TILBURG UNIVERSITY

The Elephant in the Room:

Rethinking GDPR Enforcement in the Context of Genetic Data

Is Article 32 of the GDPR providing adequate protection for genetic data processing?

Master Thesis

LLM Law and Technology

Tilburg Institute for Law, Technology and Society (TILT)

July 2022

Inês Cabugueira Marques

SNR: 2075082

Thesis Supervisor: Taner Kuru

Second Reader: Dr. Paul de Hert

Table of Contents

Acknowledgements

During my studies, my interest in the field of healthcare privacy has grown considerably. Therefore, writing a thesis concerning genetic data privacy in EU law has been a pleasure, which has allowed me to deepen my knowledge in the field.

As this thesis marks the end of my education so far, I would like to thank my family for their incredible support in writing this thesis. Especially my parents, for giving me the possibility to expand my horizons and study abroad. You have been my biggest motivation and inspiration for as long as I can remember, and I could not have done this without you.

Furthermore, I would like to thank Mr Taner Kuru for providing extensive feedback and allowing me to improve throughout this process. Thank you for your guidance, especially regarding your insights and the constant challenge of my ideas. In addition, I would like to thank Dr Paul de Hert for stepping in as a second reader and providing his expertise.

Lastly, to Efe and my friends, thank you for always being there for me.

Chapter 1 | Introduction

1.1. Background

In recent years, healthcare has undergone significant technological development, from 3D printing machines able to develop new organs to evolution in remote care and telemedicine. Big data has contributed to a substantial improvement in healthcare, enabling the aggregation and analysis of various data sources, which may improve primary care in healthcare services.[1] The use of big data in healthcare was induced by the development of electronic health records (EHRs), which are typically comprehensive (containing records of clinical encounters with patients' healthcare providers) and can be viewed by anyone with access to them.[2]

In turn, EHRs led to the widespread storing and sharing of genomic data contained in these records.[3] For instance, a physician in an emergency department treating a woman for a sprained ankle is likely to have access to the woman's genetic information. This is a concern in the hospital setting, as the data is highly sensitive and valuable, yet almost all departments handle it. As a result, healthcare takes on a complexity never seen before, and the response today is necessarily multi-professional, mainly within health organisations, in which teams record the various health data to which they have access.[4]

Nonetheless, personalised medicine and global health research benefit from the greater sharing of genomic data, as it provides the information required to improve clinical care and empower device and drug manufacturers in developing tests and treatments for patients. Moreover, the benefits of wide-scale sharing increase exponentially as data can be consistently reanalysed and reinterpreted with new knowledge and big data analytic tools available, providing exceptionally detailed information on individuals and their relatives.[5] Therefore, genetic data

[1] Marcello Ienca and others, 'Considerations for Ethics Review of Big Data Health Research: A Scoping Review' (2018) 13 PLoS ONE 1, 2

[2] Kyle B Brothers and Mark A Rothstein, 'Ethical, legal and social implications of incorporating personalized medicine into healthcare' (2015) Vol. 12,1, 44

[3] Marcello Ienca and others (n1) 9

[4] Sérgio Deodato, *A proteção dos dados pessoais de saúde*, (7th edn, Fundação Cupertino de Miranda, U. Católica Editora 2017) 30

[5] Williams G and others, 'Regulating the Unknown: A Guide to Regulating Genomics for Health Policy-Makers' (2021) European Observatory on Health Systems and Policies 7 <https://www.euro.who.int/en/about-us/partners/observatory/publications/policy-briefs-and-summaries/regulating-the-unknown-a-guide-to-regulating-genomics-for-health-policy-makers-2021> accessed 20 February 2022

collected can inform clinical decision-making and improve care as a whole to the benefit of patients.

However, the increased need for data sharing, which requires aggregation and analysis of genomic data in large databases, challenges current governance mechanisms. Mainly, since genetic data provides identification of the data subject throughout their lifetime and post-mortem[6]. Thus, with increased data sharing, it is challenging to ensure absolute confidentiality for data subjects, who may suffer severe consequences in the event of data breaches.[7] For instance, disclosure of patients' genetic data may cause various harms: a) they may suffer discrimination if their genomic data is inappropriately disclosed, e.g. health insurance companies may take into account the predisposition of the individual for coronary diseases; b) healthcare quality may be at risk if patients fear the disclosure of genomic data in healthcare services since they will abstain from sharing information with healthcare providers, which will result in an incomplete health record; and c) harm to public health and stigmatisation.[8] Moreover, by disclosing previously unknown phenotypes, a genetic data breach might reveal a health condition that the participant had wished not to become public.[9] Even if patients consent to share their identifiable genomes, they may not consent to the detailed characterisation that may occur by disclosing their genomic data.[10]

These disclosures may occur when data holders lose the data, for instance, by misplacing an unencrypted laptop or when third parties deliberately attack large genetic databases.[11] Thus, security becomes paramount when using individual-level genomic data. Therefore, the question raised is if the current legal framework fosters the protection of patients' data when stored and managed in these large databases without hindering innovation.[12]

---

[6] Kärt Pormeister, 'Genetic data and the research exemption: is the GDPR going too far?' [2017] 7 International Data Privacy Law 137, 1

[7] Jane Kaye, 'The Tension between Data Sharing and the Protection of Privacy in Genomics Research' (2012) 13 Annual Review of Genomics and Human Genetics 415, 423

[8] Kyle B Brothers and Mark A Rothstein (n2) 44

[9] Murat Sariyar, Stephanie Suhr and Irene Schlünder, 'How Sensitive Is Genetic Data?' (2017) 15 Biopreservation and Biobanking 494, 495

[10] Mahsa Shabani and Luca Marelli, ' Re-identifiability of Genomic Data and the GDPR' (2019) 20 EMBO reports 3, 2

[11] Zhiyu Wan and others, 'Sociotechnical Safeguards for Genomic Data Privacy' (2022) 0123456789 Nature Reviews Genetics, 430

[12] Kaye (n7) 423

In this regard, the relevant current legal framework is the General Data Protection Regulation ("GDPR")[13], which imposes obligations on organizations processing and managing personal data, including genetic data, by establishing a uniform framework for data protection across the EU. For example, article 9 of the GDPR establishes rules concerning sensitive data processing, including genetics. In this vein, the processing of genetic data for health-related purposes should be limited to what is necessary for the benefit of natural persons and society.[14] However, Article 9 is weakened because it opens the door for the Member States to interpret it differently, as they can introduce other conditions, including limitations, on processing genetic data.[15] Moreover, it raises controversy about the concept of 'limitations' only encompassing improvements to the standard of protection of the GDPR; or if it could also be understood to involve substantive limitations to this standard. Given the context of the provision, the former interpretation would be more in line with the spirit of the GDPR to create a minimum standard of protection for individuals.[16] Nonetheless, the lack of clarity of article 9(4) is problematic and ultimately leads to fragmentation across Member States' laws.

Furthermore, since genetic data has more significant interpretive potential than other types of (sensitive) data, it raises questions about whether it deserves specific treatment *per se* since it is alongside other special categories of data.[17] Genetic data are inherently identifying and provide information on relatives.[18] In addition, genetic data provides extensive and immutable information on data subjects and their relatives. Therefore, although the exceptional regime advocated by some scholars has no legal standing, it sets the ground to acknowledge that genetic data deserves greater attention in the GDPR and further guidance when implementing provisions in this context.

For instance, Article 32 GDPR, concerning the security of processing data, recognises the need to implement 'appropriate' technical and organisational measures to the risk. Hence,

[13] 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) [2016] \OJ L119/1

[14] Recital 53 GDPR

[15] Article 9(4) GDPR states "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health"

[16] Dara Hallinan, *Testing the GDPR in Relation to Biobanking* (2021) Vol. 131 2 Protecting Genetic Privacy in Biobanking through Data Protection Law 159, Chapter 9 189

[17] Edward S. Dove, 'Collection and protection of genomic data' [2018] in Gibbon S., Prainsack B., Hilgartner S., Lamoreaux J. (eds.) Handbook of Genomics, Health & Society. (London: Routledge, 2018) 4-5

[18] *Ibid* 5

controllers and processors must identify the specific risks of a situation, assess the impact according to the circumstance of the processing, and implement measures to mitigate those risks. However, it would be beneficial if there was guidance, for instance, by the European Data Protection Board (EDPB) clarifying the risks of genetic data processing[19] to help controllers and processors make an informed decision on which measures could be implemented. It should be considered that the risk of processing genomic data is higher than in processing health data, as once genomic data is stored in large datasets, the risk of re-identifiability increases through cross-reference with publicly available datasets, such as hospital records.[20] In addition, since genetic data value tends to increase with time, it cannot be retrieved once disclosed.[21] Even though Article 32 suggests some security measures that could be implemented, such as pseudonymisation and encryption, these measures prove inadequate to secure genetic data, as discussed further.

Therefore, besides investing in well-known measures such as anonymisation or pseudonymisation[22], new governance mechanisms that could better serve genetic data should be considered. The efficiency of standard protections used to anonymise, or de-identify sequence information is being questioned. Mainly, due to new sequencing technology that produces more affluent and more detailed information on individuals, for the possibility they create in easily re-identifying genetic data.[23]

Moreover, it is no surprise that there have been data breaches in healthcare services in the various Member States, compromising patients' data.[24] For example, there was a Portuguese Resolution[25] in 2018 in which a fine was imposed on a hospital for allowing illegitimate access to patients' health records. In addition, the software system revealed other flaws, given that the hospital had 985 registered doctor profiles, despite having only 296 doctors. Furthermore, hospital staff, psychologists, and other professionals had unrestricted access to all patient files – which

[19] Article 70 (1) (h) GDPR

[20] Mahsa Shabani and Luca Marelli (n10) 3

[21] Muhammad Naveed, 'Hurdles for Genomic Data Usage Management' (2014) 2014-Janua Proceedings - IEEE Symposium on Security and Privacy 44, 3

[22] Article 32 GDPR

[23] Kaye (n7) 423

[24] Recent cyberattacks in health infrastructures have been identified in various European countries, see Kaya and others, 'Biobanking and Risk Assessment: a comprehensive typology of risks for an adaptive governance' [2021] *Life Sci Soc Policy* 17**,** 9 <https://doi.org/10.1186/s40504-021-00117-7> accessed in 14 January 2022

[25] A Resolution concerns a decision of a deliberative or legislative body, in this case a decision of the Portuguese National Commission for Data Protection

doctors should only access – regardless of their professional category.[26] This Resolution shows the ease with which the hospital overlooked technical measures and proves that the current regime needs mechanisms to comply with the abstract provisions in the GDPR, namely Article 32.

Furthermore, there have been regulatory initiatives by the European Commission aiming to provide alternative governance models for genetic data without compromising security. Primarily, in the Commission's communication on the transformation of digital health and care in 2018, the goal – while ensuring *compliance* with the GDPR – was set to create a mechanism for the coordination between EU authorities to implement the secure exchange of genomic and other health data to advance research and personalised medicine.[27] Following this communication, the European Commission recognised the need to improve security and to have a robust data infrastructure in a recent proposal.[28] Accordingly, the European Commission will aim to set up a common framework across the Member States to share and exchange quality health data. Namely, it argues that EHR systems used in healthcare services must comply with minimum requirements to be interoperable and secure. Lastly, a recent initiative[29] aims to create a federated European infrastructure to enable secure cross-border linkage of genomic data. The data will be, in principle, analysed using distributed data analysis and AI learning techniques to ensure maximum data protection.

Despite the constant innovation in genetics and new initiatives from the European Commission, one should remember that new privacy breaching techniques will arise, and technical barriers to potential cyberattacks will decrease. Thereby, it is essential to balance privacy demands and data sharing adequately.[30] If this is achieved, would alternative governance models be more promising in handling genetic data than well-known techniques such as encryption?

---

[26] Comissão Nacional de Proteção de Dados, Portuguese Resolution n.º 984/2018, english summary available in CNPD - Deliberação n.º 984/2018 - GDPRhub

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society {SWD(2018) 126 final}

[28] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (EHDS Proposal), 3 May 2022, COM/2022/197 final

[29] European Commission, 'Federated European Infrastructure for Genomic Data', Digital Cloud Act <Funding & tenders (europa.eu)>

[30] Yaniv Erlich and Arvind Narayanan, 'Routes for breaching and protecting genetic privacy' [2014] Nature reviews Genetics 15(6) 409-421 < https://doi.org/10.1038/nrg3723> 13

1.2. Research Question

The privacy of genetic data has been challenged by recent developments in healthcare, leading to the widespread sharing and storing of genetic data. Despite the benefits of genetic data sharing, such as identifying potential correlations between diseases and genetic factors[31], it is important to consider patients' privacy. Namely, the potential impact if their genetic data is disclosed. Especially in clinical settings, doctors will have access to various datasets, increasing the chances they are cross-referenced and data is de-identified.[32] An example is the Portuguese Resolution[33], which illustrates how the GDPR's provisions are not being adequately enforced, given the insufficiency of technical and organisational measures implemented in Barreiro Hospital ("BH").[34] Thus, the question is whether patients' genetic data is sufficiently protected in healthcare institutions under the GDPR.

Hence, this thesis aims to provide an in-depth analysis of the GDPR security provisions applicable to genetic data, notably Article 32, and discuss if there is a need to improve *compliance* to ensure patients' safety. Besides, the current security mechanisms provided in Article 32 will be opposed to genetic data processing and its particularities. Further, the feasibility of alternative governance models to improve protection for genetic data will be discussed.
Thus, this thesis will answer the following **main research question**:

In light of the Portuguese Resolution n.º 984/2018, how can the EU legislator improve *compliance* with the GDPR by implementing a new type of security measure regarding storing and using patients' genetic data in healthcare services?

Hence, several **sub-questions** must be addressed:

1. What is the current genetic data security framework in the EU?

[31] Shabani M and Borry P, 'Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation' (2018) 26 European Journal of Human Genetics 149 <http://dx.doi.org/10.1038/s41431-017-0045-7> 149
[32] Mahsa Shabani and Luca Marelli (n10) 3
[33] Portuguese Resolution n. º 984/2018
[34] Article 32 (1) (b) and (d) GDPR

2. How does the Portuguese Resolution n.º 984/2018 demonstrate that the GDPR is currently ill-enforced?

3. Why are the current security mechanisms implemented in the genetic data processing context deemed inadequate to achieve utmost security for genetic data processing?

4. To what extent might alternative governance models, namely the EU Federated Database and the EHDS proposal, improve the protection of genetic data?

1.3. Literature Review

One article's approach[35] is that the Portuguese case illustrated how serious the Portuguese Data Protection Authority (CNPD)[36] is about the infringement of data protection principles by imposing stiff fines for *incompliance*. In my view, the CNPD's response does not show how the GDPR is effectively enforced by just applying a fine. The enforcement of the GDPR will continue to be problematic if, along with the fine, the CNPD does not provide the hospital with clear guidance on how to protect patients' sensitive data adequately.[37] Hence, the failure of the hospital to comply with GDPR's rules. Furthermore, the article argues for "more extensive [organisational and security] measures when it comes to special categories of data and monitoring on a large scale"[38], not clarifying what these could be. Perhaps, this lack of clarity is why the CNPD could not guide the hospital in the case at hand.

