9(2) GDPR



burden data controllers could face for satisfying data subjects' requests in these particular processing circumstances.

Just as in the recalled GDPR-based derogations, however, national legislations need to assure that appropriate conditions and safeguards for the processing are enacted and respected. The effective restraints to processing activities regarding sensitive data will largely depend on how burdensome the derogations and correspondent safeguards defined at national level will be.[150]

In light of these derogations to the mentioned principles and rights, the data protection regimes for research purposes under Articles 9(2)(i)–(j) GDPR appear to undercut data subjects' control prerogatives over their sensitive data and, with that, to shift the control over the data processed for research purposes onto data controllers. As can be seen from Table 2 below, the derogations to data subjects' rights under Chapter III are always possible for processing activities conducted for public health purposes. This suggests the controller-oriented nature of these data protection regimes, to be placed at the opposite edge in a descriptive spectrum with respect to the data subject-oriented regime for research under Article 9(2)(a) GDPR and its subjective control rationales.

In light of the recalled derogations, the research-based data protection regimes under Articles 9(2)(i)–(j) GDPR, mitigate ordinary data controllers' regulatory burdens so as to enhance the free-flow of sensitive data for research and innovation objectives. However, this de-regulatory stance over the processing for research purposes regards only ordinary data protection requirements and should be compensated by the requirement to establish safeguards that are appropriate to the protection of data subjects' fundamental rights and freedoms as required under Articles 89(1) GDPR. It is thus time to delve more in these safeguards.

[150]Paul Quinn, *The Anonymisation of Research Data- a Pyric Victory for Privacy that Should not be Pushed Too Hard by the EU Data Protection Framework?*, 24 Eur. J. Health L. 1 (2016).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

Table 2. The Data Protection Derogations for Research under the GDPR

	Art. 9(2) a GDPR consent	Art. 9(2) i GDPR Public health	Art. 9(2) j GDPR Research
Art. 5(1) e GDPR	●	●	●
Art. 5(1) b GDPR	●	●	●
Art. 17(3) c GDPR		●	●
Art. 17(3) d GDPR		●	●
Art. 14(5) b GDPR		●	●
Art 15 GDPR (national law under art. 89(2) GDPR)			
Art. 16 GDPR (national law under art. 89(2) GDPR)		●	●
Art. 18 GDPR (national law under art. 89(2) GDPR)			
Art. 21 GDPR (national law under art. 89(2) GDPR)		●	●
Art. 12-22 GDPR (national law under art. 23(1) e GDPR)		●	●

V. The Data Protection Rules for Research: The Safeguards

While medical research is being fueled by the exchange of scientific information and the resulting cooperation among different stakeholders of both the private and the public sector, the development of adequate data protection enhancing techniques is essential for creating the needed trust for data integration and aggregation practices. This is directly acknowledged by both Article 89(1) GDPR, requiring the enactment of "appropriate safeguards" in the form of "technical and organizational measures" and Article 9(2)(j) GDPR requiring the performance of "suitable and specific measures" for safeguarding data subjects' fundamental rights and freedoms.

The mentioned requirements of "*suitable and specific*" measures or "*appropriate* safeguards" reflect the legislator's intention to set onto data controllers the choice to decide on a case-by-case basis—and thus considering the research projects' peculiarities—which are the safeguards that best protect data subjects' rights without impairing the objectives of the processing activities. This is why the Regulation does not list the safeguards that need to be enacted in the context of research activities, but rather takes a dynamic approach so as to maximize their effectiveness in the highly varied data-driven research environment. Article 89(1) GDPR asks data controllers

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

to identify and properly implement the safeguards for the protection of data subjects' and patients' fundamental rights.

In accordance with the layered research data regimes, a fundamental criterion for assessing the appropriateness and suitability of the safeguards to be enacted by the controller is related to the invasiveness of the derogations mentioned in the previous paragraph: This means that the more a controller leverages on the derogations the Regulation or Member States laws allow, the tighter the safeguards to be enacted should be.

