

DOI 10.5817/MUJLT2024-1-1

ALTERNATIVE LEGAL BASES FOR PROCESSING HEALTH DATA FOR SCIENTIFIC RESEARCH PURPOSES

by

ROXANNE MEILAK BORG * MIREILLE MARTINE
CARUANA †

The processing of health data for scientific research purposes requires a legal basis under Article 6 and a justification under Article 9 (2) GDPR by way of an exception to the general prohibition in Art. 9(1) of the processing of special category data. Consent tends to be highly advocated for in this regard, in both literature and practice. However, the GDPR permits an alternative option: processing for scientific research purposes based on Union or Member State law which provides for suitable and specific safeguarding measures. This paper undertakes an in-depth examination of the 'research exception' in Art. 9 (2) (j) GDPR permitting the processing of health data for scientific research purposes, thoroughly considering its elements and its implications. It refers to examples of Member State implementing legislation and the proposed European Health Data Space Regulation for illustration purposes and argues that if implemented faithfully, Art. 9 (2) (j) strikes a better balance between the interests of the various stakeholders than consent, which is overall burdensome and may hinder research. Finally, in light of the uneven implementation of the GDPR's research exception by the Member States which creates considerable legal uncertainties and results in barriers to the free flow of research data across the EU, this paper calls for a harmonised implementing Union law in this regard.

* Roxanne Meilak Borg LL.B. (Melit.), LL.D. (Melit.), M.A. (Melit.), is a Research Assistant at the Department of Media, Communications and Technology Law within the Faculty of Laws and former Data Protection Officer of the University of Malta. For correspondence: roxanne.meilak@um.edu.mt.

† Mireille M Caruana, B.A., LL.D. (Melit.), LL.M. (Lond.), Ph.D. (Bristol), is Senior Lecturer and Head of the Department of Media, Communications and Technology Law within the Faculty of Laws at the University of Malta. For correspondence: mireille.caruana@um.edu.mt

KEY WORDS

Health Data, Scientific Research Purposes, General Data Protection Regulation (GDPR), European Health Data Space (EHDS) Regulation.

1. INTRODUCTION

The impact of scientific research on health data is far-reaching: it may result in better individual diagnosis and treatment and may lead to better management of future diseases and improved healthcare services. Within the EU, research on health data constitutes a processing operation under the General Data Protection Regulation (“GDPR”)¹ and must conform with such Regulation as well as with any additional national data protection laws Member States may have in place. The GDPR appears to take the rights and interests of the relevant stakeholders – including the research community – into account. It incorporates the term “processing for scientific research purposes” in Recitals and substantive provisions² and affirms that “scientific research” should be understood broadly to include “for example technological development and demonstration, fundamental research, applied research and privately funded research.”³

As a data processing operation, scientific research on health data requires a legal basis under Art. 6 GDPR and, since it involves data that are sensitive in nature and fall under a special category listed in Art. 9 (1) - which also prohibits the processing of such data - it must be justified under an Art. 9 (2) provision. Art. 6 does not provide a specific legal basis for data processing for scientific research, but Art. 9 (2) (j) includes the so-called “research exception” - an exception to the general prohibition of the processing of special category data where the processing is for scientific research purposes.

Currently, however, there is no widespread application of Art. 9 (2) (j). It is consent - included as both a legal basis in Art. 6⁴ and a possible exception in Art. 9 (2)⁵ - that tends to be not only advocated for in academic literature, but also, the preferred option in practice.⁶ This could

¹ Regulation (EU) 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 (General Data Protection Regulation). Official Journal of the European Union (2016/L-119/1) 4 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

² *Ibid.*, Recitals 33,156-57,159; Arts. 5 (1) (b) and (e), 9 (2) (j), 89.

³ *Ibid.*, Recital 156.

⁴ *Ibid.*, Art. 6 (1) (a).

⁵ *Ibid.*, Art. 9 (2) (a).

⁶ See Dove, E. S. and Chen, J. (2020) Should consent for data processing be privileged in health research? A comparative analysis. *International Data Privacy Law*, 10 (2), p. 119; Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. *Life*

be because it appears to afford data subjects greater control over their data,⁷ or because in practice research participants are generally still required to give their consent for ethical purposes.⁸ Be it as it may, consent as a legal basis is overall burdensome, does not necessarily result in the most comprehensive protection for research participants, and restricts researchers' flexibility, thereby hindering research.

This paper undertakes an in-depth examination of the Art. 9 (2) research exception in order to assess its legal and practical suitability as an alternative to consent. Thus, it aims to answer the following research question: Should we move away from consent in the context of data-driven research, and focus instead on effectively operationalising the Art. 9 (2) research exemption?

The paper begins by contemplating various reasons why consent is unsuitable as a legal basis and/or Art. 9 (2) exception for the processing of health data for scientific research purposes. It then considers the elements of Art. 9 (2) (j), focusing on its interplay with Article 89 (1) GDPR and the requirement of adopting "suitable and specific" safeguarding measures. It draws on the experience of selected EU MS to exemplify State practice in this respect, referring to provisions of Austrian, Belgian, Estonian, Finnish, German, Irish and Polish laws in light of such countries' geographical distribution and different legislative approaches, as well of the laws of the authors' home country of Malta. As Chapter 4 shows, the relevant national laws are disparate, and the implementation of safeguards within national legal frameworks fragmented. The views and practices of national DPAs are not considered in this review.

Next, the paper engages in a brief analysis of two specific pieces of legislation in light of the Art. 9 (2) (j) requirements. It identifies the Irish

Sciences, Society and Policy, 16 (1), p. 6; Manis, M. (2017) The processing of personal data in the context of scientific research. The new regime under the EU-GDPR. *BioLaw Journal - Rivista di BioDiritto*, 3, p. 337; Quinn, P. (2021) Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society and Policy*, 17 (4), pp. 6, 8, 29.

⁷ See Comandè, G. and 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, pp. 573-574.

⁸ In terms, for instance, of the: World Medical Association, *Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects*, June 1964. Available from: <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/> [Accessed 29 December 2023]; and the World Medical Association, *Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks*, October 2022. Available from <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/> [Accessed 29 December 2023].