While there is extensive literature on the governance of genetic data under the GDPR[39], the primary focus is on providing a technical review of privacy methods which could benefit most genomic data sharing.[40] Moreover, these articles usually lack a comprehensive approach to support organisations in complying with the GDPR, thus avoiding further data breaches. Especially

---

[35] Rosa Barcelo, 'GDPR Enforcement: Portugal' (2019) <GDPR Enforcement: Portugal | Consumer Privacy World> accessed15 October 2021

[36] Portuguese Data Protection Authority monitoring the *compliance* with the GDPR

[37] Article 51 and Recital 117 GDPR

[38] Rosa Barcelo (n35)

[39] Susan MC Gibbons & Jane Kaye, 'Governing Genetic Databases: Collection, Storage and Use' [2015], King's Law Journal, 18:2, 201-208; Kristi Harbord, 'Genetic Data Privacy Solutions in GDPR' [2019] 7 Tex. A&M L. Rev. 269; Mahsa Shabani & Luca Marelli (n10); Kaya and others (n24)

[40] Knoppers and others, 'Towards a data-sharing Code of Conduct for international genomic research' (2011) Genome Med 3, 46 <https://doi.org/10.1186/gm262> accessed 15 October 2021; Kaye (n7). See also Mahsa Shabani, 'Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems?' [2018] Journal of the American Medical Informatics Association

regarding genetic data, security/privacy methods in organisations such as hospitals should be tailored to genetic data and its particularities. For example, de-identification techniques such as pseudonymisation should consider the difficulty in determining which genetic data is re-identifiable to avoid the illegitimate identification of individuals.[41]

Therefore, this thesis will focus on genetic data management in healthcare by connecting the current enforcement gaps of Article 32 of the GDPR with a Member State case study. Furthermore, it will help analyse which privacy methods could be effectively implemented in healthcare services to prevent further breaches. Finally, this thesis will examine two promising measures: a Federated Database to enable secure cross-border linkage of genomic data, alongside the new European Health Data Space (EHDS) proposal.

While there is literature on possible innovative governance models that could be applicable[42], there is a gap in the literature explaining their vulnerabilities, such as accountability and data scalability[43]. Shabani takes an innovative approach and proposes using blockchain technology as a security measure.[44] She further explores using blockchain as a platform instead of a centralised infrastructure in which authority is distributed among actors.[45] However, liability issues may arise since blockchain platforms work without an intermediary and trust is placed on the network instead of a third party. Therefore, it can be problematic because it is not clear who is liable in case of a data breach. Shabani does not explain this, as she focuses on what method would benefit data sharing. Indeed, liability was critical in the Resolution in question, where BH used as its defence the fact that the software was in charge of a third party, denying accountability for the data breach. Therefore, the gap can be addressed by exploring those vulnerabilities and discussing what measures could be adopted that effectively protect patients' genomic data in healthcare services, thus improving *compliance* with the GDPR.

---

[41] Eric Topol, 'The Patient Will See You Now – The Future of Medicine Is in Your Hands' (2015) BasicBooks New York 234-235

[42] Juha Muilu and others, 'The federated database – a basis for biobank-based post-genome studies, integrating phenome and genome data from 600 000 twin pairs in Europe' [2007] *Eur J Hum Genet* **15,** 718–723 <https://doi.org/10.1038/sj.ejhg.5201850> accessed 15 October 2021; Kaye (n7); Shabani M (n40)

[43] Francisco Ribeiro de Sousa, 'Blockchain Pharma' [2021] ISEG Lisbon School of Economics and Management, University of Lisbon 315

[44] Mahsa Shabani (n40)

[45] *Ibid* 2

1.4. Methodology

This thesis is based on a doctrinal legal research approach. It will include the study of statutory legislation, case law and academic literature on governance of genetic data in the EU, GDPR enforcement, and cybersecurity literature concerning possible measures to manage genetic data in healthcare services.[46] In addition, an in-depth legal analysis of the security provisions of the GDPR applicable to genetic data, notably Article 32, will be conducted, and it will be assessed if the current regulatory framework is sufficient to ensure patients' data security. Moreover, an analysis will be conducted to critically evaluate the GDPR's provisions, namely the failure of BH to comply with security provisions. This analysis will be combined with surveys and reports from the Commission on Data Protection Authorities (DPAs) and GDPR enforcement across the Member States to enrich the argument regarding the current lack of enforcement of the GDPR and the need to provide further measures to improve data security in healthcare services.

When elaborating on an alternative solution, recent initiatives from the European Commission concerning the governance of genetic data will be critically assessed, considering the GDPR, to understand whether and how these initiatives can be implemented to improve the protection of patients. The Call for a Federated European infrastructure for genomics data[47] and the EHDS proposal[48] will be considered in this regard.

Lastly, considering this thesis is written from a legal standpoint and focused on EU law, particularly the GDPR, it does not provide a technical review of the feasibility of all possible techniques to improve genetic data security in healthcare services. Nor does it explore other Directives, such as the Directive (EU) 2016/1148 (NIS Directive)[49], an EU-wide cybersecurity legislation that complements the GDPR by providing adequate IT security of network and information systems. Even though both regulations interact through the principle of security of personal data[50], *compliance* obligations under these legislations should be assessed apart since they

[46] Muilu and others (n42)
[47] European Commission, 'Digital Europe Programme (DIGITAL) Call for Proposals' (2021) Cloud Data and TEF 1, 34
[48] EHDS Proposal
[49] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)
[50] Embedded in GDPR in the principle of integrity and confidentiality, presented in article 5(1) f)

serve different purposes and by different authorities.[51] Moreover, the focus on the GDPR's security provisions helps to pave the way to understand how the GDPR does not provide clear solutions regarding genetic data storage and usage.

1.5. Chapter Overview

This thesis will be structured in the following way: Following the introduction, a brief discussion on how genomic data should be treated differently from health data in GDPR will be carried out, with regards to the high risk of identifiability, the difficulties presented with anonymisation, and the relational nature of many genomic data providing detailed information on data subjects and their blood relatives. The first chapter will evaluate the current legal framework in the EU regarding genomic data security, especially Article 32 of the GDPR. The second chapter will address the Portuguese Resolution n.º 984/2018 and reflect on the GDPR enforcement.

The following chapter will discuss how to address the GDPR vulnerabilities for better governance of genetic data at the EU level. The first step is explaining how standard encryption techniques fail to provide adequate protection for genetic data and what measures have been proposed so far. Afterwards, it will be discussed how the existing regulatory framework could be better implemented through different security measures to ensure that the patient has greater control over how their genomic data is used and stored in healthcare services. Finally, two possible measures will be analysed and the possibility of using them with the current framework: a Federated Database alongside the EHDS proposal.

Chapter 2 | What is the current genetic data security framework in the EU?

The GDPR applies to personal data concerning data relating to an identified or identifiable individual.[52] Recital 26 provides a broad understanding of an 'identifiable' person, appealing to a test of 'likelihood of identification'.[53] Moreover, Recital 26 opens the door for diverse interpretations of what would constitute the "all the means reasonably likely to be used" to

[51] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 Computer Law and Security Review 105336 <https://doi.org/10.1016/j.clsr.2019.06.007> 10

[52] Article 4 (1) and Recital 26 GDPR

[53] Taner Kuru, 'Genetic Data: The Achilles' Heel of the GDPR?' (2021) 7 Eur Data Prot L Rev 45, 48

determine whether a natural person is identifiable. For example, in the *Breyer* case, concerning recital 26, the CJEU assumed there must be a likelihood for information to be combined and, thus, identify the individual.[54] Besides, the Court recognized the means of identification should be reasonably likely to be used, such as the identification of the data subject not being illegal or practically impossible.[55] For instance, even if the personal data has undergone pseudonymisation, it could be considered personal data if it can be linkable to an individual by cross-referencing additional information.[56] In contrast, anonymised data is wholly excluded from the scope of the GDPR because the individual is not or is no longer identifiable.[57]

Nevertheless, categorising identifiable and non-identifiable data is not always easy, especially concerning genetic data. Although genetic data is defined in the GDPR as personal data[58], thus identifiable, even when we are in the presence of genetic datasets where data is anonymised, likely, this data will be identifiable. Moreover, cross-linking data can increase the chance of anonymous data being traced back to the individual.[59] In this regard, scholars have adverted that GDPR should not be tailored to static categories of data, such as the identifiable/anonymous distinction; it should adapt to the constant recombination and re-contextualisation of data.[60]

Furthermore, Article 29 Working Party ("WP29") examined this issue[61], opening the possibility that there may be exceptional cases in which genetic data are not considered personal data.[62] When determining the status of genetic data and whether the data subject is identifiable, many factors are considered to determine the likelihood of identification. Namely, the institutional setting in which the processing occurs, the stage of the processing, the availability of cross-

[54] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 45
[55] *Ibid* para. 46
[56] Article 4 (5) and Recital 26 GDPR
[57] Recital 26 GDPR
[58] Article 4(13) and Recital 34 GDPR: "'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person"
[59] Luca Marelli, Elisa Lievevrouw and Ine Van Hoyweghen, 'Fit for Purpose? The GDPR and the Governance of European Digital Health' (2020) 41 Policy Studies 447 <https://doi.org/10.1080/01442872.2020.1724929> 455
[60] *Ibid* 456
[61] Article 29 Working Party, 'Opinion on Genetic Data' (2004) 9 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf >
[62] *Ibid* 5. For instance, DNA samples taken in a given place (e.g. traces at the scene of a crime) where the link to a specific person may be unclear

reference datasets, incentives, and availability of resources for re-identification.[63] This broad interpretation could make a person identifiable due to technological developments that could render anonymous data at the time of the collection into personal data.[64] Indeed, technological developments facilitate the re-identifiability of genetic data. Namely, in the setting of healthcare services, the risk of re-identifiability increases tremendously through cross-reference with publicly available datasets such as hospital health records.[65] Hence, anonymity in this setting is hardly unattainable. Hence the importance of discussing genetic data security in healthcare services, particularly considering the security provisions in the GDPR.

Furthermore, the WP29[66] identified other notable features of genetic data that make it unique compared to health data, justifying the defence of special legal protection for genetic data. These features range from the fact that it is immutable over time – posing problems when disclosed because it cannot be retrieved – its richness in terms of information content, and the kinship information concerning the blood relatives.[67] However, the GDPR, unlike the WP29, does not recognise unique characteristics and the exceptional sensitivity of this type of data since genetic data is alongside health data as a special category of data.[68] Even if Article 9(4) GDPR acknowledges that genetic data processing might benefit from further limitations, this provision also concerns biometric data and data concerning health, which only reinforces this standpoint. Hence, some scholars argue for the need to implement an exceptional regime for genetic data, as it has more significant interpretive potential than other types of data.[69] However, it remains to be seen whether this approach would be adequate in practice since it does not have legal standing.

Nonetheless, this approach starts an essential discussion in acknowledging that genetic data deserves greater attention in the GDPR and further guidance when implementing provisions in this context – especially concerning genetic data processing. For instance, according to Article 9, processing genetic data is prohibited unless it is required for the provision of health, treatment or diagnosis.[70] Nonetheless, the only safeguard when genetic data is processed under this provision

[63] Mahsa Shabani and Luca Marelli (n10) 3
[64] Taner Kuru, 'Genetic Data: The Achilles' Heel of the GDPR?' (2021) 7 Eur Data Prot L Rev 45, 48
[65] Mahsa Shabani and Luca Marelli (n10) 3
[66] Article 29 Working Party, 'Opinion on Genetic Data' (2004) 9, 4
[67] *Ibid* 4-5
[68] Article 9 (1) GDPR
[69] Edward S. Dove (n17) 5 addressing the so-called *genetic exceptionalism*
[70] Article 9 (2) (h) GDPR

is that it is strictly collected, used or shared by a person subject to professional secrecy.[71] For instance, the increased availability of genetic data would benefit from stricter processing requirements to avoid potential misuse since it could create high risks to the rights and freedoms of individuals.[72]

Unfortunately, Article 9 does not comprehensively address all concerns related to the processing of sensitive data, in particular genetic data. Firstly, this provision does not justify the processing prohibition regarding special categories of data. Recitals 71, 75 and 85 of the GDPR refer to the risks of processing with discriminatory effects as among other possible risks, such as identity theft, loss of confidentiality and unauthorised reversal of pseudonymisation. Furthermore, genetic data may reveal personal data concerning the health and characteristics of the holder and the biological group to which they belong. Hence, discrimination is not the only risk associated with genetic data processing.[73]

In addition, Article 9(4) states, 'Member States may maintain or introduce further conditions, **including limitations**, regarding the processing of genetic data, biometric data or data concerning health'. Unfortunately, the text does not clarify what limitations are permitted, as it is not sure if the provision should be interpreted to encompass restrictions on the processing that increase the protection standard; or if those limitations can also reduce the measure of protection implemented in the GDPR.[74] Accordingly, the provision opens the door for Member States to interpret it differently and, thus, fragment data security across the EU, implementing different levels of protection when processing genetic data.

It is essential to note that the draft of the GDPR comprised an essential provision empowering the Commission (and not the Member States) 'to adopt delegated acts […] for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data.'[75] Unfortunately, this provision was excluded from the

[71] Article 9 (3) GDPR

[72] Shabani M and Borry P (n31) 149

[73] Alexandre Sousa Pinheiro and others, *Comentário Ao Regulamento Geral de Proteção de Dados* (2018) Almedina 236-238

[74] Dara Hallinan (n16) 189

[75] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (General Data Protection Regulation) (2012) COM/2012/011 final – 2012/0011 (COD), 25 January, Article 9 (3)

official version. Still, it would be a possible pathway to create uniform binding and detailed standards related to processing genetic data within the EU.[76]

Moving on to the security-related provisions, the GDPR focuses on a decentralised, context-specific and risk-based approach with appropriate accountability for data controllers[77] and 'data protection by design and by default'[78], ensuring appropriate measures are implemented throughout all data processing activities.[79] Thus, security measures have to be implemented to ensure security and prevent processing in infringement of the GDPR.[80] The GDPR, unlike the prior Data Protection Directive[81], imposed this implementation obligation on both data controllers and data processors. The obligation to implement technical and organisational measures unfolds into two: that of data security (Article 32) and those required under the general rights and obligations contemplated in the GDPR (Articles 24 and 25).

Firstly, the obligation to implement technical and organisational measures is one of the results, meaning the controller must implement appropriate and effective measures to comply with the GDPR, and these must both comply with the principles set out in the regulation and fulfil the rights of the data subjects.[82] Secondly, Article 32 imposes a security duty on controllers and processors by requiring them to implement technical and organisational measures 'appropriate' to the risks of processing. Finally, it constitutes an obligation of means, meaning that once they have implemented adequate measures, if there is a data breach, they may not be infringing the GDPR.[83]

The determination of the technical and organisational means should consider several criteria: *state of the art* (the most advanced techniques available on the market); their implementation costs and nature of the processing; the scope regarding data categories, data volume, territorial extent or number of data subjects; and the context and purposes of the processing. Lastly, the risks of processing should be considered and weighed according to the

[76] Petro Sukhorolskyi and Valeriia Hutsaliuk, 'Processing of Genetic Data under GDPR: Unresolved Conflict of Interests' (2020) 14 Masaryk University Journal of Law and Technology 151, 161

[77] Article 5 (2) and article 24 (1) GDPR

[78] Article 25 GDPR

[79] Mahsa Shabani and Luca Marelli (n10) 4

[80] Recital 83 GDPR

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (1995)

[82] Article 25 GDPR

[83] Article 32 GDPR

severity and likelihood of their occurrence.[84] Thus, controllers and processors in each Member State have to identify the specific risks of a situation, assess the impact according to the circumstance of the processing, and implement measures to mitigate those risks.[85] In addition, the term ’appropriate’ occurs throughout Article 32, leaving room for data controllers across the Member States to interpret this word differently and fragment data security across the EU.

On the one hand, the GDPR focuses on *ex-ante* regulation to keep the collection and processing to the minimum necessary and proportionate to the purposes of the processing.[86] Furthermore, it introduced new obligations on controllers to conduct data protection impact assessments (DPIAs),[87] which should occur before data processing in the case of high-risk activity.[88] For instance, when processing data on a large scale in healthcare settings,[89] and even more so in the case of large-scale genetic data processing. The more identifiable the data, or the higher the risk, the greater the control needed by the data controller and processors, hence, the importance of DPIAs in the genetic data processing.