Accordingly, from an opposite perspective, the enactment of these safeguards should be read as a direct precondition for the enjoyment of the derogations outlined above. As a result, the research-based regime concretely applicable to processing activities variously carried out for research purposes is the result of a double fine-tuning process, in accordance with which the more derogations the controller avails himself, the stricter the safeguards that she will enact should be. Such interpretation is directly suggested by the guidance offered by Article 89 GDPR, which, firstly stresses that "technical and organizational measures" shall ensure "in particular ... the principle of data minimization." It does not rule out the other principles not already limited by Article 5 GDPR, but it clearly indicates that data minimization is not negotiable for the reasons we stressed before. Secondly, it sets a cryptic obligation and indication to use "further processing which does not permit or no longer permits the identification of data subjects ..."—anonymous data—if the purposes of processing can be fulfilled with these data. This is in line with Article 2 GDPR and referral 26 GDPR as well as with Article 6(4) GDPR at least as a safeguard for further processing. Note, however, that such a notion can be fine-tuned for the interest of the data controller as well by pairing the choice of selecting processing modalities which do not require identification. Under Article 11 GDPR, indeed, if the controller is able to demonstrate that it is not in a position to identify the data subject, and upon informing the data subject, if possible, Articles 15–20 GDPR shall not apply—except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification. For example, separating permanently a pseudonymized dataset from the dataset of the corresponding identifiers can easily fulfil this anonymity safeguard discharging the data controller by several burdens. Thirdly, in the alternative, it suggests implementing pseudonymization techniques, stating that the employment of such technique is encouraged "as long as (the research purposes) can be fulfilled in this manner." Additionally, it imposes a principle of segregation of data processing since derogations are strictly connected to research purposes and cannot spillover other data processing purposes.[151] Finally, it links all the "appropriate safeguards ... for the rights and freedoms of the data subject" to the overall architecture of the regulation: "in accordance with this Regulation." This statement at the beginning of Article 89 is not without consequences because in line with the principle of accountability with greater technical discretion for the data controllers comes greater responsibilities and the burden to prove that the selected technical and organizational measures are appropriate. *De facto*, Article 89 GDPR offers both instructions and rules setting a roadmap for data controllers.

In light of this clarification, further relevant "technical and organizational measures" can be derived from the general provisions of the General Data Protection Regulation, as the ones regarding data protection impact assessments under Article 35 GDPR. For the purposes of such assessments, the potential derogations to data subjects' rights even when they satisfy the strict requirements of Article 89(2) GDPR, which states "in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes," clearly flag a potential high risk for rights and freedoms due to their limitation. Thus, the preliminary analysis whether a data processing requires a DPIA pursuant to Article 35 GDPR might be more demanding and should certainly

[151]Council Regulation 2016/679, *supra* note 1, at art. 89(4).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

take into account the derogations and safeguards. Yet, this is routine under the GDPR framework and does not add further burdens.

Another relevant safeguard could be related to the employment of data protection certification mechanisms as seals or marks, if developed by Member States, the supervisory authorities, the Board, and the Commission in accordance with Article 42 GDPR. As the same provision underlines, these seals and marks would be relevant for showing controllers' compliance in processing operations with technical standards and thus with GDPR. Similarly, data protection measures by design and by default under Article 25 GDPR would structurally internalize and assure compliance to data protection law[152] and require taking in proper consideration the peculiarities of the research purposes and derogations.

With specific reference to health-related data, Article 9(4) para GDPR allows Member States to establish "further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health." This means that national laws can establish specific safeguards required for the protection of data subjects' interests in the context of health research projects. Once again, delegating national legislators does not help a uniform regulatory landscape and opens to a sort of rush to the bottom among Member States as in the fragmented American system. Nevertheless, the bottom line remains the GDPR itself ensuring appropriate safeguards and limiting the risk of a race to the bottom.

Overall, the mentioned system of safeguards for the processing of data for research purposes is directly aimed at conforming the goals of research data flows to the protection of data subjects' rights and freedoms, as potentially impaired by the loss of control over the processed information resulting from the derogations to some of data subjects' rights. Yet, once a systemic reading of the GDPR is in place, the mechanisms designed do not reveal to be burdensome for data controllers wile facilitating the free flow of data.

VI. The Interaction Between Differential Data Protection Regimes

As the above analysis has shown, processing activities for research purposes can be based on different lawful bases under the GDPR and are subject, irrespective of the chosen lawful basis, to the outlined research exception shaped by the mentioned derogations and the additional obligations to enact relevant safeguards borne by controllers.

Against this backdrop, a first question arises related to the interaction between the exceptional data protection regime regarding processing operations carried out for research purposes, based on any of the above-outlined legitimate bases, and the "ordinary" data protection regime applicable to processing activities conducted for non-research related but purely commercial purposes, as profiling operations and decisions regarding data subjects. Suggestions regarding the borderlines between the two different regulatory regimes can be drawn from recital 162 GDPR, which states the prohibition of processing data collected for statistical purposes "in support of measures or decisions regarding any particular natural person."[153]

[152]*See also Study of Science Forensic Unit (STOA) Panel for the Future of Science and Technology on How the General Data Protection Regulation Changes the Rules for Scientific Research* 34 (July 24, 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf.

[153]In this regard, some clarifications have been provided by the Article 29 Data Protection Working Party that has identified some examples in which companies carry out processing activities over personal data, without finalising them to individual decisions regarding natural persons. *See, e.g.,* Art. 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 7 (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (stating that, for example, a business may wish to "classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusions about an individual. In this case the purpose is not assessing individual characteristics and is therefore not profiling").