Health Research Regulation (“HRR”)⁹ as a solid example of a comprehensive national law setting out such requirements (despite its shortcoming, in the authors’ view, of reintroducing consent as a mandatory requirement), and considers the proposed European Health Data Space (“EHDS”) Regulation¹⁰ in view of its status as a topical and upcoming EU-wide law.

This paper does not purport to discuss appropriate alternative legal bases to consent under Art. 6 GDPR for the concerned processing; nonetheless, a brief discussion in this respect is warranted since it would be senseless to opt for an alternative exception under Art. 9 (2) without concurrently opting for an alternative legal basis under Art. 6. Scientific research is often carried out by public or publicly-funded entities; although Art. 6 does not include a specific legal basis for “scientific research purposes,” it does provide one for public authorities/organisations. Thus, this paper briefly considers the relevance and interplay of such provision (Art. 6 (1) (e)) with and for Art. 9 (2) (j), as well as for research that is carried out by private entities in the public interest, at the end of Chapter 6.

The analysis shows that the GDPR offers the normative flexibility to accommodate solutions to any potential hindrance to research posed by data protection legislation, even if disparate national laws currently fall short of fully implementing the research exception. The paper argues that with proper implementation, the GDPR’s research exception could strike a better balance between the various interests involved while also enabling the free flow of research data across the EU, resulting in the establishment of a true European research area. It thus calls for a shift towards a widespread application of Art. 9 (2) (j), in particular through a harmonised EU law implementing this provision.

2. UNSUITABILITY OF CONSENT AS A LEGAL BASIS

Consent is one of the most well-known, and advocated for,¹¹ possible legal bases under Art. 6 and exceptions under Art. 9 for data processing for scientific research purposes,¹² despite repeated assertions by EU data protection authorities that basing such data processing on consent may not

⁹ Promulgated under the Irish Data Protection Act 2018 (No. 7 of 2018). Available from <https://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf> [Accessed 29 December 2023].

¹⁰ Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, (COM/2022/197 final) 3 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197> [Accessed 29 December 2023].

¹¹ Dove, E. S. and Chen, J. (2020), *op. cit.*

¹² Quinn, P. (2021) Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society and Policy*, 17 (4), pp. 6, 8.

be advisable.¹³ In addition, there are many reasons why it is not a *suitable* option.

2.1. BURDENSOME TO OBTAIN; CAN BE WITHDRAWN

The GDPR sets a high threshold for consent as a legal basis for data processing. It is burdensome, in fact, to obtain consent in a manner that fulfils all the GDPR's requirements, since the GDPR requires consent to be "freely given", "specific", "informed" and an "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."¹⁴ Furthermore, data subjects must be given the opportunity to withdraw their consent at any point,¹⁵ and once withdrawn, all processing based on such consent must be halted.

2.2. DIFFICULT TO IMPLEMENT IN CERTAIN CIRCUMSTANCES

It is harder to fulfil the GDPR's consent requirements where data to be used for research are obtained from third parties and not directly from research participants, as for instance in the case of a researcher wishing to carry out research on patient data originally collected and held by a medical institution for healthcare purposes. In such a scenario, it is impractical and perhaps even impossible for the researcher to seek each patient's consent in a manner that complies with the GDPR.

Consent is also problematic where data are collected and stored, usually in bio- or similar "data" banks, for generic and/or future research purposes. The requirement of specificity is not met here because the research purposes are often unknown at the time of data collection. Biobanking refers to the establishment of a research database consisting of genetic samples and extracted genetic data which is of increasing importance for innovative data-driven research, and, as has been argued, requires more flexible consent

¹³ See European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, Adopted on 6 January 2020. Available from: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en [Accessed 29 December 2023], p. 20; and EDPB, 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)), Adopted on 23 January 2019. Available from: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en [Accessed 29 December 2023].

¹⁴ *Ibid.*, Art. 4 (11).

¹⁵ *Ibid.*, Art. 7 (3).

options.¹⁶ The notion of “open” or “broad” consent - whereby research participants give general consent to their data being used in future research - is particularly advocated for in this regard. The GDPR attempted to take such scenarios into consideration¹⁷ and some MS have even chosen to reflect the concept of broad consent in their national laws: for instance, the notion is incorporated in Austria’s Research Organisation Act¹⁸ and Ireland’s HRR.¹⁹ Still, EU data protection authorities have asserted that such consent is not tantamount to, or even likely to fall under, the GDPR notion of consent,²⁰ so its applicability to the present context remains uncertain.

2.3. IMBALANCE BETWEEN THE PARTIES INVOLVED

Consent is not a valid legal basis where there is an imbalance between the controller and the data subjects, as such dynamics would likely negate the element of freely-given consent.²¹ Public authorities are generally precluded from relying on consent as a legal basis²² and employers are also discouraged from basing the processing of their employees’ data on consent, since employees would likely be constrained or feel pressured to consent for fear of detrimental effects at work.²³ In the same way, individuals receiving medical treatment might feel “obliged” to consent to their health data being used for research purposes if they believed that declining could negatively affect their treatment or medical care. In fact, the Clinical Trials Regulation (“CTR”)²⁴ already imposes an obligation on clinical trials investigators to

¹⁶ Hallinan, D. and Friedewald, M. (2015) Open consent, biobanking and data protection law: can open consent be “informed” under the forthcoming data protection regulation? *Life Sciences, Society and Policy*, 11 (1), p. 3.

¹⁷ By virtue of Recital 23. See also Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sciences, Society and Policy*, 16 (1).

¹⁸ See Art. 2 (d) (3). Available from <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514> [Accessed 29 December 2023].

¹⁹ HRR, *op. cit.* Reg. 3 (1) (e).

²⁰ See Art. 29 DP WP, Guidelines on consent under Regulation 2016/679, Revised and Adopted on 10 April 2018 (17/EN, WP 259 rev.01) Available from: <https://ec.europa.eu/newsroom/article29/items/623051/en> [Accessed 29 December 2023]; and European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/678, Adopted on 4 May 2020 (Version 1.1) Available from: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en [Accessed 29 December 2023].

²¹ *Ibid.*, p. 6.

²² Recital 43 GDPR.

²³ Art. 29 DP WP, *op. cit.*, p. 6.