On the other hand, the GDPR increases *ex-post* regulation focusing on accountability and oversight.[90] Nevertheless, as Koops puts it, increased compliance and better data protection will depend on 'whether the enforcement by supervisory authorities will be effective (…) but also on whether the act of documentation will make controllers think about what they do and adapt their practice accordingly if they realise when documenting, that their activities are not compliant with the regulation'.[91] Hence, it could be said that more extensive regulation does not necessarily lead to better data protection if controllers' mindset is to follow the rules to be rule-compliant while not fully understanding the core data protection framework.[92] Therefore, the following chapters will shed light on how controllers across the EU implement GDPR security provisions. In the next chapter, a Portuguese case will be discussed in which controllers in BH did not adequately comply with article 5 and article 32 of the GDPR, resulting in an insufficiency of security measures to

[84] Article 32 GDPR
[85] Alexandre Sousa Pinheiro and others (n 73) 635-636
[86] Article 25 (2), Article 5 (1) (b) and (c) GDPR
[87] Article 35 GDPR
[88] Article 35 (1) GDPR and Recital 91
[89] Article 35 (3) (b) GDPR and Recital 91
[90] Article 5 (2) (accountability principle), Article 24 and Article 30 GDPR (records of processing activities)
[91] Bert Jaap Koops, 'The Trouble with European Data Protection Law′ (2014) 4 International Data Privacy Law 250, 255
[92] *Ibid* 255

protect patient data. More importantly, this case study will show that the GDPR is ill-enforced, which ultimately harms data subjects in vulnerable positions, such as patients in healthcare institutions.

Chapter 3 | How does the Portuguese Resolution nº 984/2018 demonstrate that the GDPR is currently ill-enforced?

After examining the provisions related to genetic data within the data protection framework, implementing appropriate security measures when processing data on a large scale, such as in healthcare settings, has been identified as the most crucial point to ensure the security of genetic data. According to the obligation to ensure confidentiality, integrity, availability, and resilience of the processing systems,[93] healthcare systems should be prepared to handle any cyberattack. Nevertheless, digital health technologies and healthcare institutions are often unprotected, making them vulnerable to cyberattacks and breaches that lead to patient harm and data misuse.[94]

One of the most significant ransomware attacks, known as WannaCry, occurred in 2017 and targeted the UK's National Health Service (NHS), affecting hospitals and surgeries across England and Scotland.[95] The attack highlighted critical security vulnerabilities, especially in large public institutions like the NHS.[96] Furthermore, during the Covid-19 outbreak, there were two crucial incidents. One occurred in Brno University Hospital[97], leading to the postponement of surgical procedures and re-routing patients to nearby hospitals, which was critical given it is one of the country's most prominent Covid-19 testing laboratories.[98] The other occurred in Düsseldorf[99] and compromised the digital infrastructure of the hospital, ultimately leading to a

[93] Article 5(1) (f), Article 32(1) b) and Recital 49 GDPR

[94] Eva Thelisson, 'AI Technologies and Accountability in Digital Health' (2021) Cambridge Bioethics and the Law Series, Cambridge University Press 13 <https://ssrn.com/abstract=3828206> accessed 20 December 2021

[95] Acronis, 'The NHS cyber attack: how and why it happened, and who did it' (Acronis, 7 February 2020) <The NHS cyber attack: how and why it happened, and who did it (acronis.com)> accessed 15 June 2022

[96] *Ibid*

[97] Security Magazine, 'Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak, (Security Magazine, 17 March 2020) <Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak | 2020-03-17 | Security Magazine> accessed 15 June 2022

[98] ENISA, 'Main Incidents in the EU and Worldwide' (2019-2020) 16 <*ENISA ETL2020 - Main Incidents in the EU and Worldwide (europa.eu)> accessed 15 June 2022

[99] William Ralston, 'The untold story of a cyberattack, a hospital and a dying woman' (WIRED, 11 November 2020) <The untold story of a cyberattack, a hospital and a dying woman | WIRED UK> accessed 15 June 2022

patient dying due to a delay in treatment. In this case, the culpability of the hospital's IT staff was considered, specifically if they could have better protected the hospital by monitoring the network more closely.[100] In this chapter, the focus will be on analysing a Portuguese case which provides an excellent example of how things can go wrong when Article 5 and Article 32 GDPR are not adequately complied with by the controllers in healthcare organisations.

On 2 July 2018, based on a complaint from the Portuguese Medical Association, the CNPD inspected the information management and access systems at BH in Portugal. Here, it acknowledged that there was no document providing for the correspondence between the functional competencies of hospital users (medical and non-medical) and the access profiles to clinical information, nor a document listing the access criteria.

BH uses the integrated hospital information system (SONHO) and the hospital clinical record system (SClínico). The former is used for hospital administrative support, and the latter registers the clinical information of users, allowing access and sharing of that information among health professionals. In SONHO, each user account has two attributes that enable the hospital to manage the access profiles to the system: the functional group and the activity group. During the inspection, the CNPD created a test user account with a profile identical to that of the nine Social Services technicians – non-medical practitioners – and verified that it allowed access, without any restrictions, to the clinical file of the patients. Moreover, using the same user account, it was possible to access information in another hospital concerning clinical episodes of a patient of BH.

The CNPD found that BH acted deliberately, knowing that it was obliged to implement technical and organisational measures essential to identifying and authenticating users. In addition, the hospital should have considered the different access privileges corresponding to its employees' professional categories and ensure the information's security. Lastly, it was responsible for having a reliable auditing system for identifications, access, and security guarantees.[101]

The CNPD found that there were three breaches of the GDPR. Firstly, it found three vulnerabilities in the authentication and access control to the patients' database. In particular, it found the hospital was allowing access to users without adequate authorisation, noting that 985 doctors had access to clinical data when the hospital in question had only 296 doctors.[102] As stated

[100] *Ibid*

[101] Portuguese Resolution n.º 984/2018 13

[102] *Ibid* 12

above, the CNPD considered that the hospital did not have an internal protocol for creating user accounts, access levels to medical information or a method for authenticating the doctors' connection with the hospital.[103] Consequently, the indiscriminate access to clinical data by professionals through profiles inappropriate to their functions and professional category breached the data minimisation principle (Article 5(1)(c) GDPR). Furthermore, the CNPD considered the existence of access credentials that allowed any doctor of any speciality to access patients' data in the hospital centre at any time and without any time limit to be unsustainable, thus, violating the principle of data minimisation.

Secondly, BH infringed the integrity and confidentiality principle (Article 5(1)(f) GDPR) by not implementing appropriate measures, which led to it being charged with two fines of €150,000. Finally, the third infringement was due to the hospital's inability to 'ensure the confidentiality, integrity, availability and ongoing resilience of the processing systems and services', which led to the application of a fine of €100,000, under Article 32(1)(b) and (d) GDPR.[104]

Even though the CNPD recognised the cooperation of BH to fix the system's vulnerabilities, it considered that it was the hospital's responsibility to take adequate security measures, which it deliberately overlooked. Furthermore, the hospital should have taken appropriate measures suited to the high risk of processing data on a large scale, which it did not. For instance, the defendant could have corrected the system that allowed professionals of various categories to access information on patients' files.

Even though the CNPD admits that the conduct did not cause concrete harm to patients, it was correct when stating, 'one cannot ignore or disregard the breach of objective duties of the controller, especially where potential access to sensitive data is at stake.'[105] Hence, it explains the importance of *compliance* with the GDPR because it is not about remedying the damages caused by a breach; it is about controllers preventing it in the first place. As explained, Article 32 embodies an obligation of means, meaning the controller is required to implement technical and organisational measures, independent of a data breach or concrete harm happening.

[103] *Ibid* 16
[104] *Ibid* 4
[105] *Ibid* 8

Furthermore, the CNPD considered several circumstances to determine the fine. Firstly, the breach concerned health data**, including genetic data (Article 9(1) GDPR)**. In addition, the gravity and duration of the infringement were reflected in the number of patients' data affected, corresponding to every hospital patient. Furthermore, as attenuating circumstances, the CNPD considered that BH had not previously committed infringements, the degree of cooperation was considered adequate, and, finally, **the monitoring parameters of the access logs to the information did not depend on the defendant**.[106]

As it stands, this argumentation was flawless. BH (controller) claimed that since the software was in charge of a third-party (processor), the hospital should not be held accountable. Even though the CNPD disagreed explicitly with this claim, it recognised it as a reason for a "reduced" fine which, in my view, demonstrated a poor understanding of the controllers' accountability principle expressed in the GDPR.[107] Even though it was not directly in charge of the IT system, the hospital should have ensured that its patients' data was secure. There was a malformation in the software, and the hospital should be held accountable for not checking such vulnerabilities before processing data.[108]

Nonetheless, due to the malformed software, a data breach occurred causing the unauthorised disclosure of access to personal data.[109] In this case, there was an internal data breach since someone unauthorised inside the hospital accessed patients' data. Among the fines imposed for internal data breaches concerning Article 32, around 50% occurred in facilities dealing with sensitive personal data, including genetics.[110] For instance, in a similar occurrence to the Portuguese one, the Hague Hospital was fined for an internal data breach, failing to implement sufficient technical and organisational measures. Namely, the hospital did not conduct regular checks on who was consulting the files, and two-factor authentication was missing.[111] In addition,

[106] Portuguese Resolution n.º 984/2018 17

[107] Article 5 (1) (f) and Article 5(2) GDPR

[108] Through a DPIA, for instance, in Article 35 (1) and Article 35 (3) (b) GDPR

[109] Article 4 (12) GDPR

[110] Utzerath J and Dennis R, 'Numbers and Statistics: Data and Cyber Breaches under the General Data Protection Regulation' (2021) 2 International Cybersecurity Law Review 339, 342

[111] Autoriteit Persoonsgegevens, 'Haga fined for insufficient internal security of patient files' (Autoriteit Persoonsgegevens ,16 July 2019) <Haga fines for insufficient internal security of patient files | Dutch Data Protection Authority (autoriteitpersoonsgegevens.nl)> accessed 15 May 2022

Article 32 was infringed in Cork University Hospital[112] due to the use and disposal of documents containing patients' data. Furthermore, in St. Olavs Hospital HF[113], poor patient records management made them accessible to all authorised users within the Central Norway Regional Health Authority. Lastly, a fine was imposed in Sweden for failing to assess risk and implementing adequate access controls in Capio St. Goran's Hospital.[114] What was noted by the EU DPAs was the insufficiency of technical and organisational measures in every situation where Article 32 fines were issued for data breaches.[115]

Interestingly, the CNPD has only issued one penalty for an Article 32 breach. Portugal is one of the countries in Europe with the lowest number of fines applied in the last four years.[116] Although the imposition of penalties is not enough to sufficiently assess the effectiveness of any supervisory authority, it is undoubtedly one of the essential elements concerning the ability to enforce the GDPR.[117] Besides, the CNPD does not publish the decisions for all the fines it applies, nor the identity of the defendants.[118] The only exception was the Portuguese decision in question, where BH was identified. This general lack of information is detrimental to the public, who remain uninformed regarding *compliance* with the GDPR.

Moreover, complying with the GDPR is resource-intensive as it requires some consideration before implementation.[119] The GDPR uses indeterminacy and abstract provisions

---

[112] Irish Examiner, 'Cork hospital fined €65k after patients' personal data found in public recycling facility' (Irish Examiner, 4 November 2020) <Cork hospital fined €65k after patients' personal data found in public recycling facility (irishexaminer.com)>

[113] European Data Protection Board, 'Norwegian DPA: St. Olavs Hospital fined' (2021) <Norwegian DPA: St. Olavs Hospital fined | European Data Protection Board (europa.eu)>

[114] DataGuidance, 'Sweden: Datainspektionen completes audit of Capio St. Goran's Hospital, imposes fine of SEK 30M' (DataGuidance, 4 December 2020) <Sweden: Datainspektionen completes audit of Capio St. Göran's Hospital, imposes fine of SEK 30M | News post | DataGuidance>

[115] Utzerath J and Dennis R (n110), 344

[116] ESET, 'The GDPR Report – Which businesses have been hit with the biggest GDPR fines?' (ESET, 9 September 2021) <The GDPR Report – Which businesses have been hit with the biggest GDPR fines? | ESET> accessed 8 June 2022

[117] Diogo Duarte, 'Porque falha em Portugal a proteção de dados pessoais' (Setenta e Quatro, 7 January 2022) available in portuguese only <Porque falha em Portugal a protecção de dados pessoais | Setenta e Quatro> accessed 14 June 2022

[118] CMS Rui Pena & Arnaut, 'GDPR Enforcement Tracker' <GDPR Enforcement Tracker - list of GDPR fines> accessed 20 June 2022

[119] Sophie Stalla-Bourdillon, University of Southampton (UK), 'Is Indeterminacy Undermining the GDPR?' in 'Can Law be Determinate in an Indeterminate World?' (Speech at the CPDP Conference, Brussels, 25 May 2022, 25:41-44:00) < CAN LAW BE DETERMINATE IN AN INDETERMINATE WORLD? - YouTube > accessed 14 June 2022

without providing comprehensive examples and guidelines. Even recitals are not specific and only address a few concerns.[120] For instance, recital 71[121] discusses the need to ensure appropriate measures to secure the processing of, among others, genetic data. Still, it does not help controllers determine what actions to implement in practice nor the risks involved – the same for ambiguous terms such as 'appropriate measures' in Article 32, which raise enforcement issues.[122] Notably, a survey was conducted in health clinics in Portugal[123], where clinics were asked how they had implemented the new measures enshrined in the GDPR. The answer was that nobody in the organisation had enough knowledge to conduct the process, thus, they had hired the services of third parties to guide them in complying with the GDPR requirements, just as in the Portuguese case.[124] This survey demonstrates, as Koops argued, that too much faith is placed in controllers[125] who do not have the training or awareness to comply with the GDPR. Creating 'more ex-ante and ex-post paperwork and checklist obligations creates a situation in which controllers will blindly follow a set of rules to be rule-compliant, while (still) not understanding much about data protection'.[126] To account for this, the WP29 mentioned 'compliance should never be a box-ticking exercise, but should be about ensuring that personal data is sufficiently protected.'[127] Perhaps that is why some scholars argue for a harm-based approach, which focuses on evidence of actual harm resulting from data misuse or security breaches.[128]

[120] Indra Spiecker gen. Döhmann, Goethe University (DE), 'Can Law be Determinate in an Indeterminate World?', (Speech at the CPDP Conference, Brussels, 25 May 20222, 24:20-24:40) < CAN LAW BE DETERMINATE IN AN INDETERMINATE WORLD? - YouTube > accessed 14 June 2022

[121] Recital 71 second paragraph GDPR states "(…) the controller should (…) implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of (…) genetic (data) (…) or that result in measures having such an effect"

[122] Kristi Harbord (n39) 290

[123] Isabel Maria Lopes and Pedro Oliveira, 'Implementation of the General Data Protection Regulation: A Survey in Health Clinics', (2018) 2018-June Iberian Conference on Information Systems and Technologies, CISTI 1

[124] *Ibid* 5

[125] Koops (n 91) 253-254

[126] *Ibid* 255

[127] Article 29 Data Protection Working Party, 'Statement of the Working Party on current discussions regarding the data protection reform package' (2013) < DRAFT FINDINGS (europa.eu)> 2-3

[128] Mahsa Shabani and Luca Marelli (n10) 2

Furthermore, the CNPD is not well-equipped with financial or human resources, making it difficult to monitor and enforce the GDPR effectively.[129] In a Brave Report[130], the CNPD was considered the fourth-smallest DPA in the EU with one of the lowest budgets. [see Appendix-1]. Even though the number of complaints handled by the CNPD has been increasing steadily every year, the ratio is still meagre. A report in 2021 indicated that of 10.413 complaints made through the CNPD's website, only 1232 were investigated and handled.[131] This conflicts with Article 52(4) GDPR, which requires the Member States to allocate sufficient funds to their DPAs to perform their tasks effectively. In addition, the lack of expertise of the DPA members of the EU DPAs was identified as a common problem[132], conflicting with Article 53(2) GDPR.[133] In Portugal, the situation is not different, as some members do not have relevant technical expertise in data protection.[134] As shown in a recent report, of a total of 35 staff members of CNPD, only 8 are technical experts. [see Appendix-2][135]

The concerns mentioned – the DPA's lack of resources and technical expertise combined with legal vagueness on concepts such as 'appropriate'[136] – have not yet been addressed. The Portuguese case is an example of this. The CNPD's lack of resources resulted in poor IT security in the hospital, which compromised patients' data. The inattention paid to improve IT security resulted from a lack of (technical) expertise in preparing this infrastructure for potential cyberattacks, given that cybersecurity is still relatively new in the health field.[137] If DPAs were more capable of advising controllers on which measures to implement to serve patients better,

[129] Article 57 (1) (a) GDPR

[130] Johnny Ryan, 'Europe's Governments Are Failing the GDPR' (Brave, April 2020) 14, 6

[131] Comissão Nacional de Proteção de Dados, 'Relatório de Atividades 2021', 21 June 2022, Lisbon <CNPD> accessed 14 July 2022, 8-14

[132] Johnny Ryan (n130) 5

[133] Article 53(2) GDPR states "Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers."