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

The stated prohibition, as read in consistency with the principle of segregation described above under Article 89(1) GDPR, can be extensively applied in case processing activities for research purposes result into further, "secondary" commercial-oriented processing, deriving from the "practical" economic employment of the statistical models designed and constructed in the context of research projects.[154] In other words, general models developed for research or statistical purposes should not be used for singling out individuals. Thus, the derogatory data protection regime for research would not apply. The example given by recital 162 GDPR regarding statistical data thus beautifully illustrates the idea of segregation of research results from their non-research use. In this respect, the key factor is keeping the research promises of "statistical confidentiality" as a counterpart to processing personal data necessary "for the production of statistical results." After all, it just echoes the basics of processing data for statistical purposes. As recital 162 GDPR illustrates, further research uses would be allowed while further non-research-oriented ones—that are those used "in support of measures or decisions regarding any particular natural person"—would not, unless consent is given.

In addition, the recalled principles enshrined in both Article 89(1) GDPR and recital 162 GDPR can provide precious guidance in order to set further boundaries among different research activities.

As the Italian cases involving Tiziana Life Sciences illustrate, processing activities of health data can be extremely complex and be related to different types of research, in terms of different research entities potentially taking part to established research projects, and of the possibilities of secondary uses of employed health datasets to radically different research projects in terms of scope and aim. Although both the administrative and the judicial decisions have been given under the Italian data protection legal framework preceding the European reform, both the decisions are interesting for the purposes of the interpretation of the subsequent framework under the General Data Protection Regulation.

More precisely, the mentioned cases well highlight the uncertainties on the applicability of the research exception regime in case of processing activities carried out for research purposes by a third-party recipient of a research-valuable dataset. These uncertainties relate directly to:

1) The applicability of the presumption of compatibility pursuant to Article 5(1) (b) or the need to assess compatibility according to Article 6(4) and eventually acquire a new consent with the related information duties as it occurs in the case of mergers codified under Article 14 GDPR;
2) The applicability of the more favorable provision under Article 9(2)(j) GDPR. As has been recalled, following the default compatibility rule set out under Articles 6(4) and 5(1)(b) GDPR, if the secondary processing is conducted for research purposes, controllers do not have to seek anew consent from data subjects but would still need to provide information pursuant to Article 14 GDPR, as long as the provision of such information does not prove impossible or requires a "disproportionate effort."[155]
3) The possibility to withdraw consent since under Article 7(2) GDPR it is always possible. The question thus arises regarding whether after withdrawal of consent by data subjects the legal basis on research is still eligible. The second decision by the Italian data protection authority seems to suggest a negative answer to this question. Conversely, the European Data Protection Board's Opinion on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, has stated that "the withdrawal of consent does not affect the processing operations that are based on other lawful grounds."[156] The European Commission, on its side,

[154]In this regard, a controller would need to have a different legal basis, such as consent or a task in the public interest, in order to employ a statistical model designed under the statistical research exemption. *See also* Wachter & Mittelstadt, *supra* note 29, at 66.

[155]Council Regulation 2016/679, *supra* note 1, at art. 14(5)(b).

[156]European Data Protection Board, *supra* note 93, at 4.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

has suggested that the compatibility analysis for secondary uses of data is never allowed when the original legal basis is consent.[157]

The choice to apply one or the other data protection regime, will largely depend on the definition of the scope of the specific research purpose. Thus, it will depend on whether the mentioned compatibility rule applies also to a different third-party organization, carrying out private and for-profit oriented research activities—as the one carried out by a company as Tiziana—in the form of different research projects that are not strictly related to the research projects for which the health data were originally collected.[158]

According to the broad interpretation of research under recital 159 GDPR, the decision of the Tribunal of Cagliari would be more adherent to the newly established, controller-friendly, research-based data protection framework,[159] as based either on specific, sectoral blanket consents, as the ones described above, or on Articles 9(2)(i) or 9(2)(j) GDPR as legitimate bases alternative to the one of consent. In this perspective, both decisions by the Italian Data Protection Authority suggest the practical opportunity to handle different types of research differently.

The EDPB itself has underlined that in the data protection regime for research "the rules contain a special regime affording a degree of flexibility for genuine research projects that operate within an ethical framework and aim to grow society's collective knowledge and wellbeing"[160] and alludes to the difficulty "to distinguish research with generalizable benefits for society from that which primarily serves private interests." A borderline difficult to trace. In the Tiziana cases genetic research could clearly benefit mankind but the fact that for-profit research could be performed by processing personal data that were collected explicitly for non-profit research purposes, casted and casts doubts on whether the presumption of compatibility would stand the test of Article 5(2)(b), Article 6(4), and Article 7.

To address these persisting interpretative doubts, the next paragraph will propose a framework that differentiates data protection regimes within the research-based regime as shaped in the black letters of the General Data Protection Regulation. This framework is primarily based on the distinction between for profit and public interest-based research.

As the last section will demonstrate, there is direct correspondence between loss of control and free flow of personal information objectives only in this last case. Conversely, when private or public data are processed for commercial-oriented research purposes, the loss of subjective control over processed data needs to be compensated with safeguards for the protection of data subjects' fundamental rights and freedoms, which come to restrain research data flows.