²⁴ Regulation (EU) No 536 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. *Official Journal of the European Union* (2014/L-158/1) 27 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0536> [Accessed 29 December 2023].

carefully assess participants’ circumstances to ensure that their consent is freely given and they are not inappropriately influenced to take part.²⁵ Thus it is likely that consent for the processing of health data for scientific research purposes would also not fulfil the “freely-given” criterion.

2.4. CONFLATION WITH ETHICAL CONSENT

Finally, it is important to recall that consent as a GDPR legal basis for data processing is not the same as “informed consent” for ethical purposes as envisaged by international instruments such as the WMA Helsinki Declaration.²⁶ “Ethical” consent is sought from individuals to ensure they are willing to participate in the concerned research, as a matter of respecting the individual’s human dignity and self-determination.²⁷ In contrast, consent for the processing of data for scientific research purposes is a possible and non-exclusive legal basis provided for by the GDPR.

Ethical consent should not be confused or conflated with GDPR consent, and as a general rule, can and should not be done away with. On the other hand, there is no legal requirement to base data processing for scientific research on consent, particularly since the GDPR provides alternative options under both Arts. 6 and 9. Thus, where a controller opts for consent for data processing, consent as a legal basis for processing and that requested for ethical purposes overlap and may prove confusing for research participants.²⁸ While this does not in itself render GDPR consent unsuitable as a legal basis, it adds to the complexity of collecting such consent in a manner that complies with the GDPR, particularly in terms of ensuring that such consent is truly properly “informed.”

3. RESEARCH EXCEPTION UNDER ARTICLE 9

3.1. ART. 9 (2) (J)

Art. 9 (1) GDPR prohibits the processing of data classified as “special category” unless an exception is provided in Art. 9 (2); Art. 9 (2) (j) sets out

²⁵ EDPB, 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)), Adopted on 23 January 2019. Available from: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en [Accessed 29 December 2023].

²⁶ WMA, *op. cit.* For discussion on the main components of ethical consent see United Nations General Assembly, Right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Adopted on 10 August 2009. Available from: <https://www.refworld.org/pdfid/4aa762e30.pdf>[Accessed 29 December 2023].

²⁷ WMA, *op. cit.*

²⁸ Dove, E. S. and Chen, J. (2020) Should consent for data processing be privileged in health research? A comparative analysis. *International Data Privacy Law*, 10 (2), p. 128.

a specific exception for the processing of special category data for research purposes, stating that the prohibition set forth in para. (1) shall not apply:

... where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Art. 9 (2) (j) is long-winded and convoluted²⁹ and sets out conditions that need to be fulfilled where it is to be relied on as a justification for the processing of special category data. It requires the concerned processing to be (i) necessary for scientific research purposes; (ii) in accordance with Art. 89 (1); and (iii) based on Union or MS law.

There is no guidance elsewhere in the GDPR or at EU level on how this provision should be interpreted or implemented. Linguistically, it is somewhat unclear whether it is the concerned processing or the requisite Union or Member State law that must be proportionate, respect the essence of the right to data protection and provide for suitable and specific safeguarding measures.³⁰ Kuner, Bygrave and Docksey³¹ and Comandè and Schneider³² take the former view. The authors of the present contribution favour the interpretation that the requisite Union or MS law should authorise the data processing for scientific research purposes and set out the scope of these purposes in a manner that is proportionate and respectful of data protection rights. Such a law would thus not only explicitly identify “suitable and specific” safeguarding measures for the concerned processing, but also provide a broader context for the concerned processing. Notably, there is currently no EU law implementing Art. 9 (2) (j).

3.2. ARTICLE 89(1)

Art. 89 (1), cross-referred to in Art. 9 (2) (j), requires processing for scientific research purposes to be:

²⁹ Ducato, R. (2020) Data protection, scientific research and the role of information. *Computer Law & Security Review*, 37, p. 5.

³⁰ The Italian version of Art. 9(2)(j) GDPR could be said to support the first interpretation; the English version could be read in both ways, and the French and Maltese versions appear to leave no doubt that the second interpretation is the correct one. The examination of other language versions is limited to the languages known to the authors. Ideally, all the other language versions would also be examined in order to reach a reliable conclusion and perhaps gain more insight into the legislator’s intention.

³¹ Kuner, C., Bygrave L. A., Docksey, C. and Drechsler, L. (eds.) *The EU General Data Protection Regulation (GDPR), A Commentary*. New York: Oxford University Press, p. 381.

³² See (n 6) p. 580.

...subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. These safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

By way of context, Art. 89 (1) applies to the processing of *all* personal data (not just special category data) for scientific research purposes. It is a substantive provision within the GDPR, which as a Regulation is directly applicable in the Member States. As such, Art. 89 (1) does not require implementation into, nor indeed need to be reflected within, national laws. There is nonetheless some debate regarding whether the “appropriate safeguards” it calls for should be listed in national law, and whether the provision imposes an obligation on Member States in this regard or whether it is researchers as controllers who must implement safeguarding measures.³³ Furthermore, there is no guidance in the GDPR or otherwise at EU level about what the “appropriate safeguards” should be.³⁴

3.3. THE INTERPLAY BETWEEN ART. 9 (2) (J) AND ART. 89 (1)

The reference to Art. 89 (1) and its corresponding obligations in Art. 9 (2) (j) appears to complicate matters, since both provisions set out a respective requirement pertaining to safeguarding measures. Furthermore, whilst it is clear that the “suitable and specific measures” required by Art. 9 (2) (j) must be provided for in Union or MS law, it remains unclear whether Art. 89 (1) “appropriate safeguards” should also be listed in law. This dissonance was even acknowledged during the GDPR’s legislative process, in the form of an observation to such effect put forth by the Belgian delegation,³⁵ which appears to have not been taken into consideration since the relevant text remained unchanged.

³³ Milieu Consulting SRL, Study on the appropriate safeguards under article 89 (1) GDPR for the processing of personal data for scientific research, Adopted in August 2021 (EDPS/2019/02-08) Available from: https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-appropriate-safeguards-under_en [Accessed 29 December 2023] p. 9.

³⁴ See Kuner et al. *op. cit.*

³⁵ See Council of the European Union, Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States, 9 October 2019 (12756/1/19, REV 1) Available from: <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf> [Accessed 29 December 2023] p. 4.