[134] Diogo Duarte (n117)

[135] Alan Toner and Johnny Ryan, 'Europe's enforcement paralysis' (Irish Council for Civil Liberties, April 2022) 10

[136] Article 32 GDPR

[137] Salem T Argaw and others, 'Cybersecurity of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks' (2020) 20 BMC Medical Informatics and Decision Making 1, 2

compliance issues would most probably decrease.[138] As a result, it led in this case to the insufficiency of technical and organisational measures in place.[139]

Furthermore, this insufficiency also occurs because the security measures enshrined in Article 32 GDPR fail to address genetic data security issues.[140] Although the case generally concerns illegitimate patient records access, these contain sensitive data, including genetics. However, there is no guidance on what measures would be appropriate in genetic data processing,[141] although its relevance is demonstrated in the number of investigations conducted on techniques that could be used to protect genomic data, which have ended in policy changes.[142] For instance, there are various documents by the EDPB and ENISA, concerning the security of personal data processing under Article 32 of the GDPR.[143] Even though any EU document has provided guidance on genetic data processing until now, it would be a possible pathway to bring certainty to this matter. Another pathway would be considering the threshold established in DPA decisions, such as the one released by the Italian DPA issuing specific provisions for processing genetic data.[144] This decision addressed the access to stored genetic data through authentication systems and possible security measures if this data is contained in large databases.[145]

In fact, the extensive and immutable information that genetic data can provide, if mishandled, about data subjects and their relatives makes it crucial for there to be a specific technical measure adequate to the risk of processing this type of data in a healthcare setting.

---

[138] Giovanni Sartor, EUI (IT), 'Can Law be Determinate in an Indeterminate World?', (Speech at the CPDP Conference, Brussels, 25 May 20222, 57:00-57:30) < CAN LAW BE DETERMINATE IN AN INDETERMINATE WORLD? - YouTube > accessed 14 June 2022

[139] Article 5(1) f) and Article 32 GDPR

[140] Namely, the pseudonymization and encryption of personal data (Article 32(1)(a)); the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems (Article 32(1)(b)); the ability to restore the availability and access to personal data in a timely manner in case of an incident (Article 32(1)(c), for example by setting up a disaster recovery plan); and a process for regularly testing, assessing and evaluating the effectiveness of security measures (Article 32(1)(d))

[141] Recital 71 second paragraph GDPR

[142] Thomas Finnegan, Alison Hall and Jeffrey M Skopek, *Identification and Genomic Data* (2017) www.phgfoundation.org, PHG Foundation 17

[143] European Data Protection Board, 'Guidelines 3/2019 on processing of personal data through video devices' (2020); ENISA, 'Handbook on Security of Personal Data Processing' (2017)

[144] Garante Per La Protezione Dei Dati Personali, 'Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, coma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]' (2019) available in Italian only < Provvedimento recante le prescrizioni relative al trattamento di... - Garante Privacy> accessed 15 July 2022

[145] *Ibid* 9

Nonetheless, although Recital 15 GDPR stresses that the protection of natural persons should not depend on the techniques used[146], Article 32 expresses a clear preference for the measures it provides, making it likely that regulators will expect data controllers and processors to use them when possible.[147] These measures will be addressed in the following chapter, as well as their feasibility for securing genetic data processing.

The GDPR often depends on national laws to determine some of the vague concepts presented throughout its text. As a result, different interpretations among the Member States may lead to inconsistency in ensuring health and genetic data security. For example, in Portuguese law, special protection is given to genetic data; however, it focuses on scientific research activity. Less attention is given to the misuse of genetic data in healthcare settings, such as the case discussed. In addition, national law does not develop concepts of personal data or pseudonymisation, relying only on the GDPR's abstract norms.[148] Thus, these should be more explanatory for the Member States to enforce provisions securely for the individual's best interests.

Chapter 4 | Why are the current security mechanisms implemented in the genetic data processing context deemed inadequate to achieve utmost security for genetic data processing?

After examining the Portuguese Resolution, it was concluded that there was an insufficiency of technical and organisational measures implemented in BH, resulting in compromised patients' health records, including genetic data. Now, the focus should be on developing the current security mechanisms used in such institutions, according to GDPR, and why they fall short of protecting genetic data.

The particularity regarding hospitals is that, while in other organisations, health records are usually restricted to a limited department where cybersecurity measures can be centralised, in a healthcare setting, the data is susceptible and yet handled by almost all departments.[149]

---

[146] Principle of Technological Neutrality embedded in Recital 15 GDPR

[147] Kuner C., A. Bygrave L. and Docksey C, *The EU General Data Protection Regulation (GDPR): A Commentary*, (1st edn, Oxford University Press, 2020) 636

[148] Slokenberga S, Tzortzatou O and Reichel J, *GDPR and Biobanking* (2021) Volume 43, <https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/46125/2021_Book_GDPRAndBiobanking.pdf?sequence=1&isAllowed=y> 347-354

[149] Salem T Argaw and others (n137) 2

Furthermore, cybersecurity in the healthcare setting is unique due to the sensitive information at risk and the consequences for patients' security. When dealing with genetic information, this data carries the potential to re-identify the data subject. In addition, patients cannot change their genetic information in their health records after a data breach. As recognised by Pormeister, the difference is that the dimension of risk associated with genetic data is considerably higher in terms of different categories of sensitive data.[150] Namely, since genetic data provides scientific, medical and personal information relevant throughout the life of an individual, as well as includes the potential to reveal information on blood relatives.[151] Hence, this urgency to implement appropriate security mechanisms to protect genetic data will set the ground for analysing the current techniques.

In this vein, Article 32 of the GDPR explicitly gives all the margin of discretion to controllers and processors in each Member State to identify the specific risks of a situation, assess the impact according to the circumstance of the processing, and implement 'appropriate' measures to mitigate those risks.[152] There is no 'one size fits all' solution to information security[153], which might weaken enforcement, as it relies solely on the controller to make reasonable decisions about achieving proportionate protection of the rights and freedoms of data subjects in practice.[154] Hence, the role of data protection authorities is lowered, as their supervisory task is confined to developing guidelines on impact assessments and other accountability tools, developing enforcement procedures, and focusing on compliance and enforcement in situations of greater risk.[155] At the same time, the GDPR enhances the application of the accountability principle through DPIAs[156] and notifications of breaches by data controllers.[157]

---

[150] Kärt Pormeister (n6) 1

[151] Article 29 Working Party, 'Opinion on Genetic Data' (2004) 9 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/ files/2004/wp91_en.pdf> 4

[152] Kuner C., A. Bygrave L., and Docksey C (n147) 635

[153] Bird and Bird, 'Guide to the General Data Protection Regulation (GDPR)' [2019] Guide to the General Data Protection Regulation n/a 158-159 <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/> accessed 1 May 2022

[154] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502, 504

[155] Maria Eduarda Gonçalves, 'The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward' (2017) 26 Information and Communications Technology Law 90 <https://doi.org/10.1080/13600834.2017.1295838>, 91

[156] Article 35 GDPR

[157] Article 33 GDPR

Moreover, Article 32 of the GDPR outlines technical and organisational measures which must, whenever possible, be adopted by the data controllers: pseudonymisation and data encryption[158]; and the development of systems to test 'the effectiveness of security and confidentiality measures'.[159] Pseudonymised data is personal data which cannot be attributed to a specific data subject without the use of additional information, which is kept separately and is subject to technical and organisational measures to guarantee data is not de-identified.[160] Encryption is usually used to achieve this, turning personal data into an encrypted form, making it unusable by anyone who does not have the key. In general, the stronger the de-identification technique, the greater the loss of data utility and the more challenging it is to implement effectively.[161]

In the healthcare domain, encryption is helpful to protect patients' sensitive information in their health records. In addition, it helps separate the medical facts from the patient's identity, potentially allowing medical research to develop.[162] To protect sensitive data, almost all private companies and public initiatives now use encryption and secure data platforms, such as Estonia's Keyless Signature Infrastructure (KSI) blockchain technology.[163]

Nevertheless, encryption has certain limitations when it comes to genetic data. Firstly, encryption systems are subject to failure after some time, while genomic data has value throughout one's life, even post-mortem.[164] Encrypted data is only considered confidential if the cost of decryption by the adversary is higher than the value of the data after successful decryption. It is not the case with genomic data, which is immutable, and the tendency is that its value will increase over time with new sequencing technology available. Thereby, the lifetime of genetic data is much longer than the lifetime of a cryptographic algorithm.[165]

---

[158] Both enshrined in article 32 (1) (a) GDPR

[159] Article 32 (1) (d) GDPR

[160] Article 4 (5) GDPR

[161] Mike Hintze, 'Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency', (2018) 8 International Data Privacy Law 86, 87

[162] ENISA, 'Data Pseudonymisation Techniques: Advanced Techniques & Technical Analysis of Cybersecurity Measures in Data' (2021) <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases> 27

[163] For further detail on what KSI blockchain entails: e-Estonia, 'KSI Blochain' <KSI Blockchain - e-Estonia> accessed 20 March 2022

[164] Thomas Finnegan, Alison Hall and Jeffrey M Skopek (n142) 20

[165] Muhammad Naveed (n21) 3

Secondly, encryption makes it difficult to deal with genetic data due to the loss of utility in encrypted form to improve healthcare and research. Genetic data provides valuable information, and, especially when human life is at stake, it can be delicate to apply encryption.[166] In addition, computing and data storage needs are problematic.[167] Whenever computation is done, for instance, for medical genetic testing on a sequenced genome, the data must be decrypted, making it vulnerable to leaks.[168] Similarly, when genetic data is stored, a user will likely decrypt it for easier access instead of constantly re-encrypting it.[169]

Finally, given the challenge in assessing the risk of re-identifiability, pseudonymisation is difficult to attain in a healthcare environment where cross-referencing datasets might link the data to a patient.[170] Hence, encryption techniques may not be enough to secure genetic data. That is why security controls have been applied along with pseudonymisation, such as methods of suppressing or sampling data, and more sophisticated techniques, such as k-anonymity.[171]

Furthermore, relying on anonymisation techniques to secure genetic data is challenging. As the WP29 stressed, 'anonymisation results from processing personal data to prevent identification irreversibly'.[172] This Opinion further analyses the limitations of anonymisation techniques, referring to an example of genetic data, which can be further linked to the individual even without identifiers directly related to the data subject.[173] Hence, anonymity becomes impossible to guarantee as a linkage between datasets becomes easier.[174]

The inadequacy of genomic data to be anonymised is due mainly to its re-identification potential. Firstly, the genome provides detailed information that facilitates the re-identification of the data subject.[175] Means of re-identification, such as DNA fingerprint and DNA profiling, set the

---

[166] Naveed M and others, 'Privacy in the Genomic Era HHS Public Access' (2015) 48 ACM Comput Surv 1 <nihms691226.pdf> 3

[167] Thomas Finnegan, Alison Hall and Jeffrey M Skopek (n142) 20

[168] Dario Gil, 'How to Preserve the Privacy of Your Genomic Data' (Scientific American, 9 November 2020) <How to Preserve the Privacy of Your Genomic Data - Scientific American> accessed 20 June 2022

[169] Global Alliance for Genomics and Health, 'Crypt4GH: A secure method for sharing human genetic data' <Crypt4GH: A secure method for sharing human genetic data (ga4gh.org)> accessed 1 November 2021

[170] Mahsa Shabani and Luca Marelli (n10) 3

[171] Hintze (n 161) 87. See also for further discussion on k-anonymity method: Sweeney L, 'K-Anonymity: A Model for Protecting Privacy' (2002) 10 International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 557

[172] Article 29 Working Party, 'Opinion 05/2014 on Anonymization Techniques' (2014) < xxxx/xx/EN (europa.eu)> 6

[173] *Ibid* 10

[174] Marcello Ienca and others (n1) 3

[175] Dara Hallinan, 'Testing the GDPR in Relation to Biobanking' (2021) 2 Protecting Genetic Privacy in Biobanking through Data Protection Law 159 Chapter 7 144

ground for genomic data to provide a unique identifier of a person; thus, associated information will qualify as identifiable.[176] Secondly, if at an earlier stage, anonymisation may seem possible, remaining anonymous throughout the period during which genetic data is stored or processed is not. WP29 argued that when discussing the possibility of remaining anonymous, the 'possibility for technological development during the processing' should be considered.[177] In the case of genetic data, it is difficult to predict the technological and scientific developments that will happen; thus, ongoing anonymity remains a mere ideology.[178]

Moreover, anonymisation falls short of securing genetic data, as the re-identification risks cannot be sufficiently mitigated while maintaining a genetic dataset's utility for clinical use and research.[179] Thus, processing genetic data in an anonymised state – not subject to technical and organisational safeguards – will increase the circulation of this data in an open-access model, which may ultimately re-identify the individual and thus de-anonymise the dataset.[180]

One author worth mentioning in this regard is Erlich. He aims to identify general gaps in genetic privacy. His article "Identifying personal genomes by surname inference" initiated a vital debate regarding how it is possible to derive surnames from genomic sequencing data and, thus, identify individuals through surnames.[181] Erlich argues that genetic datasets are not likely to anonymise fully and are also not desirable. It is essential to share genetic information to identify genetic variants and, thus, prevent or provide information on the development of genetic disorders.[182] Hence, genomic data requires re-evaluating current medical confidentiality and privacy standards.[183] Erlich notes that privacy is context-dependent, which is why it is so hard to attain. Therefore, this author argues that a trust-centric framework must be built, with appropriate communication of the risks that data might be identifiable, and that a contract will help reduce this

[176] *Ibid* 144

[177] Article 29 Working Party, 'Opinion 4/ 2007 on the concept of personal data' (Policy, 01248/ 07/ EN WP 136, 2007) 15

[178] Dara Hallinan (n175) 145

[179] Agencia Española de Protección de Dados, '10 Misunderstandings Related to Anonymisation' (2021) <21-04-27_aepd-edps_anonymisation_en_5.pdf (europa.eu)> 4

[180] Mahsa Shabani and Luca Marelli (n10) 4

[181] WF Marzluff and others, 'Identifying Personal Genomes by Surname Inference' (2013) 321 Science Vol. 339

[182] Yaniv Erlich, 'Personal Genomes: Accessing, Sharing and Interpretation Conference' (11-12 April 2019) Wellcome Genome Campus Advanced Courses and Scientific Conferences <Personal Genomes: Accessing, Sharing and Interpretation — 20190411 – Wellcome Connecting Science courses and conferences> accessed 15 may 2022

[183] Dov Greenbaum, Jiang Du and Mark Gerstein, 'Genomic Anonymity: Have We Already Lost It?' (2008) 8 American Journal of Bioethics 71-74, 74

risk, with proper sanctions if re-identification occurs.[184] Therefore, because anonymisation is impossible, the focus should be on imposing stringent data protection around genomic data.