F. Shaping Differential Data Protection Research Regimes

Our analysis has illustrated that the intertwining of flexibilities and derogations the GDPR offers for research leaves open to interpretation several instances.[161] As anticipated, this also occurs under the new Open Data Directive, which has extended the scope of data re-use, however leaves to Member States the ultimate definition of the access regimes. Against this backdrop, however, a clear limit to eventual arbitrary decisions by data controllers in the data research domain is clearly established, according to the European Data Protection

[157]*Can We Use Data For Another Purpose?*, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en#:~:text=References-,Answer,compatible%20with%20the%20original%20purpose.

[158]Leaving the interpretative question open, see Dove, *supra* note 92, at 1025.

[159]*See generally* Marco Bassini, *Il nuovo regolamento generale sulla protezione dei dati personali e il settore farmaceutico*, *in* Giuseppe F. Ferrari, Osservatorio del Farmaco 109 (2019).

[160]European Data Protection Supervisor, A Preliminary Opinion on Data Protection and Scientific Research 18 (Jan. 6, 2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[161]*Id.*

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

Supervisor (EDPS),[162] by the impossibility of disowning the "essence of the (fundamental) right to data protection." This means that the derogations provided by the special regime cannot be abused by data controllers acting for research purposes. To sanction this need, the EDPS suggests a highly restrictive interpretation of the research-based regime.[163]

Nevertheless, and following such a cautious interpretative approach, a possible restraint to the creeping abusive application of the differential data protection regime for research can be found in the distinction between public interest and commercial-oriented research.

In the previous paragraphs it has been shown that under recital 159 GDPR, the GDPR's notion of research encompasses both public and privately funded research differently from other normative definitions of research, even within the EU, as the one enshrined in the new Copyright Directive. Under the latter, following a subjective approach to research, the distinction between these two types of research causes the application of the ordinary regulatory regime to privately funded "research" activities, and of the special regulatory regime only to public funded-research activities.[164] On the other side of the Atlantic, the CCPA adopts a rather objective approach, excluding from the scope of the research exception those processing activities that are linked to commercial research purposes.[165]

At a closer examination, however, it appears that within the same recital 159 GDPR a differentiation between public interest and commercial research is also envisaged. Indeed, the same letter of the recital sets the ground for a free flow of research data within the EU through the reference to Article 179(1) TFEU, but it also highlights both the peculiar link between research that might require "the publication or otherwise disclosure of personal data in the context of scientific research purposes" and the need to adapt the application of the GDPR to the implications of scientific research "in the interest of the data subject," "in particular in the health context." The chosen examples relate to the public interest to verify scientific results allowing the repeatability of scientific experiments or the verification of data provenance, on the one hand, and, on the other the benefits of scientific research for the data subject as well.

The beneficial effect of research investigations resulting from the sharing of data has been explicitly acknowledged by the European Commission's Strategy for data, which highlights the relevance for the achievement of society's well-being of the employment of public sector information by private entities; government-to-business-G2B-data sharing; the sharing and use of privately-held data by other companies; business-to-business-B2B-data sharing; as well as the use of privately-held data by government authorities; government-to-business-G2B-data sharing.

In consistency with these statements, the recently proposed Data Governance Act considers also privately-funded research as pursuing "a purpose of general interest."[166] In this respect the Act establishes a registration mechanism for legal entities, also of private nature, which are willing to make available datasets for purposes of general interest. As it states, "the voluntary compliance of such registered entities with a set of requirements should bring trust that the data made available on *altruistic purposes* is serving a general interest purpose."[167] However, the legal entities willing to be registered as "Data Altruism Organizations recognized in the Union" must be not-for-profit[168] and must share their data "without seeking a reward."[169] In light of these declarations the Data Governance Act appears to shape a notion of "altruistic" research that is already implicitly provided by recital 159 GDPR,

[162] *Id.*

[163] *Id.* at 22.

[164] *See* Giancarlo Frosio, Christoph Geiger & Oleksandr Bulayenko, *Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/EU*, *in* PROPIEDAD INTELECTUAL Y MERCADO ÚNICO DIGITAL EUROPEO, 27–71 (Begoña González Otero & Julián López Richart eds.2019).

[165] Price, Kaminski, Minssen & Spector-Bagdady, supra note 59, at 450.

[166] *Proposal for Data Governance Act*, *supra* note 18, at recital 35.

[167] *Id.* at recital 36 (emphasis added).

[168] *Id.*

[169] *Id.* at art. 2(10).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

promoted by private legal entities with a not-for-profit character and that engage in jointly conducted research activities without targeting economic returns.