Nonetheless, despite any possible confusion, and although they may appear at face value as an undue repetition, the obligations set forth in Arts. 9 (2) (j) and 89 (1) are distinct and likely apply cumulatively where Art. 9 (2) (j) is relied on for the processing of special category data for research purposes.³⁶

It is not hard to understand the legislator's line of reasoning in respect of the obligation to have "suitable and specific" safeguarding measures for the processing referred to in Art. 9 (2) (j). Such an obligation laid out in law offers "added" protection to data subjects' rights and interests, particularly since the processing is not based on their consent. It also reflects the general practice of affording greater protection to special category data processed for research purposes.³⁷ On the other hand, one could question why there is mention of Art. 89 (1) in Art. 9 (2) (j) at all, if the former already separately establishes an overarching obligation in respect of all data processing for research purposes. A possible explanation could be that the reference to Art. 89 (1) is intended here as a reminder of the importance of adequately protecting the concerned data subjects. The cumulative application of Art. 89 (1), then, may be considered as a safety net of sorts, that provides a two-tier level of protection irrespective of what Member States choose to enact in any law setting out the "suitable and specific measures" required by Art. 9 (2) (j). However, this explanation still does not clarify what either set of measures should or could entail; nor the difference, if any, in practice, between them; nor indeed exactly what they are intended to protect, since they refer respectively to "the fundamental rights and the interests of the data subject"³⁸ and "the rights and freedoms of the data subject."³⁹

4. IDENTIFYING SAFEGUARDING MEASURES

4.1. APPROPRIATE SAFEGUARDS

The terms "suitable and specific measures" set out in Art. 9 (2) (j) and "appropriate safeguards" set out in Art. 89 (1) are both legacy terms inherited from the GDPR's predecessor, the Data Protection Directive. Neither term is defined in the GDPR; nor as stated above, is the difference between them. Furthermore, to date no comprehensive guidelines with specific examples of such measures have been proffered,⁴⁰ even though the Art. 29 WP called for a definition for the term "safeguards" in as early as 2011, advocating for the provision of *examples* of such, and itself mentioning data security, specific

³⁶ See Ducato (2020), *op. cit.*, p. 5; Comandè, G. and Schneider, G. (2022), *op. cit.*, p. 580.

³⁷ Milieu Consulting SRL, *op. cit.*, p. 51.

³⁸ GDPR, Art. 9 (2) (j).

³⁹ GDPR, Art. 89 (1).

⁴⁰ EDPS (2020), *op. cit.*, p. 5.

notification and permit requirements in this regard.⁴¹ Art. 89 (1) also proffers some, albeit extremely limited, insight into what “appropriate safeguards” could be, since it requires “technical and organisational measures” that “ensure respect for the principle of data minimisation” and identifies by way of a non-exhaustive example the specific measure of pseudonymisation. However, guidance at EU level is limited to the above two instances, and the task of identifying and implementing appropriate safeguarding measures is left in the hands of the Member States and/or the controllers and processors engaged in the processing.

Academic literature has attempted to shed light on the matter. Some authors suggest that to choose and implement appropriate safeguards, inspiration should be drawn from principles already enshrined in the GDPR, such as proportionality, data security and data minimisation.⁴² Other authors recommend looking to international instruments, including ones governing ethics, for further direction. Staunton et al⁴³ considered texts such as the Council of Europe Convention for the protection of individuals with regards to the automatic processing of individual data⁴⁴ and the UNESCO Universal Declaration on Bioethics and Human Rights⁴⁵ to identify possible safeguards that could also fulfil the requirements of Art. 89 (1), ultimately recommending six possible standards: “consent that is appropriately governed; independent review and oversight; accountable processes; clear and transparent policies; adoption of security measures; and training and education of all those involved in the use and re-use of personal data in research.”⁴⁶

An analysis of existing “appropriate safeguards” in selected EEA States identified commonly implemented measures including pseudonymisation and anonymisation, risk assessments, data protection impact assessments (“DPIAs”), rules regarding access to and the physical handling of data, oversight by ethics committees and involvement of national data protection

⁴¹ Art. 29 DP WP, Advice paper on special categories of data (“sensitive data”), Adopted on 20 April 2011 (Ref. Ares(2011)444105) Available from: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [Accessed 29 December 2023] p. 11.

⁴² See Kuner et al (2021), *op. cit.*, p. 381.

⁴³ Staunton et al. (2022) Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research. *Frontiers in Genetics*, 13, p. 9.

⁴⁴ Of 28 January 1981 (ETS 108) Available from: <https://www.refworld.org/docid/3dde1005a.html> [Accessed 29 December 2023].

⁴⁵ Of 19 October 2005. Available from: <https://en.unesco.org/about-us/legal-affairs/universal-declaration-bioethics-and-human-rights> [Accessed 29 December 2023].

⁴⁶ Staunton et al (2022), *op. cit.*, p. 9.

authorities.⁴⁷ Further insight into appropriate safeguarding measures is provided by the proposed EHDS Regulation, which refers to “establishing the safeguards for processing, in terms of lawful purposes, trusted governance for providing access to health data (through health data access bodies) and processing in a secure environment, as well as modalities for data processing, set out in the data permit.”⁴⁸

The status quo in Member States has however been described as a “patchwork of safeguards.”⁴⁹ Although common measures may be applied across the EU, this is not done in a homogenous manner, particularly since there is currently no obligation of uniformity at EU level.

4.2. MEMBER STATE APPROACHES

Member States have thus tended to take unique and fragmented approaches towards adopting and implementing safeguards within their national legal frameworks. This section exemplifies how measures such as anonymisation and pseudonymisation and DPIAs, that are commonly acknowledged and resorted to as safeguards for data processing for research purposes, are implemented differently in different Member States.

4.2.1 Anonymisation and pseudonymisation

Anonymisation and pseudonymisation are both long-established safeguarding measures in the field of research, with pseudonymisation affirmed as “one of the safeguards most relevant to health sector research.”⁵⁰ They are generally prevalent in data protection legislation, and have even been incorporated in the proposed EHDS Regulation.⁵¹ Often, the use of anonymised data for research purposes is presented as the preferred default position, and the use of pseudonymised data permitted where it is not possible to achieve the purposes of the processing with anonymous data.