Although Article 32 provides three approaches to secure data processing, it allows the possibility that they may be insufficient to ensure security and confidentiality in specific circumstances which are for controllers to evaluate. However, the measures required in practice are unclear, even though sensitive data requires more security.[185] Thus, scholars argue for an improved governance model that ensures secure transmission, linkage and storage of data, especially concerning genetic data.[186] Importance should be given to using a system that limits access to the data, such as access control systems, on a need-to-know basis, authentication mechanisms, and legal sanctions.[187] In addition, regular backups and audits, as well as updating software, are essential to ensure that security patches are in place and, thus, avoid security breaches.[188]

Regarding governance, there have been suggestions for preventing the mishandling of genetic data in medical records. One example is the private storage of data by patients. Shabani suggested this approach as one way to circumvent the problems related to storing raw genetic data from patients in health records.[189] It would decrease unintended access by third parties while addressing infrastructure and storage cost issues that could significantly overload and reduce the efficiency of healthcare providers.[190] Moreover, it would be coherent with the EU's ambitions to give patients more control over their data. Hence, patients would better understand responsibilities and concerns by having control of their medical data, which could lead to better policies.[191] Models in which patients own their data and share rights are being implemented in Germany, the UK and

[184] Yaniv Erlich (n182)

[185] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information and Communications Technology Law 65-98 <https://doi.org/10.1080/13600834.2019.1573501> 88

[186] Susan MC Gibbons and Jane Kaye (n39) 203

[187] Thomas Finnegan, Hall and Skopek (n142) 36

[188] Lynne Coventry and Dawn Branley, 'Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward' (2018) 113 Maturitas 48 <https://doi.org/10.1016/j.maturitas.2018.04.008> 50

[189] Mahsa Shabani, Danya Vears and Pascal Borry, 'Raw Genomic Data: Storage, Access, and Sharing' (2018) 34 Trends in Genetics 8 <http://dx.doi.org/10.1016/j.tig.2017.10.004>

[190] *Ibid* 1

[191] Mohit Aggarwal, 'Towards Medical Data Ownership by Patients : Implications , Challenges and Solutions' (2018) Msc Health Informatics 33 <TCD-SCSS-DISSERTATION-2018-056.pdf> accessed 1 April 2022

Switzerland.[192] Currently, this model - Healthbank - is the first people-owned health data exchange platform, on which it is up to users to collect and allow the sharing of data and stop the sharing at any time.[193]

Nevertheless, as Koops underlined, the data subject's control over their data is a 'fallacy', especially concerning the public sector. In the public sector, the grounds to process usually rely on legal obligations or public interest; thus, consent does not play a significant part in maintaining records.[194] Similarly, when facing a specific medical situation, the interest of public health can outweigh consent, for example, in the pandemic situation where people were identified against their will in the interest of public health.[195] Moreover, private storage requires a certain level of patient awareness and competence about the implications of long-term genetic data storage. Hence, if they do not have proper understanding and training, it can lead to further gaps in the development of healthcare delivery and even worsen security and privacy concerns.[196] If private storage is seen as too demanding for patients, another option would be for health clinics to provide more transparent data storage and access policies for patients, increasing their trust relationship.

Another strategy could be implementing voluntary participation through an *opt-in* or *opt-out* regime, increasing patients' trust in the confidentiality and usage of their data. The latter regime has already been implemented in the Member States, such as Austria, Denmark, and Finland, providing patients with some control over their data.[197] For instance, in an *opt-out* scheme, patients can opt-out of their data being shared for purposes other than their care. However, even this control has constraints. For example, if the person concerned decides to opt out of the system, e.g. due to state access to personal patient data, it could harm this person by reducing the quality of care

[192] For further information see also health bank coop, <Healthbank - Control Your Health Data> accessed 15 May 2022
[193] *Ibid*
[194] Koops (n91) 253
[195] Karl Stoeger and Martina Schmidhuber, 'The Use of Data from Electronic Health Records in Times of a Pandemic-a Legal and Ethical Assessment' (2020) 7 Journal of Law and the Biosciences 1, 7
[196] Mohit Aggarwal (n 191) 47
[197] Karl Stoeger and Martina Schmidhuber (n195) 2

provided.[198] Furthermore, it could impact the patient's biological relatives, who would be deprived of a potential organ donation by the person who decided to opt out.[199]

Lastly, synthetic data in healthcare should be discussed as a current innovative mechanism. Synthetic data means data is generated artificially; thus, actual patient data is not used. It is a promising mechanism as it mitigates the problem of data paucity when there is not enough data available to be analysed. Furthermore, it protects the privacy and confidentiality of authentic data since it cannot be traced back to the individual.[200] Thus, it would be considered anonymised data.[201]

However, because this mechanism is still in its infancy, current models may not be ready to generate synthetic data. They may lead to vulnerabilities in the system, such as information leakage.[202] Thus, more extensive and sophisticated security measures, such as differential privacy and increasing expertise in the field, need to be adopted. Furthermore, it is still unclear how the GDPR will apply to synthetic data due to the challenge of categorizing it as anonymized or pseudonymised.[203] Notably, the more a synthetic dataset resembles actual data, the more valuable it will be for analysts, but the more it will reveal about real people. Consequently, the potential risk of re-identification increases.[204] If this is the case, synthetic data should be qualified as pseudonymised, to which the GDPR applies.[205]

Further developments or suggestions remain regarding the security of genetic data. There are still several challenges health clinics face when complying with the GDPR, especially with the emergence of digital health records. The interoperability of records provides multiple potential access gateways and makes a health record more complete and, thus, more valuable for possible attacks.[206] Even though health records could be accessed previously, they were stored in paper

---

[198] *Ibid* 6

[199] Organ Donation Taskforce, 'The Potential Impact of an Opt-out System for Organ Donation in the UK. An Independent Report from the Organ Donation Taskforce' (2008) 36 Journal of medical ethics 1 <http://www.ncbi.nlm.nih.gov/pubmed/20817820> 34

[200] Anmol Arora and Ananya Arora, 'Synthetic Patient Data in Health Care: A Widening Legal Loophole' (The Lancet, 28 March 2022) 399 <http://dx.doi.org/10.1016/S0140-6736(22)00232-X> accessed 15 May 2022

[201] Recital 26 GDPR

[202] Richard J Chen and others, 'Synthetic Data in Machine Learning for Medicine and Healthcare' (2021) 5 Nature Biomedical Engineering 493 <http://dx.doi.org/10.1038/s41551-021-00751-8> 494

[203] *Ibid* 495-496

[204] European Data Protection Supervisor, 'Synthetic Data' <Synthetic Data | European Data Protection Supervisor (europa.eu)> accessed 15 June 2022

[205] Article 4 (5) GDPR

[206] Lynne Coventry and Dawn Branley (n188) 48

files, which meant that only physical breaches could occur, decreasing the number of potential violations.

Hospitals still lack investment in cybersecurity due to public financing constraints, high *compliance* costs, and a lack of healthcare organisation management.[207] Even with 30% of all data breaches impacting the healthcare sector, less than 11% of Hospital IT teams argue that cybersecurity is a high priority.[208] Notably, the infrastructure needs to be ready to handle EHRs, which are costly and challenging to implement. In addition, inadequate staff training may result in internal data breaches, leading to over-the-top financial losses for healthcare organisations.[209]

Notwithstanding having adopted a common framework regarding personal data protection, the perception of personal data still varies across the Member States. Some are stricter than others when implementing security measures. Thus, Member States must alter their mindset to see data protection in the health sector from the same perspective for the patients' benefit and increase their trust in healthcare systems. In this context, the EDPB plays a vital role in clarifying the GDPR norms through opinions and (binding) decisions and ensures consistent enforcement practices at the national level.[210]

Nonetheless, until this mindset is achieved, it will be challenging to implement very sophisticated and complex measures if the protection core is still dismissed. With that in mind, it is time to consider alternative governance models and their feasibility to promote security of genetic data, such as the federated infrastructure for genetic data and the EHDS proposal. As will be shown, these initiatives have the most laudable aim to achieve the same level of data protection across the Member States and improve healthcare. However, it remains to be seen if these goals align with the different levels of maturity among Member States' health systems.

---

[207] ENISA, 'Cloud Security for Healthcare Services' (2021) <*ENISA Report - Cloud Security for Healthcare Services.pdf> 16

[208] Ipsos, 'Perspectives in Healthcare Security' (CyberMDX, updated on 9 September 2021) <Perspectives in Healthcare Security Ipsos Report | CyberMDX> accessed 10 May 2022

[209] Bocong Yuan and Jiannan Li, 'The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation' (2019) 16 International Journal of Environmental Research and Public Health 5

[210] Articles 64 and 65 (respectively, opinions and binding decisions) and article 70(1)(t) GDPR

Chapter 5 | To what extent might alternative governance models, namely the EU Federated Database and the EHDS proposal, improve the protection of genetic data?

After examining the shortcomings of current security mechanisms to protect genetic privacy, the focus will be on analysing alternative governance models that could better preserve genetic data. Across all Member States' organisations, databases that store or analyse genetic data must be protected against security breaches. However, as discussed, a large proportion of breaches in healthcare still occur due to human error, which means there needs to be a combination of a robust digital infrastructure with training on cybersecurity and other measures.[211] When implemented, strong technical measures guarantee data quality, integrity, and security, allowing their secure usage and storage.[212]

In this vein, there have been recent initiatives to develop healthcare in the EU and promote digital health. For instance, the European Commission proposed a federated database for genomic data in November last year. This initiative aims to develop an interoperable and secure federated infrastructure to be used in genetic datasets, supported by advanced IT tools, such as blockchain and AI, for improving health research and clinical practice.[213]

A federated database is a decentralised approach in which data is stored locally and prevents unauthorised access by making all datasets anonymous.[214] However, as discussed in the previous chapter, genetic anonymisation is hardly attainable. Moreover, genomic data is continuously evolving, and a large amount of information is increasingly available in databases. It will also mean the federated approach will require time and financial investment, and it will need to provide a scalable infrastructure to keep up with the increasing volume and complexity of data.[215] Accordingly, the deployment of federated networks will require the development of current governance frameworks.[216] As a decentralised infrastructure, coordination is done in a

[211] Williams G and others (n5) 17
[212] Marcello Ienca and others (n1) 9
[213] European Commission, 'Digital Europe Programme (DIGITAL) Call for Proposals' (2021) Cloud Data and TEF 1, 34
[214] Muilu and others (n42) 722
[215] *Ibid* 723
[216] Harry Hallock and others, 'Federated Networks for Distributed Analysis of Health Data' (2021) 9 Frontiers in Public Health 6

more distributed way, with direct communication between end-users, increasing their autonomy.[217]

Furthermore, this model promotes data security since the data analysis is done locally by bringing the algorithm to the data.[218] This model will help fulfil the data minimisation principle[219] since this infrastructure avoids data aggregation in a centralised model. Nevertheless, the distributed analysis will require expertise in medical and data analytical fields, which seems challenging when dealing with medical data.[220]

Moreover, it is still unclear how the legal framework, mainly the GDPR, will apply to this initiative regarding *compliance* with legal and regulatory obligations.[221] For instance, a federated database using AI/ML algorithms has limited transparency on how the algorithm works.[222] Hence, in this infrastructure, it is difficult to transparently execute the training operations and provide adequate information to the data subject on how their data is being processed.[223] It will affect the capacity of the controller to adequately perform a DPIA and validate the infrastructure's *compliance* with the GDPR.[224] The DPIA and document processing operations[225] are critical assessments embedded in the accountability principle[226], especially when processing genetic data. Nevertheless, the lack of transparency prevents DPAs from comprehensively inspecting covert operations in this infrastructure.[227] Accordingly, it will be difficult for the DPAs to identify a breach of the GDPR, avoid risky processing operations, and propose better security measures.[228]

As it stands, the Call does not cover this transparency issue of the federated infrastructure. It merely states it should 'provide a federated network of connected genomic databases, deploying

---

[217] Primavera De Filippi, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) Alternativ Journal of Peer Production 1 <https://hal.archives-ouvertes.fr/hal-01382006> 5

[218] FM Aarestrup and others, 'Towards a European Health Research and Innovation Cloud (HRIC)' (2020) 12 Genome Medicine 1, 9

[219] Recital 39 and Article 5(1) (c) GDPR

[220] Aarestrup and others (n218) 10

[221] Harry Hallock and others (n216) 5

[222] Nguyen Truong and others, 'Privacy Preservation in Federated Learning: An Insightful Survey from the GDPR Perspective' (2021) 110 Computers and Security 102402 <https://doi.org/10.1016/j.cose.2021.102402> accessed 15 June 2022 15

[223] Recital 39, Article 5 (1) (a) and Article 12 GDPR

[224] Article 35 GDPR

[225] Article 30 and Article 35 (3) (b) GDPR

[226] Article 5 (2) GDPR

[227] Nguyen Truong and others (n222) 18

[228] *Ibid* 18

trust mechanisms with security and privacy by design'.[229] However, it fails to specify how it expects to achieve security. For instance, a federated database will require that security mechanisms be implemented in end-users' nodes (locally)[230] to fulfil the integrity, confidentiality, and security principle.[231] However, healthcare organisations may have variations in IT infrastructures and security policies, increasing fragmentation.[232] It could be solved by integrating existing infrastructures and cybersecurity policies across healthcare institutions. Thus, the risk of different levels of cybersecurity at each node could be mitigated.[233] Nevertheless, as presented in a study report[234], there is still a long way to go; currently, only 5 Member States have cybersecurity policies implemented in their healthcare organisations – Spain, Sweden, Finland, Cyprus, and Belgium.

Furthermore, genomic data in this database could be better protected using privacy-preserving measures such as differential privacy and homomorphic encryption.[235] Encryption before accessing data may also be needed.[236] Again, the Call does not address these concerns. It merely refers to Article 12 of the Digital Europe Programme,[237] which states that activities must comply with 'applicable security rules' in Union and national law and include a self-security assessment to identify how *compliance* with the law will be achieved.[238] Therefore, the Call aims to raise a dialogue with stakeholders and encourage their autonomy in coming up with innovations/techniques in the field of genomic data.

Nonetheless, due to the sensitivity of this Call's topic, it would be better if the proposal provided more clarity on how this *compliance* would be best accomplished. A self-assessment

[229] European Commission, 'Digital Europe Programme (DIGITAL) Call for Proposals' (2021) Cloud Data and TEF 1, 35
[230] Nguyen Truong and others (n222) 16
[231] Article 5 (1) (f) and Article 32 GDPR
[232] Harry Hallock and others (n216) 5
[233] *Ibid* 5
[234] European Commission, 'Study on eHealth, 'Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union, Lot. 1 – Interoperability of Electronic Health Records in the EU' (2020) Final Country FactSheets <Artificial Intelligence in Healthcare report | Shaping Europe's digital future (europa.eu)>
[235] Nguyen Truong and others (n 222) 18
[236] Harry Hallock and others (n 216) 3
[237] European Commission, Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance) <EUR-Lex - 32021R0694 - EN - EUR-Lex (europa.eu)>
[238] *Ibid* Article 12 (2)

without legal guidance might make it easier for the applicants to circumvent *compliance* with the GDPR, especially considering stakeholders' different levels of technical expertise.

Moreover, the federated infrastructure will use advanced IT tools, including machine learning (ML) and blockchain, whenever adequate to secure access to and distributed analysis of complex datasets.[239] Hence, deploying these techniques, even though they might increase interoperability and efficiencies in healthcare delivery, creates an opportunity for data breaches to occur, making patients' data more vulnerable.[240] Especially with blockchain, it can significantly impact security as it raises the question of who controls the data and, thus, is accountable for it. According to the GDPR, the controller is required to determine the purposes and means of the processing[241] and is liable for activities processed on his behalf.[242] In the context of a distributed infrastructure, however, it is arguable whether the controller exists or has the same responsibilities since the data is stored on the blockchain.[243] Thus, liability issues may arise with blockchain platforms since they work without an intermediary and trust is placed on the network rather than a third party. It can be problematic because it is not clear who is liable in case of a data breach.[244]

Lastly, blockchain may also raise concerns regarding data storage and purpose limitations.[245] One of the design features of blockchain is that transaction records cannot be changed or deleted.[246] Hence, the data subject's right to have their data erased[247] in the blockchain is infeasible as the system is designed to prevent it.[248] Accordingly, data is maintained on every network node and is publicly accessible, irrespective of the original collection and processing purpose. This can be problematic in the case of a data breach, especially for genetic data, as its value tends to increase with time and, once disclosed, cannot be retrieved.[249] Therefore, it

[239] European Commission, 'Digital Europe Programme (DIGITAL) Call for Proposals' (2021) Cloud Data and TEF 1, 34

[240] Towards European Health Data Space (TEHDAS), 'Why health is a special case for data governance', 23 June 2021, <Joint Action Towards the European Health Data Space – TEHDAS - Tehdas> 18

[241] Article 24 (1) and 25 (1) GDPR

[242] Recital 74 and Article 5 (2) GDPR

[243] Robert Herian, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation and Technology 156, 9

[244] Mahsa Shabani (n40) 2

[245] Article 5 (1) (b) and (e) GDPR

[246] Herian (n243) 13

[247] Article 17 GDPR

[248] Herian (n243) 13

[249] Muhammad Naveed (n21) 3

reinforces the need to find adequate expertise to assist the controller in securing these technological advances in the context of large-scale processing of genetic data.[250] Also, the concerns posed with this infrastructure – security, data storage and purpose limitation, transparency and accountability – should be handled before it is implemented.