A similar approach has been welcomed also by the European Data Protection Board's Guidelines on "the processing of data concerning health for the purpose of scientific research in the context of the Covid-19 outbreak," where it is observed how also private entities can play a role in pursuing public interest, especially in an extraordinary situation, such as the pandemic, where it is suggested that the collaboration between private entities and public institutions can be essential for a faster production of results.[170]

These statements are highly interesting also for the purposes of interpreting the notion of research within the GDPR. Indeed, while the already recalled specification within recital 159 GDPR "and privately funded research" clearly sustain the extension of the research exception to private motivated/funded research, it also signals a possible differentiation of regimes echoed as well in the need to take into consideration "reasons for further measures in the interest of the data subject." For example, in the case of research for orphan diseases, it clearly "gives reason for further measures in the interest of the data subject," indicating that their interests are served better by the sharing of data. Thus, the fact that "the general rules of this Regulation should apply in view of those measures" shows in turn that the GDPR regime could be softened, as in the differential research-data regimes we described.

Seeds of a taxonomy thus are appearing, distinguishing among various combinations of interests including public, private, and for profit-oriented research, and primarily related to research with advantages to the general public, with further advantages for data subjects, and research mostly profit-oriented. Pharmaceutical research, for instance, is indirectly beneficial to the data subject and society at large but mostly motivated by profit. Its balance tips towards public interest in cases when it "is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health" for example during a pandemic or "ensuring high standards of quality and safety of health care and of medicinal products or medical devices."[171]

Thus, the differential regimes for research data, while do not differentiate among private and public funding, clearly differentiate in terms of the more "egoistic" or "altruistic" aim of the research. The subjective perspective regarding the private or public nature of the funding, and thus the private or public nature of the entities conducting research, appears to be quite irrelevant since it can well be the case that also privately funded research serves broader public interest goals, as it can occur with the research and development of a vaccine or with the special derogations and aids offered for orphan drugs.

Conversely, the objective perspective highlighting that the public interest and commercial-based research activities are linked is highly informative. In this respect, as recital 159 GDPR seems to propose, the boundary is to be drawn between those research enquiries whose results also benefit data subjects and research that, as acknowledged under the CCPA, mainly serve controllers' economic interests. However differently from the CCPA, the "broad interpretation" of the notion of research recalled by the same recital 159 GDPR appears also to suggest encompassing this latter type of research in the research-based data protection regime.

Against this backdrop, we propose to employ such distinction for the purposes of scaling the flexibilities or "privileges"—as the Data Ethics Commission defines them—of the special research-based data protection regime. As has been illustrated above, these flexibilities are directly given by the national definitions of the derogations and the data controllers' choice about needed safeguards.

Under these premises, a restrictive interpretative approach as the one required by the European Data Protection Supervisor suggests the opportunity to modulate these flexibilities differently with

[170]European Data Protection Board, Guidelines 03/2020 on the Processing of Data Concerning Health for the Purposes of Scientific Research in the Context of the Covid-19 Outbreak para. 64 (Apr. 21, 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

[171]Council Regulation 2016/679, *supra* note 1, at art. 9(2)(i).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

respect to public interest-oriented, or altruistic, research and profit-driven one, regardless of the sources of their funding. Such modulation should thus be primarily rooted in the principles of proportionality and fairness, which assures the protection of data subjects from controllers' and processors' abuse, by preventing disproportionate harms stemming from the power asymmetries that characterize the technology-driven processing environment, and in particular the research processing environment.

The said principle suggests tempering the flexibilities existing under the research-based regime in accordance with data subjects' interests and reasonable expectations. Indeed, referral 159 GDPR clearly illustrate it in the domain of orphan drugs where the research output "gives reason for further measures in the interest of the data subject" and requires reading accordingly the GDPR.

From this perspective, data subjects' control rationales and free flow of information goals are the parameters upon which the taxonomy is based. Control rationales suggest that both the derogations and the safeguards required under the research-based regime should thus be respectively restricted to the minimum and stretched to the highest when it comes to merely commercial-oriented research data processing. Conversely, public interest-oriented research activities could enjoy a more enabling regulatory regime, designed around deeper derogations, if needed, defined at national level, and less burdensome safeguards, helping the flows of research data.

The three prongs unfolding of the research regime based on Consent,[172] Public interest,[173] and Research,[174]reflects clearly in the interplay between data pools and their eventual swinging from one regime to the other.