A case in point, the Belgian Data Protection Act⁵² dictates as a general rule that anonymous data must be used for research purposes. The controller is nonetheless permitted to use pseudonymised data “if it is

⁴⁷ Milieu Consulting SRL, *op. cit.*

⁴⁸ EHDS, *op. cit.*, Recital 37.

⁴⁹ Milieu Consulting SRL, *op. cit.*, p. 5.

⁵⁰ DG Food and Health Safety (2021) *Assessment of the EU Member States' rules on health data in the light of GDPR*. Luxembourg: Publications Office of the European Union. Available from: https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en [Accessed 29 December 2023] p. 61.

⁵¹ EHDS, *op. cit.*, Art. 44.

⁵² Adopted on 30 July 2018. Available from: <https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf> [Accessed 29 December 2023].

not possible to achieve the research by processing anonymous data” and “non-pseudonymised data” “if it is not possible to achieve the research or statistical purpose by processing pseudonymised data.”⁵³ Belgian law also identifies specific circumstances under which data processed for research purposes must be anonymised or pseudonymised.⁵⁴ For instance, data to be used for research must be anonymised or pseudonymised once they have been collected from the data subjects,⁵⁵ when they shall be used for further processing⁵⁶ and when they shall be shared with one or more additional controllers for further processing.⁵⁷

The Maltese DPA takes a similar, albeit less rigid, stance. Mirroring Art. 89 (1) GDPR, it imposes pseudonymisation as an overarching obligation in respect of data processing for research purposes, but requires that where such purposes “can be fulfilled by processing which does not permit, or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.”⁵⁸ The Irish DPA sets out an obligation for “suitable and specific measures [to be] taken to safeguard the fundamental rights and freedoms of data subjects’ where data are to be processed for research purposes.⁵⁹ It does not require the use of pseudonymised data in research; it merely lists this as a possible “suitable and safeguarding measure.”⁶⁰ It too provides that processing shall be fulfilled in a manner which does not permit, or no longer permits, identification of data subjects if it is still possible to achieve the purposes in this manner.⁶¹

This waterfall system has also been reflected in the proposed EHDS Regulation. Art. 44, governing the sharing of electronic health data, follows the principles of data minimisation and purpose limitation. As a first step it permits the relevant authority (the “health data access body”), to provide requested health data “in an anonymised format;”⁶² where “the purpose of the data user’s processing cannot be achieved with anonymised data” such data may be provided in “pseudonymised format.”⁶³

⁵³ *Ibid.*, Art. 197.

⁵⁴ *Ibid.*, Arts. 198-204.

⁵⁵ *Ibid.*, Art. 198.

⁵⁶ *Ibid.*, Art. 199.

⁵⁷ *Ibid.*, Art. 201.

⁵⁸ Data Protection Act, Chapter 586, Laws of Malta. Available from: <https://legislation.mt/Legislation> [Accessed 29 December 2023] Art. 6 (4).

⁵⁹ Data Protection Act 2018, Act Number 7 of 2018. Available from: <https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html> [Accessed 29 December 2023] Art. 42.

⁶⁰ *Ibid.*, Art. 36 (1) (iv).

⁶¹ *Ibid.*, Art. 42 (3).

⁶² EHDS (2023), Art. 44 (2).

⁶³ *Ibid.*, Art. 44 (3).

Some MS laws furthermore require pseudonymised data to be anonymised as soon as the research allows and/or once the purposes of the processing have been fulfilled.⁶⁴ Notably, however, not all MS laws require data to be used for research to be anonymised. For instance, Estonian law merely establishes an obligation to process data for scientific purposes “in a pseudonymised format”⁶⁵ and the Finnish Data Protection Act calls for pseudonymisation of data only where the processing of special category data is concerned.⁶⁶

4.2.2 DPIAs

The GDPR explicitly mandates a DPIA in cases where the processing is likely to result in a high risk to the rights and freedoms of natural persons.⁶⁷ It identifies general circumstances where DPIAs are mandatory, such as in the case of “processing on a large scale of special categories of data”⁶⁸ but fails to provide concrete examples of such scenarios, leaving it to the relevant controllers to determine whether or not a DPIA is mandatory in respect of their particular processing operations. Further guidance in this regard has been proffered by the Art. 29 WP;⁶⁹ nonetheless, apart from establishing that the “storage for archiving purposes of pseudonymised personal data concerning vulnerable data subjects of research projects or clinical trials” requires a DPIA,⁷⁰ these guidelines do not specifically address scientific research or research on health data.

⁶⁴ See in this regard: Austrian Data Protection Act. Available from: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597&FassungVom=2018-05-25> [Accessed 29 December 2023] Section 7 (5); Irish HRR (2018), *op. cit.*, Reg. 3 (1) (c) (vii); German BDSG. Available from: https://www.gesetze-im-internet.de/englisch_bds_g/englisch_bds_g.html [Accessed 29 December 2023] Section 27 (3); Malta Subsidiary Legislation 528.10. Available from <https://legislation.mt/Legislation> [Accessed 29 December 2023] Reg. 4; Polish Act on Higher Education and Science. Available from: <https://www.gov.pl/attachment/d6975935-4b24-4be3-96f1-09c51589958a> [Accessed 29 December 2023] Art. 469b (4).

⁶⁵ Author’s translation. Data Protection Act. Available from: <https://www.riigiteataja.ee/en/eli/523012019001/consolide> [Accessed 29 December 2023] Section 6 (1).

⁶⁶ (1050/2018) Available from: <https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf> [Accessed 29 December 2023] Section 6.

⁶⁷ *Ibid.*, Art. 35.

⁶⁸ *Ibid.*, Art. 35 (3) (b).

⁶⁹ Art. 29 DP WP, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, Revised and Adopted on 4 October 2017 (17/EN, WP 248 rev.01) Available from: <https://ec.europa.eu/newsroom/article29/items/611236/en> [Accessed 29 December 2023] pp. 9-12.

⁷⁰ *Ibid.*, p. 11.

Despite both the overarching obligation for all controllers and processors to conduct a DPIA where this is mandated under Art. 35 GDPR, and the fact that scientific research is not highlighted as requiring a DPIA by the relevant authorities, some of the Member States whose laws were reviewed for this article chose to include a specific obligation, in their national laws, to conduct such an assessment in respect of processing activities for the purpose of scientific research; particularly where this is conducted on special category data.