Aligned with the initiative discussed, attention should be given to the EHDS Proposal launched at the beginning of May this year.[251] This proposal aims to digitise health records across the EU to increase interoperability between healthcare institutions. It is a laudable goal in the context of healthcare. EHRs allow structured medical data to be shared between authorised health professionals to improve healthcare delivery at a low cost.[252] Nevertheless, their implementation will require significant investments in technology and infrastructure changes in healthcare institutions.[253] The proposal also established a cross-border infrastructure for primary care (MyHealth@EU).[254] In addition, it designates a digital health authority for each Member State[255] in charge of ensuring *compliance* with the immediate use of electronic health data provisions; and health data access bodies[256] for secondary use purposes. The idea is that a central health data entity at the EU level provides standards and national health data entities implement them. The data permit authority in Finland's social and healthcare sector is an essential reference for how these federal entities may work successfully (Findata).[257]

Importantly, EHDS complements the GDPR, proposing a uniform and consistent health data-specific legal framework.[258] EHDS, together with the rights enshrined in the GDPR, will aim to give the data subject greater control over their health data. For instance, to be able to easily

[250] Recital 97 GDPR

[251] EHDS Proposal

[252] José Luis Fernández-Alemán and others, 'Security and Privacy in Electronic Health Records: A Systematic Literature Review' (2013) 46 Journal of Biomedical Informatics 541, 559 <http://dx.doi.org/10.1016/j.jbi.2012.12.003>

[253] Sima Ajami and Razieh ArabChadegani, 'Barriers to Implement Electronic Health Records (EHRs)' (2013) 25 Materia Socio Medica 213, 213

[254] Recital 24 EHDS Proposal

[255] Article 10 EHDS Proposal

[256] Recital 42 and Article 36 EHDS Proposal

[257] DigitalEurope, 'DigitalEurope's recommendations for the European Health Data Space' (DigitalEurope, 3 February 2021) <DIGITALEUROPE's recommendations for the European Health Data Space - DIGITALEUROPE> accessed 15 May 2022; FinData, 'Findata has issued a regulation on the requirements of secure operating environments' (Findata, 27 October 2020) <Findata has issued a regulation on the requirements of secure operating environments - Findata> accessed 15 May 2022

[258] EHDS Proposal 8

access their data in an electronic form and share it with health professionals across the EU[259], promoting their right of access[260] and data portability.[261] Moreover, the data subject will be able to add information and rectify errors in their electronic health data[262], according to the right of rectification[263], and restrict healthcare professionals' access.[264] It is essential to note that the proposal recognises the lack of harmonisation between the Member States regarding Article 9(4) GDPR, which allows the Member States to maintain or introduce further conditions on the processing of sensitive data, as discussed previously. Accordingly, the proposal aims to build the capacity of Member States to strengthen digital health systems through sharing best practices and expertise.[265]

Nevertheless, using EHRs can raise security concerns and lead to further data breaches when security tools are not implemented effectively. Thus, the proposal introduces criteria for interoperability and security of EHRs systems and requires self-certification by manufacturers.[266] Like the GDPR[267], the EHDS establishes that data must be processed in secure environments provided by health data access bodies, with adequate security measures in place.[268] However, there are still different standards and regulations used in EHR systems, so harmonisation is required to ensure compliance. In addition, healthcare professionals' training in security and privacy, especially when handling digital records, should not be underestimated.[269]

Interestingly, one week before the EHDS proposal came into place, an attack occurred on a hospital system in Portugal.[270] It brought down the computer network and prevented the consultation and updating of patients' medical records, which, in many cases, had to be done manually. Due to this attack, the hospital has been without access to users' clinical data. This lack

[259] *Ibid* Recital 11
[260] Article 15 GDPR
[261] Recital 68 and Article 20 GDPR
[262] Recital 10 EHDS Proposal
[263] Article 16 and Recital 65 GDPR
[264] Article 5 (1) (c) GDPR
[265] Article 59 EHDS Proposal
[266] *Ibid* Recital 27
[267] Article 32 GDPR 'Security of Processing'
[268] Article 50 EHDS Proposal
[269] Fernández-Alemán and others (n252) 559
[270] SIC Notícias, 'Ataque informático ao Garcia de Orta: hospital está sem acesso a dados clínicos há 3 semanas' (SIC Notícias, 17 Maio 2022) available in portuguese only <Ataque informático ao Garcia de Orta: hospital está sem acesso a dados clínicos há 3 semanas - SIC Notícias (sicnoticias.pt)> accessed 15 May 2022

of access to the system puts users' healthcare and clinicians' safety at risk.[271] Surprisingly, due to a lack of digital records management, all digital health records were hacked, with only paper files not affected by the attack.

Therefore, it is arguable that security breaches like these are likely to happen when the Member States try to keep pace with new technological advances, such as the digitisation of records, without security and privacy standards having been effectively implemented in healthcare institutions. The consequences are the increasing undermining of patients' privacy and further distrust in healthcare delivery across the Member States, not only from patients but also from clinicians who do not fully understand the impact of these technologies or how to implement them.

Furthermore, the proposal recognises that protective measures must be proportional to the risk of re-identification and consider the particularities of different data categories and techniques.[272] However, it fragments the framework by leaving the clarification of the adequate measures to a delegated act which is not yet in place. Moreover, the proposal, as it stands, does not address security gaps and further contributes to the lack of harmonisation across Member States. It is even more problematic concerning genetic data, which, in Article 19, states that it should become more easily accessible in an electronic format. However, without adequate security strategies, it may lead to the de-anonymisation of genetic datasets.[273] Hence, the concerns raised – different levels of maturity among Member States' health systems, lack of harmonisation among EHRs systems, and the legal uncertainty on adequate protective measures – need to be addressed before the proposal can be implemented.

The two initiatives discussed provide immense opportunities for improving healthcare delivery, but the question is whether healthcare providers are ready to implement them. First, the focus should be on building a trust-centric environment and ensuring clinicians are involved in these projects. While healthcare is becoming more complex, these new initiatives provide valuable outcomes with the proper awareness and training.[274] Moreover, these initiatives raise the question: Are they too progressive for now?

---

[271] *Ibid*

[272] Recital 64 EHDS Proposal

[273] Marelli, Lievevrouw and Van Hoyweghen (n59) 450

[274] Rajiv Sikka, Group CIO, Medanta Hospitals, 'AI Maturity and Implementation in the Healthcare Sector' in 'Future of Healthcare: AI' (AQMEN365, 19 May 2022, 15:20-15:40) <Future Healthcare: AI (aqmen365.com)> accessed 19 May 2022

The EHDS proposal provides a vital step forward in improving interoperability in the healthcare sector and ensuring a uniform and sectoral framework.[275] To achieve that, it aims to bring Member States' infrastructure up to date and harmonise them. However, this may take some time, as the Member States have different maturity levels regarding different categories of health data and its implementation.[276] For instance, according to a survey conducted before the EHDS proposal, Portugal does not yet have legislation regarding the storage and sharing of healthcare data.[277] In contrast, Estonia has national legislation and protocols concerning storing and sharing this data. Also, while Nordic countries have more centralised mechanisms and are more efficient, others, such as Spain and Italy, are decentralised.[278] Denmark, for instance, has one of the world's most integrated patient information infrastructures due to an early approach to digitisation and high state funding.[279]

Furthermore, changing the system's infrastructure to a more digital and interoperable one is not easy; it could even be highly costly. More importantly, each country needs a mindset shift regarding the perception of personal data. One of the biggest challenges for healthcare professionals to start implementing measures is a lack of basic understanding of what is required, leading to a lack of focus.[280] It is hard to invest in something Member States do not understand, even if the initiatives from the European Commission have the most laudable aims.

In addition, despite the broad powers and competencies given to DPAs[281], these authorities lack funding, leading to gaps in the enforcement of the GDPR.[282] Notably, the vast majority of

[275] EHDS Proposal 8

[276] EHDS Proposal Recital 17

[277] European Commission, 'Study on EHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union' (2021) Lot. 2: Artificial Intelligence for health and care in the EU <https://euagenda.eu/publications/study-on-ehealth-interoperability-of-health-data-and-artificial-intelligence-for-health-and-care-in-the-european-union>130

[278] Susana Solís Pérez, 'The European Health Data Space: bridging the health data divide' in 'Summer Summit Conference' (Digital Europe, 20 June 2022, 14:20-15:05) <Summer Summit 2022 - DIGITALEUROPE> accessed 20 June 2022

[279] Sarah Wadmann, Mette Hartlev and Klaus Hoeyer, 'The Life and Death of Confidentiality: A Historical Analysis of the Flows of Patient Information' [2022] BioSocieties 3 <https://doi.org/10.1057/s41292-021-00269-x> accessed 20 April 2022

[280] Bashir Agboola, CTO, Hospital for Special Surgery, 'Implementation strategies for digital healthcare' in 'Transforming Healthcare Delivery Conference' (AQMEN365, 25 May 2022, 14:20-14:40) <Transforming Healthcare Delivery (aqmen365.com)> accessed 25 May 2022

[281] Article 55 to 58 GDPR (Chapter VI Section 2)

[282] Emma Woollacott, 'Under-Resourced Data Protection Authorities Fail to Enforce GDPR' (Forbes, 26 May 2020) <Under-Resourced Data Protection Authorities Fail To Enforce GDPR (forbes.com)> accessed 25 May 2022

DPAs argue that they do not have enough resources to carry out their tasks, including their duty to monitor and enforce the GDPR (Article 57(1) (a)).[283] [see Appendix-3] The EDPS and WP29 identified the risks posed by insufficient resources, such as the lack of capacity to address ongoing demands and acting as 'an impediment to rather than an enabler of innovation and growth.'[284] To counteract this, the Commission has taken a stand and encouraged pooling of efforts, such as joint investigation on cross-border issues, and created a pool of experts to mitigate resource constraints and increase supervisory authorities' enforcement capacities. The Commission will also take infringement action against Member States that fail to comply with their resource obligations under Article 52(4) GDPR.[285] Recently, the EDPB released a statement[286] on a coordinated enforcement framework, enabling DPAs to work together in cases of strategic importance, for instance, matters dealing with a structural problem in the various Member States.[287]

Accordingly, it is crucial to address the lack of expertise and resource constraints in DPAs; otherwise, when faced with new technological-driven initiatives, such as those discussed, to protect genetic data, there will likely be enforcement problems.[288] Given that patients' safety is the basis for providing quality and reliable healthcare delivery, only when security issues are fully addressed can digital health and other technological initiatives flourish. Otherwise, it will only lead to increasing fragmentation between the Member States and undermining patients' security.[289]

In the future, a bottom-up approach seems desirable at the EU level. However, while the focus is on moving the European Union towards technological and digital development, security remains fragile as the initiatives presented do not provide an answer on how to ensure patients' safety when deploying them. Furthermore, these initiatives would be more valuable if they considered the varying degrees of maturity in each Member State. To achieve that, presumably, the way forward would be to provide a figure with a closer link between legislation and

[283] European Data Protection Board, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' (2021) 31 <edpb_report_2021_overviewsaressourcesandenforcement_v2_0.pdf (europa.eu)> 5

[284] Sofija Voronova and Anna Nichols, 'Understanding EU Data Protection Policy' (2020) EPRS 10 <Understanding EU data protection policy | Think Tank | European Parliament (europa.eu)> accessed 15 June 2022

[285] *Ibid* 11

[286] European Data Protection Board, 'Statement on Enforcement Cooperation' 1 (EDPB, 28 April 2022) <Statement on enforcement cooperation | European Data Protection Board (europa.eu)> accessed 18 June 2022

[287] *Ibid* 1

[288] Johnny Ryan (n130) 1

[289] Bashir Agboola (n280)

implementation of the GDPR for legislation to become more adaptable. A possible suggestion would be to have a delegation from the European Commission visit each Member State to understand the capabilities and resources available to resolve the technical difficulties in the field and, thus, deploy achievable measures to protect sensitive (genetic) data. Henceforth, they could gain more insight from the people "on the ground", such as local enforcers, regulators or NGOs, and the result would be adaptable legislation in all Member States. The EDPB has been engaging in similar initiatives aiming for more consistency, including promoting practical cooperation between supervisory authorities.[290] One example is the development of task forces in essential cases, for instance, matters dealing with a novel data protection issue.[291] The task force aims to promote cooperation, sharing of best practices and resource expertise between DPAs. For instance, in September 2021, the EDPB established a cookie banner task force to exchange views on legal analysis, infringements, and **support activities on the national level**.[292] A similar task force could be developed to resolve technical difficulties and deploy adequate measures to protect genetic data at the national level, working towards enhanced harmonisation across the Member States by bridging the gap between legislation and implementation. In addition, developing NGOs focused on strategic enforcement, such as the NOYB,[293] in each Member State could encourage DPAs to engage with their responsibilities and enforce the GDPR.[294]

Furthermore, the data protection officer (DPO) is steered by DPA's concrete guidelines[295] and monitors internal compliance with the GDPR.[296] In Portugal, there has not been an interaction between DPA and DPO, which led to the possibility of creating an authority responsible for all the healthcare organisations at the Member State Level.[297] This authority could, then, encourage the

[290] Article 70 (1) (u), (v), and (w), and Recital 139 GDPR

[291] European Data Protection Board (n286) 1

[292] European Data Protection Board, 'EDPB establishes cookie banner taskforce' (EDPB, 27 September 2021) <EDPB establishes cookie banner taskforce | European Data Protection Board (europa.eu)> accessed 15 June 2022

[293] Austrian Non-Governmental Organization (NGO) focused on strategic enforcement of digital rights (particularly privacy and data protection rights) in the EU, for more information see also <NOYB enforces your right to privacy everyday> accessed 15 June 2022

[294] Ursula Pachl, 'What does effective enforcement mean?' in 'The Future of Data Protection: Effective Enforcement in the Digital World' (EDPS Conference, 16 June 2022, 10:00-11:00) <Home | EDPS Conference 2022> accessed 16 June 2022

[295] Article 39 (1) (d) and (e) GDPR

[296] Article 39 (1) (b) and Recital 97 GDPR

[297] Serviços Partilhados do Ministério da Saúde, 'Privacidade da Informação no setor da Saúde', (SPMS, 21 March 2017) available only in portuguese < *Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf> accessed 15 May 2022

drawing up of codes of conduct[298] which would help to densify the legislation. Namely, there could be a code of conduct for genetic data security to develop adequate measures for genetic data processing. Bringing up codes of conduct to clarify the GDPR's provisions is not new. For instance, in May 2021, the first pan-European sector-specific code for cloud infrastructure service providers was approved.[299] Also, at the national level, the Member States such as Italy, Norway, and Poland, are developing ministerial guidelines and codes of conduct for tailoring the application of the GDPR to the healthcare context.[300]

However, when it comes to genetic data, the focus has been on developing codes of conduct for improving genetic data sharing and for secondary/research purposes.[301] Nevertheless, a code of conduct on genetic data security densifying Article 32 is yet to be seen. It could help clarify the measures to be taken, such as developing a standard risk assessment framework for genetic data processing. In addition, it would help data controllers adopt new technologies with the appropriate design, security and privacy considerations and promote healthcare innovation.