G. Applying the Spectrum of Differential Data Protection Regimes to Data Pools

I. From Public Interest Research to For Profit-Oriented Research

The exploitation of private or public data pools by businesses for profit-oriented research, as the one conducted by Tiziana Life Science Corporation in the aforementioned ruling, may pose higher risks for the protection of data subjects' rights and freedoms, including to any form of moral objection and overture to specific kinds or goals for the research itself, including data philanthropy. In the Tiziana case, many citizens consensually volunteered to pursuing data-philanthropy aims that might lead the transfer for further use to fail the test under Article 6(4) GDPR. Such assessment is to be primarily conducted in accordance with a risk-based evaluation required by the same Regulation under the data protection impact assessment. Accordingly, the principles of proportionality and necessity—first of all—would require processing activities conducted for for-profit research purposes to rely on the legitimate basis that is more respectful of data subjects' interests and rights, that is consent. Consent and the related possibility of its withdrawal structurally assures a higher degree of control, also if it is related only to certain research areas as suggested by recital 33 GDPR. In addition to this, taking into account the safeguards for the essence of the fundamental right to data protection, consent allows for a negotiation around the willful conferment of personal data. The effectiveness of such control is mitigated by the presumption of compatibility under Article 6(4) and 5(1)(b) GDPR, enabling further processing for research purposes. Exactly in the view of the necessity of data subjects' stronger control prerogatives, the same mentioned principles advocate a strict interpretation of such compatibility rules, to restrict the further flows of research data to the realm of data subjects' self-informational determinations, and to what is proportionate for the prevention of greater risks to the same data subjects. In other words, changing the context[175] from merely altruistic goals to also for-profit ones might lead to failing the compatibility test.

[172] *Id.* at arts. 6(1)(a), 9(2)(a).
[173] *Id.* at arts. 6(1)(e), 9(2)(i), 9(2)(g).
[174] *Id.* at arts. 6(1)(e), 9(2)(j), 89.
[175] *Id.* at art. 6(4)(f).

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

Note, however, that it is not a clear-cut solution. Indeed, if genetic data under the Tiziana cases were made "manifestly made public by the data subject" without limitations, the further use would be clearly permissible. Similarly, if the informed consent had a scope compatible with the further use or a sufficiently large–although specific as required by the GDPR–blanket consent was acquired.

In the same vein of setting parameters for the research "privileges," also, the derogation to the principle of storage limitation under Article 5(1)(e) GDPR should be restricted to the storage that is strictly necessary to the performance of the specific research project and not be stretched for other purposes. According to a similar perspective, the possibility to derogate to the information duty under Article 14(5)(b) GDPR should also be restrained by applying a higher standard of impossibility or "disproportionate effort" of providing information by the controller. What is disproportionate for public interest research might not be for profitable interests.

Conversely, research for profit can also benefit from the derogations if appropriate safeguards are provided, for instance, selecting "processing which does not require identification.[176] Equally, the derogations to ordinary data protection rights could be circumscribed to the sole derogations directly allowed by the Regulation and not be aggravated by Member States laws.

This interpretative possibility is to be directly drawn from Article 89(4) GDPR establishing a principle of segregation: privileges only apply to research purposes and do not extend to other purposes. A striking example can be offered by research for marketing and the use of the research outputs for marketing. While personal data processing for scientific studies on marketing would enjoy the research privileges, the use of the same data for purely marketing purposes would not in consistency with the principle of segregation as illustrated also by recital 162 GDPR stressing that the results of statistical purposes processing operations should not be used "in support of measures or decisions regarding any particular natural person."

It remains unclear if the same proportionality and necessity principles guide a more severe interpretation of when, in the case of commercial-oriented research, the actioning of data subjects' rights would "render impossible or seriously impair the achievement" of set research objectives, as required by Article 89(2) GDPR.

On the side of the safeguards required under Article 89(1) GDPR, the same principles of proportionality, fairness and segregation suggest the enactment of higher context-sensitive safeguards for preventing research processing activities to result into the processing of health data for pure, non research-based, commercial purposes. Such processing is indeed prohibited under Article 9(1) GDPR, unless the data subject gives explicit and specific consent for these purposes as required under Article 9(2)(a) GDPR. This suggests a higher threshold of "appropriateness" of the safeguards to be employed under Article 89 GDPR with respect to private or public health data pools employed for commercial-oriented research. More precisely, the safeguards should be appropriate whenever these prevent uses of data that would not be acceptable for the data subjects. A higher appropriateness threshold regarding the safeguards to be enacted would thus feed confidence and trust in privately conducted health research, otherwise impaired by the weakening of individual control over treated health data.

In terms of the requirements under Article 89(1) GDPR, this requires a close scrutiny of the:

1) adherence to the principle of data minimization;
2) requirement to use anonymized data for the purposes of the research activities; or if this is not possible to use pseudonymization techniques;
3) respect to the principle of data segregation;
4) principle of accountability as generally supporting the whole system of data protection safeguards.

[176] *Id.* at art. 11.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

A more precise identification of relevant safeguards can be defined in consideration of the possible harms stemming from a processing operation. In case of processing activities that are likely to result in a high risk to the rights and freedoms of natural persons, these harms are to be identified by the controllers' data protection impact assessment under Article 35 GDPR. Harms stemming from the processing of private data pools can be related to the data subjects' moral suffering related to the disclosure of sensitive health conditions, stigmatizations, and the generation of stereotypes regarding certain groups in the health sector and beyond. Moreover, the processing of data for the purposes of for-profit research easily results into purely commercial activities, as monitoring and marketing by third parties, also potentially triggering profiling activities, which are formally prohibited under Article 22 GDPR. Processing activities of sensitive data conducted for research purposes may thus engender heavy intrusions in data subjects' personal lives, to be accurately addressed through the establishment of adherent safeguards.