Belgium, Finland and Ireland all require a DPIA where health data are to be processed for research purposes. Belgian law mandates a DPIA for the processing of all special category data for scientific purposes unless there is a code of conduct in place;⁷¹ Finland mandates a DPIA where special categories of data are to be processed for research purposes if data subjects' rights are to be derogated from in terms of the same law.⁷² In the latter case, the DPIA must be sent to the Data Protection Ombudsman before processing begins. Ireland requires an assessment to be made in respect of the concerned health research, and where such an assessment indicates a "high risk to the rights and freedoms of individuals", requires a DPIA.⁷³

Thus, while Member States have incorporated the same notions and measures discussed above into their national data protection legislative frameworks, they have done so to different extents, in relation to different categories of data and in respect of different circumstances.

5. WAY FORWARD

5.1. LAWS IMPLEMENTING ART. 9 (2) (J)

The measures considered in the previous section likely not only qualify as "appropriate safeguards" within the meaning of Art. 89 (1), but also fulfil the requirements of "suitable and specific measures" required by Art. 9 (2) (j) if and when they are provided for in a law that sets out the scope and purposes of processing of special category data for research purposes. The suitability of any such measures in the context of Art. 9 (2) (j) will depend more on their being tailor-made to the specific research context (e.g. research carried out in the context of a bio- or other "data" bank) than on their inclusion in any pre-established set of measures. Therefore, the focus of any discussion on Art. 9 (2) (j) should be the specific law it calls for. In order to elucidate this point, it is helpful to consider two pertinent pieces of legislation in light

⁷¹ See EHDS (2022), Sections 191, 187.

⁷² See Estonian Data Protection Act, *op. cit.*, Section 31.

⁷³ HRR, *op. cit.*, Reg. 3 (1) (c) (i) and (ii).

of the Art. 9 (2) (j) requirements: the Irish HRR⁷⁴ and the proposed EHDS Regulation.⁷⁵

5.1.1 Irish Health Research Regulations

The Irish HRR govern the processing of personal data for “the purposes of health research,” requiring controllers who are processing data for such purposes to take a number of “suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject.”⁷⁶ Notably, this law not only spells out a list of safeguarding measures, but also sets out the scope of its application by defining the concept of “health research.”⁷⁷

The HRR thus establish safeguarding measures for a specific context, in relation to particular processing operations and defined purposes. Although the wording of Reg. 3 (1) is not exactly the same as that of Art. 9 (2) (j),⁷⁸ and the HRR do not specifically state that they are intended to implement Art. 9 (2) (j), the structure of the law and the rules it sets out may be said to correspond to the Art. 9 (2) (j) criteria. Nonetheless, it is not without its limitations: while in theory the HRR present an opportunity for controllers to opt for a legal basis other than consent for data processing for health research purposes, they re-introduce the GDPR notion of “explicit consent” as an obligatory safeguard.⁷⁹ Thus, in practice, controllers still need to seek data subjects’ consent for their research activities. Moreover, it appears that the HRR will apply irrespective of the Art. 9 (2) exception chosen by controllers for the relevant processing.

5.1.2 EHDS Regulation

The proposed EHDS Regulation aspires towards a European “space” for electronic health data and mechanisms by which such data may be requested for various specific purposes, including for scientific research. It thus aims to make electronic health data more readily-available across the EU and to establish a “governance framework” for the access and use of such data for predetermined purposes.⁸⁰ In fact, in its substantive provisions, the EHDS sets out the relevant categories of data, the purposes for which they may

⁷⁴ HRR, *op. cit.*

⁷⁵ EHDS, *op. cit.*

⁷⁶ HRR, *op. cit.*, Reg. 3 (1).

⁷⁷ *Ibid.*, Reg. 3 (2).

⁷⁸ The former speaks of safeguarding the “fundamental rights and freedoms of the data subject” and the latter of safeguarding the “fundamental rights and *interests* of the data subject.”

⁷⁹ HRR, *op. cit.*, Reg. 3 (1) (e).

⁸⁰ EHDS (2022), *op. cit.*, Art. 1 (1).

be processed, and requisite safeguards.⁸¹ In contrast with the HRR, it also explicitly states that it is intended to form a legal basis “in accordance with Art. 9 (2) (g) (h) (i) and (j) GDPR,” albeit in a non-binding recital.

It remains unclear, however, which purposes listed under Art. 34 specifically correspond to Art. 9 (2) (j). Furthermore, controllers intending to access electronic health data in pseudonymised format under the EHDS must themselves determine an appropriate legal basis under Art. 6 GDPR and reflect this in their request for a data permit.⁸² However, there is no parallel requirement to reflect the exception availed of under Art. 9 (2) in a data permit request. The proposed Regulation has in fact been criticized for its lack of clarity by both the EDPB and the EDPS,⁸³ and it remains to be seen how it will be applied in practice if adopted in its current form.

5.2. CODES OF CONDUCT

Against a background of divergent MS laws and practices pertaining to data processing for scientific research purposes, a harmonised EU law implementing Art. 9(2)(j) is not currently envisaged. As discussed, the EHDS itself does not deliver sufficient clarity regarding the use of health data for scientific research purposes. Furthermore, national laws implementing Art. 9 (2) (j) may provide legal certainty for entities operating solely within a concerned Member State’s territory, but do little to encourage or enable seamless data flows across the EU and the ERA.

The GDPR presents a possible solution to this too, by permitting the drawing up of Codes of Conduct which may then be approved by the relevant supervisory authority or EDPB.⁸⁴ Such Codes are perceived as useful tools for lawful collaboration and data sharing across the EU.⁸⁵ Nevertheless, developing such a Code intended to bridge existing gaps between Member States is neither a straightforward nor a fast process.⁸⁶ Various Codes relating to health research have been proposed following the entry into force of

⁸¹ *Ibid.*, Arts. 33 and 34.

⁸² *Ibid.*, Art. 45 (4).

⁸³ EDPB and EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, Adopted on 12 July 2022. Available from: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en [Accessed 29 December 2023] p. 23 paras. 87-90.

⁸⁴ Art. 40.

⁸⁵ EDPS, p. 25. See also: Krekora-Zajac, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on GDPR art.40. *Frontiers in Genetics*, 12, p. 2.