In addition, in self-regulation, DPAs in Norway and France also propose regulatory sandboxes.[302] A regulatory sandbox is a tool shielding the testing of innovative technologies, products or services under a regulator's supervision[303] to ensure privacy by design.[304] For instance, in Norway, a regulatory sandbox was built to provide free guidance to companies on personal data protection issues while promoting the development of innovative AI solutions.[305] In this sense, regulators can better understand the impact of these innovative technologies, allowing them to

[298] Article 40 and Article 57(1) (m) GDPR

[299] CISPE.cloud, 'CISPE Code of Conduct' <https://www.codeofconduct.cloud> accessed 26 June 2022

[300] Marelli, Lievevrouw and Van Hoyweghen (n59) 459-460

[301] M. Phillips and others, 'Genomics: data sharing needs an international code of conduct' (Nature, 5 February 2020) <Genomics: data sharing needs an international code of conduct (nature.com)> accessed 15 October 2021; Molnár-Gábor, O Korbel, 'Genomic data sharing in Europe is stumbling – Could a code of conduct prevent its fall?' (EMBO Molecular Medicine,18 February 2020) <Genomic data sharing in Europe is stumbling—Could a code of conduct prevent its fall? | EMBO Molecular Medicine (embopress.org)> accessed 10 October 2021; European Commission, 'D5.2: An International Code of Conduct for Data Sharing in Genomics: A Proposal' (2021) SIENNA Project

[302] Sebastião Barros Vale, LLM, Dr. Gabriela Zanfir-Fortuna and Dr. Rob van Eijk, 'Insights into the Future of Data Protection Enforcement: Regulatory Strategies of European Data Protection Authorities for 2021-2022' (Future of Privacy Forum, July 2021) 9 <FPF-Europe-report-DPA-Strategies -from-2021-and-beyond-3-2-1.pdf> accessed 15 June 2022

[303] European Parliament, 'Artificial Intelligence Act and Regulatory Sandboxes' (EPRS, June 2022) <Artificial intelligence act and regulatory sandboxes | Think Tank | European Parliament (europa.eu)> 1

[304] Article 25 (1) GDPR

[305] For more information on Norway's sandbox see also Datatilsynet, 'Sandbox for responsible artificial intelligence', <Sandbox for responsible artificial intelligence | Datatilsynet> accessed 15 June 2022

develop adequate supervision and enforcement policies.[306] As in the case of the AI Act,[307] the EHDS would benefit from having a similar sandbox provision.[308] Moreover, it would also be helpful to use sandboxes in the federated initiative. For instance, the design and testing of the federated database could be promoted with sandboxes, allowing experimentation with governance frameworks and technologies to ensure systems are secure when deployed.[309]

Lastly, inspiration should be taken from the most advanced healthcare systems in the EU, such as the Danish. Since an early stage, digitisation of hospital records has been in place with appropriate data linkage and usage for multiple purposes.[310] Consequently, EHR systems in Denmark are fully operational and cover 99% of healthcare organisations.[311] Also, genomic data development is a significant priority for the Danish healthcare system, notably through the creation of a National Genome Centre. Furthermore, to secure sensitive genetic data, Denmark has been building up a model in which the State is entrusted with the data due to the high level of trust in the Danish government.[312]

In addition, the Danish National Genome Centre[313] has been working on a security model in which people with access to sensitive patient data would not be allowed to download, copy or erase data from the genome database, ensuring the accuracy and integrity of the data.[314] Thus, it would guarantee that a patient's genetic analysis is only available in one copy.[315] Since 1968, every Danish citizen has had a unique personal identifier (CPR number). Citizens can also obtain a security number – NEM-ID. Thus, two-factor authentication is used for logging-in to healthcare services. Health professionals can only access personal health data to treat a person.[316] In Denmark,

[306] European Parliament (n303) 2

[307] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 21 April 2021, < EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)> Articles 53-54

[308] Susana Solís Pérez (n278)

[309] European Commission, 'Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021-2022' Brussels, 10.11.2021 C(2021)7914 final 89

[310] Sarah Wadmann, Hartlev and Hoeyer (n 279) 15

[311] Study on eHealth (n234) 76

[312] The Medical Futurist, 'Where Is Digital Health Heading in Denmark?' (The Medical Futurist, 7 February 2019) <Where Is Digital Health Heading In Denmark? - The Medical Futurist> accessed 15 May 2022

[313] Danish National Genome Center <Danish National Genome Center (ngc.dk)> accessed 15 May 2022

[314] Article 5 (1) (d) and (f), and Recital 39 GDPR

[315] Danish National Genome Center

[316] Article 5(1) (c) GDPR

all activity is logged, and the log files are accessible to the citizen. Thus, patients can monitor their log files and report any irregularities. In addition, citizens receive a letter if a GP or specialist who is not carrying out any treatment on them has accessed their data.[317] Thus, in the event of unauthorised access, immediate action is taken.[318]

In contrast, in BH in Portugal, professionals had indiscriminate access to patient's data, regardless of the speciality and professional category, due to broad access credentials. In addition, the patients did not have access to the activity logs nor reported any irregularity, which could have helped in the early detection of the unauthorised access in this hospital and thus prevented the damage to sensitive data. If immediate action had been taken, for instance, reporting the unauthorised access without waiting for CNPD intervention, perhaps the breach in the hospital would not have happened, or at least not to the extent it did.

Although the reasons for the incomplete GDPR implementation in Portugal are diverse - such as the diminished culture of privacy in organisations, the lack of specialised professionals, and the passiveness of public and private entities - it is the action or inaction of the government in funding and legislation that stands out as the primary cause.[319] Hence the importance of the example of Denmark, where there is substantive State action and citizens place trust in it. By sharing best practices and measures implemented in advanced EU countries like Denmark, data breaches could be prevented, and digital transition could flourish, anchored in citizens' trust.

To conclude, the two initiatives discussed – the federated database and the EHDS proposal – are promising alternative governance models for securing genetic data. However, as highlighted, they may be ambitious for now due to security not being fully operational. Nevertheless, solutions were suggested to address these concerns and advance in the EU so that Member States look at data protection in the health sector from the same perspective.

Chapter 6 | Conclusion

Nowadays, much investment has been made in developing big data in healthcare through adopting EHRs and the widespread storage and sharing of genetic data. However, the same

[317] Christian Nøhr and others, 'Nationwide Citizen Access to Their Health Data: Analysing and Comparing Experiences in Denmark, Estonia and Australia' (2017) 17 BMC Health Services Research 1, 7
[318] Article 5(1) (f), Recital 39 and Article 34 GDPR
[319] Diogo Duarte (n117)

investment has not been made in protecting this data.[320] Especially when sensitive personal information is concerned, and many data subjects are being monitored, security measures must be set to avoid data breaches. Therefore, it appears questionable whether the GDPR promotes patient information security when handled in these large databases without impeding innovation.[321]

In this vein, this thesis highlighted the particularities with genetic data, such as the high risk of identifiability, the difficulties presented with anonymisation and the relational nature of many genomic data providing detailed information on data subjects and relatives. However, even though recognised in the WP29/EDPB guidelines and other documents, insufficient attention to unique features of genetic data can be considered one of the principal vulnerabilities of the GDPR. Thus, it reflects on the security provisions, notably Article 32 GDPR, which do not address security measures adequate to the risk of processing genetic data.[322] This set the ground for an analysis of the current security mechanisms.

Moreover, this thesis analysed a Portuguese Resolution[323] in which there was illegitimate access to patients' records, including genetics. The breach occurred due to the insufficiency of measures implemented in Barreiro Hospital. Although Article 32 provides a set of approaches for securing data processing[324], it allows the possibility that they may be insufficient to ensure security and confidentiality in specific circumstances. Hence, this thesis argued that this is the case with genetic data due to its value increasing over time and high risk of identifiability, enabling linkage between datasets. Furthermore, even though Article 32 recognises other 'appropriate measures' might be applicable, it does not provide concrete guidelines on what these may be.[325] Accordingly, this thesis argued the need for improving GDPR enforcement by addressing this Resolution.

---

[320] Suzanne Vergnolle, 'A quest for resource: efficient enforcement through innovation' in 'The Future of Data Protection: Effective Enforcement in the Digital World' (EDPS Conference, 17 June 2022, 13:30-14:30) <Home | EDPS Conference 2022> accessed 17 June 2022

[321] Jane Kaye (n7) 423

[322] Article 32 GDPR

[323] Portuguese Resolution n.º 984/2018

[324] Namely, the pseudonymization and encryption of personal data (Article 32(1)(a)); the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems (Article 32(1)(b)); the ability to restore the availability and access to personal data in a timely manner in case of an incident (Article 32(1)(c), for example by setting up a disaster recovery plan); and a process for regularly testing, assessing and evaluating the effectiveness of security measures (Article 32(1)(d))

[325] Recital 71 second paragraph GDPR

Therefore, this thesis explored how innovative governance structures could better serve genetic data. Thus, two recent initiatives were analysed: a federated infrastructure for genetic datasets and the EHDS proposal. Furthermore, the interplay between these initiatives and the GDPR was examined, as the feasibility of implementing them. However, a common problem was identified – the lack of security safeguards embedded in the texts of the proposals. Thus, this thesis argued that these initiatives might be too ambitious for now.

Lastly, suggestions were provided, such as the need to bridge the gap between legislation and implementation through a delegation to understand the capabilities and resources available in each Member State. This could be combined with sharing best practices and experiences across European countries. For instance, more genetic-secure and digitally advanced countries like Denmark should share their experience with other countries. Codes of conduct[326] were also discussed to tailor the GDPR's security provisions to the genetic data processing context. Once more, these codes of conduct should consider European countries' best practices to evolve and disseminate faster.

It is essential to consider that there are still no magic formulas to protect genetic data. Therefore, there is a need to improve data security but, whenever possible, allow the data to be useful for healthcare development. Perhaps this challenging trade-off is why genetic data security has been substantially overlooked in the GDPR, just like the proverbial elephant in the room. Hopefully, this thesis will foster an essential discussion on the concrete solutions still to be implemented to make the GDPR a more enforceable and secure framework in the context of genetic data, increasing patients' confidence in healthcare institutions.

[326] Article 40 GDPR

Bibliography

Primary Sources

Legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) (2016)

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) [2016] OJ L119/1

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance) (2021) <EUR-Lex - 32021R0694 - EN - EUR-Lex (europa.eu)>

Legislative Proposals by the European Commission

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012), COM/2012/011 final

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (AI Act) (2021), COM/2021/206 final

Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (EHDS), 3 May 2022, COM/2022/197 final

Italian Legislation

Garante Per La Protezione Dei Dati Personali, 'Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, coma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]' (2019) available in Italian only < Provvedimento recante le prescrizioni relative al trattamento di... - Garante Privacy> accessed 15 July 2022

Case Law

Court of Justice of the European Union

Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779

Portuguese Case Law

Comissão Nacional de Proteção de Dados, Portuguese Resolution n.º 984/2018, ECLI: Processo n.º 9932/2018, english summary available in CNPD - Deliberação n.º 984/2018 - GDPRhub

Secondary Sources

Official EU Documents

European Commission

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society {SWD(2018) 126 final}

European Commission, 'Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021-2022' Brussels, 10.11.2021 C(2021)7914 final 89

European Commission, 'D5.2 : An International Code of Conduct for Data Sharing in Genomics : A Proposal' (2021) SIENNA Project

European Commission, 'Digital Europe Programme (DIGITAL) Call for Proposals' (2021) Cloud Data and TEF 1

European Commission, ‘Federated European Infrastructure for Genomic Data’, Digital Cloud Act <Funding & tenders (europa.eu)>

European Commission, ‘Study on eHealth, ‘Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union, Lot. 1 – Interoperability of Electronic Health Records in the EU’ (2020) Final Country FactSheets <Artificial Intelligence in Healthcare report | Shaping Europe’s digital future (europa.eu)>

European Commission, ‘Study on EHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union’ (2021) Lot. 2: Artificial Intelligence for health and care in the EU https://euagenda.eu/publications/study-on-ehealth-interoperability-of-health-data-and-artificial-intelligence-for-health-and-care-in-the-european-union

European Parliament

European Parliament, ‘Artificial Intelligence Act and Regulatory Sandboxes’ (EPRS, June 2022) <Artificial intelligence act and regulatory sandboxes | Think Tank | European Parliament (europa.eu)>

Article 29 Data Protection Working Party

Article 29 Working Party, ‘Opinion on Genetic Data’ (2004) 9 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf

Article 29 Data Protection Working Party, ‘Article 29 Working Party Opinion 4/2007 in the Concept of Personal Data’ (2007) 136 1 <ec.europa.eu>

Article 29 Data Protection Working Party, ‘Statement of the Working Party on current discussions regarding the data protection reform package’ (2013) < DRAFT FINDINGS (europa.eu)>

Article 29 Working Party, ‘Opinion 05/2014 on Anonymization Techniques’ (2014) < xxxx/xx/EN (europa.eu)>

European Data Protection Board

European Data Protection Board ‘Contribution to the evaluation of the GDPR' (February 2020)

European Data Protection Board, ‘Guidelines 3/2019 on processing of personal data through video devices’ (2020)

European Data Protection Board, ‘Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities’ 31 (2021)

European Data Protection Board, ‘Statement on Enforcement Cooperation’ 1 (EDPB, 28 April 2022) <Statement on enforcement cooperation | European Data Protection Board (europa.eu)> accessed 18 June 2022

European Union Agency for Cybersecurity

ENISA, ‘Handbook on Security of Personal Data Processing’ (2017)

ENISA, ‘Main Incidents in the EU and Worldwide’ (2019-2020) <*ENISA ETL2020 - Main Incidents in the EU and Worldwide (europa.eu)> accessed 15 June 2022

ENISA, ‘Cloud Security for Healthcare Services’ (2021) <*ENISA Report - Cloud Security for Healthcare Services.pdf> accessed 15 May 2022

ENISA, 'Data Pseudonymisation Techniques: Advanced Techniques & Technical Analysis of Cybersecurity Measures in Data' (2021) <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>

Official Documents from the Portuguese Data Protection Authority

Comissão Nacional de Proteção de Dados, 'Relatório de Atividades 2021', 21 June 2022, Lisbon <CNPD> accessed 14 July 2022

Academic Sources

Books

Alexandre Sousa Pinheiro and others, *Comentário Ao Regulamento Geral de Proteção de Dados* (2018) Almedina

Deodato S, *A proteção dos dados pessoais de saúde*, (7th edn, Fundação Cupertino de Miranda, U. Católica Editora 2017) 30

Hallinan D, *Protecting Genetic Privacy in Biobanking through Data Protection Law* (Oxford University Press 2021)

Kuner C., A. Bygrave L. and Docksey C, *The EU General Data Protection Regulation (GDPR): A Commentary*, (1st edn, Oxford University Press, 2020)

Kuner C., A. Bygrave L. and Docksey C (eds), *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update (OUP 2021)*

Slokenberga S, Tzortzatou O and Reichel J, *GDPR and Biobanking* (2021) Vol 143 <https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/46125/2021_Book_GDPRAndBiobanking.pdf?sequence=1&isAllowed=y>

Articles

Aarestrup FM and others, 'Towards a European Health Research and Innovation Cloud (HRIC)' (2020) 12 Genome Medicine 1

Ajami S and ArabChadegani R, 'Barriers to Implement Electronic Health Records (EHRs)' (2013) 25 Materia Socio Medica 213

B Brothers K and A Rothstein M, 'Ethical, legal and social implications of incorporating personalized medicine into healthcare' (2015) Vol. 12,1, 44

Argaw ST and others, 'Cybersecurity of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks' (2020) 20 BMC Medical Informatics and Decision Making 1

Arora A and Arora A, 'Synthetic Patient Data in Health Care: A Widening Legal Loophole' (2022) 399 The Lancet 1601 http://dx.doi.org/10.1016/S0140-6736(22)00232-X

Barros S Vale A and Zanfir-Fortuna G van Eijk R, 'Insights into the Future of Data Protection Enforcement: Regulatory Strategies of European Data Protection Authorities for 2021-2022'

Chen RJ and others, 'Synthetic Data in Machine Learning for Medicine and Healthcare' (2021) 5 Nature Biomedical Engineering 493 http://dx.doi.org/10.1038/s41551-021-00751-8

Coventry L and Branley D, 'Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward' (2018) 113 Maturitas 48 https://doi.org/10.1016/j.maturitas.2018.04.008