II. Keeping Public Interest Research on the Go

A different standard of data protection emerges for public interest-oriented research. Both private and public research organizations can potentially be involved in public interest-oriented research activities. Examples of public interest-oriented research areas can be found in Article 9(2)(i) GDPR, listing the protection against serious cross-borders threats to health, the accomplishment of high standards of quality and safety of health care and of medicinal products or medical devices. Additional suggestions with respect to public interest-related sectors can be found in recital 54 GDPR, further referring to "morbidity and disability," "the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality." Research related to these sectors is thus certainly to be considered of public interest-oriented nature, disregarding the public or private nature of its funding. Here a simple example can be research related to post-market surveillance where private, for-profit, and public interest walk hand in hand.

Note however, that national implementations of the GDPR have offered a more stringent test. For instance, the UK Data Protection Act 2018 establishes that the processing will only meet the requirement under the research exception for a basis in UK law if the processing not only is conducted for research purposes and is carried out in accordance with Article 89(1) GDPR, that is the enactment of adequate safeguards, but is also conducted in the public interest.[177] This public interest requirement applies to any research processing of health data reliant upon the research exception, whether carried out by private or public bodies. The public interest is envisaged under UK law whenever there is a trade-off between the individual interests in data protection and the benefits of research, which justifies the fact that the data subjects who are individually affected have a reason to accept those interferences. This is exactly the case of research in the interest of the data subject, mentioned by recital 159 GDPR.

Conversely, in the absence of such a trade-off, personal interferences are not acceptable if not grafted in an express consent of the data subject, exceptionally allowing an interference in their personal sphere. As anticipated, following this same logic, recital 162 GDPR regarding the processing of personal data for statistical purposes suggests that the results of these processing operations should not be used "in support of measures or decisions regarding any particular natural person."

Against this backdrop, the acceptability of the processing of sensitive data is to be defined on the basis of a proportionate balance between the reasons for protection of data subjects' fundamental rights and other fundamental rights, such as the right to health, promoted by research activities over health data.

[177]UK Data Protection Act 2018, § 10(2), sch. 1, part 4.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

This acceptability criterion could justify research activities in a legitimate basis that is more controller-oriented as the one under Article 9(2)(j) GDPR. This appears exactly to be acknowledged by Article 110 of the Italian data protection law, which states that processing activities for research purposes do not require data subjects' consent if the research activities that are carried out are defined on the basis of Union or national laws as required under Article 9(2)(j) GDPR, or in case the retrieval of consent would make the achievement of research objectives impossible or otherwise impair them seriously. The Italian provision thus well reflects how with respect to processing for research purposes, the principles of necessity and proportionality allow a detachment from individual control rights.

In the same perspective, exactly the public interest nature of research activities could justify the possibility to interpret the default compatibility rule under Articles 5(1)(b) and 6(4) GDPR in a broader manner when it comes to the further processing of data for public interest-oriented research purposes; and the storage of employed data for longer periods taking advantage of the flexibilities under Article 5(1)(e) GDPR.

Likewise, acceptability of research activities from the data subjects' perspective could sustain the derogation to information duties under Article 14(5)(b) GDPR even when safeguards would not trigger the application of Article 11 GDPR. Such derogation would be directly motivated upon the impossibility or "disproportionate effort" for the data controller to provide to data subjects relevant information, while accommodating individual and collective fundamental rights, as it occurs in the case of public health emergencies.

Based on the same reasoning, compliance with the other data subjects' rights under Chapter III GDPR would be more likely to "render impossible or seriously impair the achievement" of public interest research objectives, thus justifying derogations under Member State laws as allowed under Article 89(2) GDPR.

With respect to this type of research, control rationales may be less stringent in accordance with a risk-based evaluation as the one conducted through the data protection impact assessment. Conversely, free flow of research data goals may gain priority, with the recalled limit provided under recital 162 GDPR. This may justify lower burdens for data controllers with respect to the safeguards under Article 89 GDPR, which would need to be modulated in consistency with the public-oriented nature of the enacted research activities. This means that in case of public interest-oriented purposes of the research, as the development of a vaccine, the safeguards could be restrained to the minimum normative requirements, to what is necessary to fuel data subjects' confidence that the data is used only in a manner that is acceptable for the community.

As a regular test, the public oriented nature of the research indicates that the driving public interest benefits of a given data processing clearly outweigh the risks to the fundamental right to data protection and does not crashes its essence while for-profit reasons do not weigh in. In this perspective, public interest-targeted research should surely imply controllers' observance of the general data protection principles recalled by Article 89(1) GDPR, expressly referring to "safeguards in accordance with this Regulation." As occurs for commercial-based research, the principle of accountability is central also for public interest-oriented research to ensure the essence of personal data protection is not hindered. Processing activities for public interest research purposes should thus also comply with the minimum standard set by Article 89(1) GDPR, particularly regarding the principle of data minimization and the enactment of data pseudonymization techniques.