⁸⁶ Krekora-Zajac, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on GDPR art.40. *Frontiers in Genetics*, 12, p. 3.

the GDPR, but thus far, these are either a work in progress,⁸⁷ have not been formally approved,⁸⁸ or are still awaiting approval from the relevant authority.⁸⁹

5.3. LEGAL BASIS UNDER ART. 6 GDPR

It is an established principle that controllers who have identified an exception under Art. 9 (2) for the processing of prohibited special category data, must still also have a legal basis under Art. 6 for the concerned processing.⁹⁰ It is not the aim of this paper to discuss all possibilities under Art. 6, however, the authors note that the most appropriate legal basis under this provision will differ depending on the type of entity that is carrying out the research - whether it is a public or private organisation - and the nature or purpose of the research.

Scientific research is often carried out by public or publicly-funded organisations and in the public interest. Thus, such entities could on the basis of their public nature rely on the widely-accepted legal basis for public authorities in the first limb of Art. 6 (1) (e), which permits data processing “for the performance of a task carried out in the public interest,” in lieu of consent. The authors believe that a private entity could also - in principle - rely on this provision if and when the concerned research is in the public interest. Private entities would naturally need to justify why they are opting for this provision as opposed to Art. 6 (1) (f) and demonstrate the inherent public interest in

⁸⁷ BBMRI-ERIC’s “Code of Conduct for Health Research.” Further information available from: <https://code-of-conduct-for-health-research.eu/> [Accessed 28 December 2023].

⁸⁸ Coreon’s Code of Conduct for Health Research. Available from: <https://www.coreon.org/wp-content/uploads/2023/06/Code-of-Conduct-for-Health-Research-2022.pdf> [Accessed 29 December 2023].

⁸⁹ EUCROF’s Code of Conduct for Service Providers in Clinical Research. Further information available from: https://www.eucrof.eu/images/21_03_22_20210306_EUCROF_Code_-_Introduction_Note.pdf [Accessed 29 December 2023]; EFPIA’s Code of Conduct on Clinical Trials and Pharmacovigilance. Further information available from: <https://www.efpia.eu/news-events/the-efpia-view/statements-press-releases/efpia-statement-on-a-gdpr-code-of-conduct/> [Accessed 28 December 2023].

⁹⁰ See: Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014 (844/14/EN, WP 217) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [Accessed 29 December 2023] pp. 15-16; Donnelly, M. and MacDonaugh, M. (2019) Health, Consent and the GDPR Exemption *European Journal of Health Law*, 26, p. 101; Comandè, G. and Schneider, G. (2021) Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. *German Law Journal*, 23, p. 570; and Case C-667/21 *Krankenversicherung Nordrhein* [2023] ECLI:EU:C:2023:1022.

their research activities, and may thus find it more challenging to apply this basis in practice.⁹¹

In any case, and most importantly to the present discussion, Art. 6 (1) (e) also requires a corresponding national law that governs the relevant processing. The authors postulate that the law required by Art. 9 (2) (j) could thus serve a “double” purpose and strive to also fulfil the requirements set out in Art. 6 (1) (e). This would make it straightforward for controllers to opt for Arts. 9 (2) (j) and 6 (1) (e) when processing data for scientific research purposes.

6. CONCLUSION

Consent tends to be the most resorted to legal basis and/or exception for the processing of special category data for scientific research purposes. As this paper has shown, this is potentially problematic for researchers due to the strict consent requirements under the GDPR. Furthermore, it does not necessarily result in effective protection for concerned data subjects. The GDPR itself permits an alternative option by virtue of Art. 9 (2) (j), which requires in particular that the processing be based on a Union or national law providing for adequate protection for data subjects’ fundamental rights and interests. Thus, this provision not only alleviates researchers of the burden of having to base their processing on the legal basis of consent but, if correctly implemented, also ensures that data subjects’ rights and interests are more adequately and effectively protected than if the processing were to be based on their consent.

Art. 9 (2) (j) refers to Art. 89 (1), establishing a two-tier requirement of safeguarding measures; those required by Art. 9 (2) (j) itself, termed “suitable and specific measures” and the Art. 89 (1) “appropriate safeguards.” While there is no guidance on the difference, if any, between these two sets of measures, it is likely that in practice each set will comprise similar or even identical measures. However, those set out in Art. 89 (1) apply to the processing of all personal data (not just special category data), while the suitable and specific measures required by Art. 9 (2) (j) should be incorporated in the requisite law that also sets out the context, scope and purposes of the processing.

Since there is currently no EU law implementing Art. 9 (2) (j), Member States have taken a fragmented approach, and although there are many safeguarding measures commonly applied across the EU, these are implemented differently in each Member State. Laws implementing Art. 9 (2) (j) are thus specific to the country in which they have been adopted.

⁹¹ Quinn (2021), *op. cit.*, p. 9.

Even in the proposed EHDS Regulation, which purports to be a legal basis in accordance with Articles 9 (2) (g) - (j) GDPR for the secondary use of health data and to establish safeguards for processing, there is remaining uncertainty as to when and how it would be applicable, in practice, in respect of data processing for scientific research purposes.

National laws are helpful to provide legal certainty for entities operating within a Member State. However, they do little to facilitate data sharing as is necessary to establish and maintain a European research area free of internal barriers to the flow of research data. Codes of Conduct may aid with bridging existing differences between different Member State laws and practices. Such Codes represent a more attainable option in the immediate future than a harmonised EU law; however, although several have been proposed since the GDPR's entry into force, none have been formally adopted yet. Further research is required to explore how the law may be applied vis-a-vis upcoming technological infrastructures such as those proposed in the EHDS, how Codes of Conduct may serve to bridge the gaps in this regard and the added value AI/machine learning brings to the research health sector.

As already envisaged in the EHDS initiative, a harmonised EU law implementing Art. 9 (2) (j) is what is needed to strike a fair balance between the various stakeholder interests in the field of health research, as well as to contribute towards the free movement of personal data for research purposes within the EU.