III. Mixing Interests in Private-Public Research

With respect to mixed private-public health datasets employed for research purposes, the data protection research regime should be calibrated based on the influence that commercial undertakings have within established research partnerships or organizations. The degree of influence of

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

these entities indeed determines the risk of commercial "capture" of research results, especially when for-profit interests weigh in.

The involvement of for-profit organizations and thus their influence in the governance of research projects and results can be derived from specific parameters. In this respect, the Copyright Directive mentions some parameters that can be relevant also for the purposes of data protection. In particular, recital 12 of the Directive refers the influence by commercial-oriented organizations in research activities to "structural situations" as a qualified shareholder control or the presence of specific members of for-profit organizations in the management of research projects. These structural situations may engender a direct control by these organizations over research infrastructures and thus over initiated research patterns. As the recital suggests, these structural situations may in turn favor a preferential access to the results of the research by for profit organizations. Note also that such preferential access would be dealt with in separate agreements.

In the event a "decisive influence" of for-profit organizations over the established research partnership or organization exists, safeguards should be as strict as in the case of a fully for-profit conducted research. Conversely, in case the control of the research endeavors over mixed private-public datasets primarily resides onto the public entity, the identified mentioned data protection flexibilities could be exploited to the maximum.

However, under the GDPR, it is not who funds the research that matters, but its scope. The reason why this is so and why it is a better solution can be clarified by an example. Using the dichotomy under the Copyright Directive could prove to be difficult with respect to private-public partnerships established for grounds of public health protection, as is occurring in the fight against the Coronavirus pandemic. For instance, in the collaboration between private and public actors, as in the "Innovative Medicines Initiative," based on a public-private partnership between the European Commission and the pharmaceutical industry,[178] it might trigger the enactment of higher data protection safeguards and lower derogations from the ordinary regime, merely because of the presence of commercial-oriented stakeholders. Nonetheless, purposes of public health protection, and the need of immediate research actions, could conversely suggest a relaxation of data protection checkpoints. In the specific cases where mixed health data pools are employed for research purposes in the public interest in the area of public health, such as for the protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, the higher level of restrictions on the processing of special categories of personal data can be relaxed, in accordance with what is required for the processing for public interest purposes under Article 9(2)(j) GDPR, disregarding the public or private nature of the subjects involved.[179]

H. Conclusion

This study has identified three "differential" data protection regimes for research entailed in the General Data Protection Regulation, given by a data subject-centered regime; a public interest-oriented regime and a general research-based regime. It has demonstrated how the European data protection framework provides the interpretative criteria for the distinction between a for profit research-based data protection regime and a public interest research-based data protection regime providing effective tools to manage it and to leverage private-public partnerships and data sharing with a fluid movement from one differential regime to the other.

The variations between these data protection regimes are rooted in the GDPR's double fine-tuning system based on the balancing among coded data protection principles and rules and the establishment of *ad hoc* safeguards for the protection of data subjects' rights and freedoms by data

[178] *See* IMI-Innovative Medicines Initiative, https://www.imi.europa.eu/.

[179] This interpretation is also suggested by Hintze, *supra* note 23, at 134.

https://doi.org/10.1017/glj.2022.30 Published online by Cambridge University Press

controllers. It has been indeed demonstrated how moving along the spectrum of the differential data protection regimes the greater the loss of individual control is, the greater the shift of burden of protection onto data controllers is in terms of additional safeguards required under Article 89(1) GDPR accompanied by a wider autonomy in selecting the safeguards in line with the specifics of the research processing needs.

We theorized a similar scaling with respect to differential research-based regimes, to level an asymmetrical flow between for profit and public interest research regimes. This means that in case of for-profit research activities data subjects are entitled to a greater control over occurring processing operations due to a fuller application of data protection principles and rights and a more severe layer of safeguards that controllers need to enact; conversely, in case of public interest-based research possible derogations can be exploited with greater ease by data controllers, which can establish lighter additional safeguards.

Against a generally favorable set of regimes for processing personal data for research, the double fine-tuning data protection system under the European framework has the effect of limiting the application of higher protection standards to be followed by data controllers to data sharing practices for merely commercial-oriented research. To the contrary, in case of public interest-based research, data protection regimes facilitate the free flow of personal information and the interrelated sharing activities.

Overall, the study has shown how the European data protection law provides a highly sophisticated regulation of data processing activities for research purposes, balancing sharing and innovation goals with the high level of protection for data subjects' fundamental rights it purports fine tuning research privileges and individual rights privileges scaling them in various ways.

We argue that the sensitivity of the European data protection regulatory model could inspire the developments of U.S. data protection regulations for research purposes since it offers a pro-research set of differential regimes able to foster data flow without hampering the essence of the fundamental right to personal data protection. A much-needed solution after the final collapse of the Privacy Shield.

Cite this article: Comandè G, Schneider G (2022). Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. *German Law Journal* **23**, 559–596. https://doi.org/10.1017/glj.2022.30