LIST OF REFERENCES

- [1] Article 29 Data Protection Working Party, Advice paper on special categories of data ("sensitive data"), Adopted on 20 April 2011 (Ref. Ares(2011)444105) Available from: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [Accessed 29 December 2023]
- [2] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, Revised and Adopted on 10 April 2018 (17/EN, WP 259 rev.01) Available from: <https://ec.europa.eu/newsroom/article29/items/623051/en> [Accessed 29 December 2023]
- [3] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Revised and Adopted on 4 October 2017 (17/EN, WP 248 rev.01) Available from:

- <https://ec.europa.eu/newsroom/article29/items/611236/en>
[Accessed 29 December 2023]
- [4] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014 (844/14/EN, WP 217) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [Accessed 29 December 2023].
- [5] Austrian Data Protection Act. Available from: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597&FassungVom=2018-05-25> [Accessed 29 December 2023].
- [6] BBMRI-ERIC, Code of Conduct for Health Research. Further information available from: <https://code-of-conduct-for-health-research.eu/> [Accessed 28 December 2023].
- [7] Belgian GDPR Implementing Act. Available from: <https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf> [Accessed 29 December 2023].
- [8] Comandè, G. and 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.
- [9] Council of Europe Convention for the protection of personal data Of 28 January 1981 (ETS 108) Available from: <https://www.refworld.org/docid/3dde1005a.html> [Accessed 29 December 2023]. Coreon's Code of Conduct for Health Research. Available from: <https://www.coreon.org/wp-content/uploads/2023/06/Code-of-Conduct-for-Health-Research-2022.pdf> [Accessed 29 December 2023].
- [10] Council of the European Union, Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States, 9 October 2019 (12756/1/19, REV 1) Available from: <https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf> [Accessed 29 December 2023]
- [11] DG Food and Health Safety (2021) *Assessment of the EU Member States' rules on health data in the light of GDPR*. Luxembourg: Publications Office of the European Union. Available from: https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en [Accessed 29 December 2023]
- [12] Donnelly, M. and MacDonaugh, M. (2019) Health, Consent and the GDPR Exemption *European Journal of Health Law*, 26

- [13] Dove, E. S. and Chen, J. (2020) Should consent for data processing be privileged in health research? A comparative analysis. *International Data Privacy Law* 10 (2).
- [14] Ducato, R. (2020) Data protection, scientific research and the role of information. *Computer Law & Security Review*, 37
- [15] EFPIA's Code of Conduct on Clinical Trials and Pharmacovigilance. Further information available from: <https://www.efpia.eu/news-events/the-efpia-view/statements-press-releases/efpia-statement-on-a-gdpr-code-of-conduct/> [Accessed 28 December 2023].
- [16] Estonian Data Protection Act. Available from: <https://www.riigiteataja.ee/en/eli/523012019001/consolide> [Accessed 29 December 2023]
- [17] EUCROF Code of Conduct for Service Providers in Clinical Research. Further information available from: https://www.eucrof.eu/images/21_03_22_20210306_EUCROF_Code_-_Introduction_Note.pdf [Accessed 29 December 2023]
- [18] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/678, Adopted on 4 May 2020 (Version 1.1) Available from: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en [Accessed 29 December 2023].
- [19] EDPB, 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)), Adopted on 23 January 2019. Available from: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en [Accessed 29 December 2023].
- [20] EDPB and EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, Adopted on 12 July 2022. Available from: https://edpb.europa.eu/our-work-tools/our-documents/edpbbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en [Accessed 29 December 2023] p. 23 paras. 87-90.
- [21] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, Adopted on 6 January 2020. Available from: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en [Accessed 29 December 2023]

- [22] Finnish Data Protection Act (1050/2018) Available from: <https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf>[Accessed 29 December 2023]
- [23] German BDSG. Available from: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html [Accessed 29 December 2023]
- [24] Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sciences, Society and Policy*, 16 (1).
- [25] Hallinan, D. and Friedewald, M. (2015) Open consent, biobanking and data protection law: can open consent be “informed” under the forthcoming data protection regulation? *Life Sciences, Society and Policy*, 11 (1).
- [26] ICO. (2023) *Public Task*. [online] Cheshire:ICO. Available from: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/public-task/> [Accessed 29 December 2023].
- [27] Irish Data Protection Act 2018. Act Number 7 of 2018. Available from: <https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html> [Accessed 29 December 2023]
- [28] Irish Health Research Regulations. Available from: <https://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf>[Accessed 29 December 2023].
- [29] Krekora-Zajac, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on GDPR art.40. *Frontiers in Genetics*, 12
- [30] Kuner, C., Bygrave L. A., Docksey, C. and Drechsler, L. (eds.) *The EU General Data Protection Regulation (GDPR), A Commentary*. New York: Oxford University Press
- [31] Malta Subsidiary Legislation 528.10. Available from <https://legislation.mt/Legislation> [Accessed 29 December 2023]
- [32] Manis, M. (2017) The processing of personal data in the context of scientific research. The new regime under the EU-GDPR. *BioLaw Journal - Rivista di BioDiritto*, 3.
- [33] Milieu Consulting SRL, Study on the appropriate safeguards under article 89 (1) GDPR for the processing of personal data for scientific research, Adopted in August 2021 (EDPS/2019/02-08) Available from: https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-appropriate-safeguards-under_en [Accessed 29 December 2023]

- [34] Polish Act on Higher Education and Science. Available from: <https://www.gov.pl/attachment/d6975935-4b24-4be3-96f1-09c51589958a> [Accessed 29 December 2023]
- [35] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, (COM/2022/197 final) 3 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197> [Accessed 29 December 2023].
- [36] Quinn, P. (2021) Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society and Policy*, 17 (4).
- [37] Regulation (EU) No 536 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. *Official Journal of the European Union* (2014/L-158/1) 27 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0536> [Accessed 29 December 2023].
- [38] Staunton et al (2022) Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research. *Frontiers in Genetics*, 13.
- [39] UNESCO Universal Declaration on Bioethics and Human Rights Of 19 October 2005. Available from: <https://en.unesco.org/about-us/legal-affairs/universal-declaration-bioethics-and-human-rights> [Accessed 29 December 2023]
- [40] United Nations General Assembly, Right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Adopted on 10 August 2009. Available from: <https://www.refworld.org/pdfid/4aa762e30.pdf> [Accessed 29 December 2023].
- [41] World Medical Association, *Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects*, June 1964. Available from: <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/> [Accessed 29 December 2023]
- [42] World Medical Association, *Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks*, October 2022. Available from <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/> [Accessed 29 December 2023].