De Filippi P, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) Alternativ Journal of Peer Production 1 https://hal.archives-ouvertes.fr/hal-01382006

Dove E, 'Collection and Protection of Personal Health Data' [2018] SSRN Electronic Journal

Erlich Y and others, ‘Redefining Genomic Privacy: Trust and Empowerment’ (2014) 12 PLoS Biology

Erlich Y and Narayanan A, ‘Routes for breaching and protecting genetic privacy’ [2014] Nature reviews Genetics 15(6) 409-421 < https://doi.org/10.1038/nrg3723> accessed 15 December 2021

Fernández-Alemán JL and others, ‘Security and Privacy in Electronic Health Records: A Systematic Literature Review’ (2013) 46 Journal of Biomedical Informatics 541 http://dx.doi.org/10.1016/j.jbi.2012.12.003

Finnegan T, Hall A and Skopek JM, ‘Identification and Genomic Data Identification and Genomic Data Acknowledgements Identification and Genomic Data’ (2017) www.phgfoundation.org

Gibbons SM and Kaye J, ‘Governing Genetic Databases: Collection, Storage and Use’ (2007) 18 King’s Law Journal 201

Gonçalves ME, ‘The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward’ (2017) 26 Information and Communications Technology Law 90 https://doi.org/10.1080/13600834.2017.1295838

Greenbaum D, Du J and Gerstein M, ‘Genomic Anonymity: Have We Already Lost It?’ (2008) 8 American Journal of Bioethics 71

Hallock H and others, ‘Federated Networks for Distributed Analysis of Health Data’ (2021) 9 Frontiers in Public Health

Harbord K, ‘Genetic Data Privacy Solutions in the GDPR (2019) Texas A & M Law Review 7

Herian R, ‘Blockchain, GDPR, and Fantasies of Data Sovereignty’ (2020) 12 Law, Innovation and Technology 156

Herian R and others, 'The Use of Data from Electronic Health Records in Times of a Pandemic-a Legal and Ethical Assessment' (2021) 9 Journal of Law and the Biosciences 1 http://dx.doi.org/10.1038/s41551-021-00751-8

Hintze M, 'Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency' (2018) 8 International Data Privacy Law 86

Hoofnagle CJ, Sloot B van der and Borgesius FZ, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information and Communications Technology Law 65 https://doi.org/10.1080/13600834.2019.1573501

Ienca M and others, 'Considerations for Ethics Review of Big Data Health Research: A Scoping Review' (2018) 13 PLoS ONE 1

Kaya and others, 'Biobanking and Risk Assessment: a comprehensive typology of risks for an adaptive governance', [2021], *Life Sci Soc Policy* 17**,** 10 <https://doi.org/10.1186/s40504-021-00117-7> accessed in 14 January 2022

Kaye J, 'The Tension between Data Sharing and the Protection of Privacy in Genomics Research' (2012) 13 Annual Review of Genomics and Human Genetics 415

Knoppers BM and others, 'Towards a Data Sharing Code of Conduct for International Genomic Research' (2011) 3 Genome Medicine 1

Koops BJ, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250

Kuru T, 'Genetic Data: The Achilles' Heel of the GDPR?' (2021) 7 European Data Protection Law Review 45

Leckenby E and others, 'The Sandbox Approach and Its Potential for Use in Health Technology Assessment: A Literature Review' (2021) 19 Applied Health Economics and Health Policy 857 https://doi.org/10.1007/s40258-021-00665-1

Lopes IM, Guarda T and Oliveira P, 'General Data Protection Regulation in Health Clinics' (2020) 44 Journal of Medical Systems 1

Marelli L, Lievevrouw E and Van Hoyweghen I, 'Fit for Purpose? The GDPR and the Governance of European Digital Health' (2020) 41 Policy Studies 447 <https://doi.org/10.1080/01442872.2020.1724929>

Markopoulou D, Papakonstantinou V and de Hert P, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 Computer Law and Security Review 105336 https://doi.org/10.1016/j.clsr.2019.06.007

Marzluff WF and others, 'Identifying Personal Genomes by Surname Inference' (2013) Science Vol. 339, 321

Molnár-Gábor F and Korbel JO, 'Genomic Data Sharing in Europe Is Stumbling—Could a Code of Conduct Prevent Its Fall?' (2020) 12 EMBO Molecular Medicine 1

Muilu J, Peltonen L and Litton JE, 'The Federated Database - A Basis for Biobank-Based Post-Genome Studies, Integrating Phenome and Genome Data from 600 000 Twin Pairs in Europe' (2007) 15 European Journal of Human Genetics 718

Naveed M, 'Hurdles for Genomic Data Usage Management' (2014) 2014-Janua Proceedings - IEEE Symposium on Security and Privacy 44

Naveed M and others, 'Privacy in the Genomic Era HHS Public Access' (2015) 48 ACM Comput Surv 1

Nøhr C and others, 'Nationwide Citizen Access to Their Health Data: Analysing and Comparing Experiences in Denmark, Estonia and Australia' (2017) 17 BMC Health Services Research 1

Organ Donation Taskforce, 'The Potential Impact of an Opt-out System for Organ Donation in the UK.An Independent Report from the Organ Donation Taskforce' (2008) 36 Journal of medical ethics 1 <http://www.ncbi.nlm.nih.gov/pubmed/20817820>

Pormeister K, 'Genetic Data and the Research Exemption: Is the GDPR Going Too Far?' (2017) 7 International Data Privacy Law 137

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- A Nd Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502

Ribeiro de Sousa F, 'Blockchain Pharma' (2021) ISEG, Lisbon School of Economics and Management, University of Lisbon, Portugal 312

Sariyar M, Suhr S and Schlünder I, 'How Sensitive Is Genetic Data?' (2017) 15 Biopreservation and Biobanking 494

Shabani M, Vears D and Borry P, 'Raw Genomic Data: Storage, Access, and Sharing' (2018) 34 Trends in Genetics 8 http://dx.doi.org/10.1016/j.tig.2017.10.004

Shabani M and Borry P, 'Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation' (2018) 26 European Journal of Human Genetics 149 <http://dx.doi.org/10.1038/s41431-017-0045-7> accessed in 15 January 2022 152

Shabani M, 'Blockchain-Based Platforms for Genomic Data Sharing: A de-Centralized Approach in Response to the Governance Problems?' (2019) 26 Journal of the American Medical Informatics Association 76

Shabani M and Marelli L, ‘ Re-identifiability of Genomic Data and the GDPR ’ (2019) 20 EMBO reports 3

Stoeger K and Schmidhuber M, ‘The Use of Data from Electronic Health Records in Times of a Pandemic-a Legal and Ethical Assessment’ (2020) 7 Journal of Law and the Biosciences 1

Sukhorolskyi P and Hutsaliuk V, ‘Processing of Genetic Data under GDPR: Unresolved Conflict of Interests’ (2020) 14 Masaryk University Journal of Law and Technology 151

Sweeney L, ‘K-Anonymity: A Model for Protecting Privacy’ (2002) 10 International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems 557

Thelisson E, ‘AI Technologies and Accountability in Digital Health’ (2021) Cambridge Bioethics and the Law Series, Cambridge University Press <https://ssrn.com/abstract=3828206> accessed 20 December 2021 13

Topol E, ‘The Patient Will See You Now – The Future of Medicine Is in Your Hands’ (2015) BasicBooks New York

Truong N and others, ‘Privacy Preservation in Federated Learning: An Insightful Survey from the GDPR Perspective’ (2021) 110 Computers and Security 102402 <https://doi.org/10.1016/j.cose.2021.102402>

Utzerath J and Dennis R, ‘Numbers and Statistics: Data and Cyber Breaches under the General Data Protection Regulation’ (2021) 2 International Cybersecurity Law Review 339

Voronova S and Nichols A, ‘Understanding EU Data Protection Policy’ (2020) European Parliament

Yuan B and Li J, 'The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation' (2019) 16 International Journal of Environmental Research and Public Health

Zhiyu Wan and others, 'Sociotechnical Safeguards for Genomic Data Privacy' (2022) 0123456789 Nature Reviews Genetics, 430

Wadmann S, Hartlev M and Hoeyer K, 'The Life and Death of Confidentiality: A Historical Analysis of the Flows of Patient Information' [2022] BioSocieties https://doi.org/10.1057/s41292-021-00269-x

Wan Z and others, 'Sociotechnical Safeguards for Genomic Data Privacy' (2022) 0123456789 Nature Reviews Genetics

Other Sources

Acronis, 'The NHS cyber attack: how and why it happened, and who did it' (Acronis, 7 February 2020) <The NHS cyber attack: how and why it happened, and who did it (acronis.com)> accessed 15 June 2022

Agencia Española de Protección de Dados, '10 Misunderstandings Related to Anonymisation' (2021) <21-04-27_aepd-edps_anonymisation_en_5.pdf (europa.eu)>

Alan Toner and Johnny Ryan, 'Europe's enforcement paralysis' (Irish Council for Civil Liberties, April 2022) 10 < DPA report 2021 -updated 13 April 2022 (iccl.ie)> accessed 14 July 2022

Autoriteit Persoonsgegevens, 'Haga fined for insufficient internal security of patient files' (Autoriteit Persoonsgegevens ,16 July 2019) <Haga fines for insufficient internal security of patient files | Dutch Data Protection Authority (autoriteitpersoonsgegevens.nl)> accessed 15 May 2022

Barcelo R, 'GDPR Enforcement: Portugal' (2019) <GDPR Enforcement: Portugal | Consumer Privacy World> accessed15 October 2021

Bird and Bird, 'Guide to the General Data Protection Regulation (GDPR)' [2019] Guide to the General Data Protection Regulation n/a https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

CISPE.cloud, 'CISPE Code of Conduct' <https://www.codeofconduct.cloud> accessed 26 June 2022

CMS Rui Pena & Arnaut, 'GDPR Enforcement Tracker' <GDPR Enforcement Tracker - list of GDPR fines> accessed 20 June 2022

CPDP Conference, 'Can Law be Determinate in an Indeterminate World?' (CPDP Conference, 7 June 2022) < CAN LAW BE DETERMINATE IN AN INDETERMINATE WORLD? - YouTube> accessed 14 June 2022

Danish National Genome Center <Danish National Genome Center (ngc.dk)> accessed 15 May 2022

DataGuidance, 'Sweden: Datainspektionen completes audit of Capio St. Goran's Hospital, imposes fine of SEK 30M' (DataGuidance, 4 December 2020) <Sweden: Datainspektionen completes audit of Capio St. Göran's Hospital, imposes fine of SEK 30M | News post | DataGuidance>

Datatilsynet, 'Sandbox for responsible artificial intelligence', <Sandbox for responsible artificial intelligence | Datatilsynet> accessed 15 June 2022

DigitalEurope, 'DigitalEurope's recommendations for the European Health Data Space' (DigitalEurope, 3 February 2021) <DIGITALEUROPE's recommendations for the European Health Data Space - DIGITALEUROPE> accessed 15 May 2022

Digital Europe, ‘Summer Summit Conference’ (Digital Europe, 20 June 2022) <Summer Summit 2022 - DIGITALEUROPE> accessed 20 June 2022

Diogo Duarte, ‘Porque falha em Portugal a proteção de dados pessoais’ (Setenta e Quatro, 7 January 2022) available in portuguese only <Porque falha em Portugal a protecção de dados pessoais | Setenta e Quatro> accessed 14 June 2022

ESET, ‘The GDPR Report – Which businesses have been hit with the biggest GDPR fines?’ (ESET, 9 September 2021) <The GDPR Report – Which businesses have been hit with the biggest GDPR fines? | ESET> accessed 8 June 2022

Erlich Y, ‘Personal Genomes: Accessing, Sharing and Interpretation Conference’ (11-12 April 2019) Wellcome Genome Campus Advanced Courses and Scientific Conferences <Personal Genomes: Accessing, Sharing and Interpretation — 20190411 – Wellcome Connecting Science courses and conferences> accessed 15 may 2022

European Data Protection Board, ‘EDPB establishes cookie banner taskforce’ (EDPB, 27 September 2021) <EDPB establishes cookie banner taskforce | European Data Protection Board (europa.eu)> accessed 15 June 2022

European Data Protection Board, ‘Norwegian DPA: St. Olavs Hospital fined’ (2021) <Norwegian DPA: St. Olavs Hospital fined | European Data Protection Board (europa.eu)>

European Data Protection Supervisor, ‘Synthetic Data’ <Synthetic Data | European Data Protection Supervisor (europa.eu)> accessed 15 June 2022

European Data Protection Supervisor, ‘The Future of Data Protection: Effective Enforcement in the Digital World’ Conference (EDPS, 16 and 17 June 2022) <Home | EDPS Conference 2022> accessed 16 and 17 June 2022

FinData, ‘Findata has issued a regulation on the requirements of secure operating environments’ (Findata, 27 October 2020) <Findata has issued a regulation on the requirements of secure operating environments - Findata> accessed 15 May 2022

Gil D, ‘How to Preserve the Privacy of Your Genomic Data’ (Scientific American, 9 November 2020) <How to Preserve the Privacy of Your Genomic Data - Scientific American> accessed 20 June 2022

Global Alliance for Genomics and Health, ‘Crypt4GH: A secure method for sharing human genetic data’ <Crypt4GH: A secure method for sharing human genetic data (ga4gh.org)> accessed 1 November 2021

Health bank coop, <Healthbank - Control Your Health Data> accessed 15 May 2022

Informaconnect, ‘Future Healthcare: AI Conference’ (AQMEN365, 19 May 2022) <Future Healthcare: AI (aqmen365.com)> accessed 19 May 2022

Informaconnect, ‘Transforming Healthcare Delivery Conference’ (AQMEN365, 25 May 2022) Transforming Healthcare Delivery (aqmen365.com) accessed 25 May 2022

Ipsos, 'Perspectives in Healthcare Security' (CyberMDX, updated on 9 September 2021) <Perspectives in Healthcare Security Ipsos Report | CyberMDX> accessed 10 May 2022

Irish Examiner, ‘Cork hospital fined €65k after patients’ personal data found in public recycling facility’ (Irish Examiner, 4 November 2020) <Cork hospital fined €65k after patients' personal data found in public recycling facility (irishexaminer.com)>

KSI Blockchain’ <KSI Blockchain - e-Estonia> accessed 20 March 2022

Mohit Aggarwal, 'Towards Medical Data Ownership by Patients : Implications , Challenges and Solutions' (2018) Msc Health Informatics <TCD-SCSS-DISSERTATION-2018-056.pdf> accessed 1 April 2022, 33

NOYB, <NOYB enforces your right to privacy everyday> accessed 15 June 2022

Phillips M and others, 'Genomics: data sharing needs an international code of conduct' (Nature, 5 February 2020) <Genomics: data sharing needs an international code of conduct (nature.com)> accessed 15 October 2021

Ralston W, 'The untold story of a cyberattack, a hospital and a dying woman' (WIRED, 11 November 2020) <The untold story of a cyberattack, a hospital and a dying woman | WIRED UK> accessed 15 June 2022

Ryan J, 'Europe's Governments Are Failing the GDPR' (2020) Brave 14 < DPA report 2020 (brave.com)> accessed 14 June 2022

Security Magazine, 'Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak, (Security Magazine, 17 March 2020) <Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak | 2020-03-17 | Security Magazine> accessed 15 June 2022

Serviços Partilhados do Ministério da Saúde, 'Privacidade da Informação no setor da Saúde', (SPMS, 21 March 2017) available only in portuguese < *Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf> accessed 15 May 2022

SIC Notícias, 'Ataque informático ao Garcia de Orta: hospital está sem acesso a dados clínicos há 3 semanas' (SIC Notícias, 17 Maio 2022) available in portuguese only <Ataque informático ao Garcia de Orta: hospital está sem acesso a dados clínicos há 3 semanas - SIC Notícias (sicnoticias.pt)> accessed 15 May 2022

The Medical Futurist, 'Where Is Digital Health Heading in Denmark?' (The Medical Futurist, 7 February 2019) <Where Is Digital Health Heading In Denmark? - The Medical Futurist> accessed 15 May 2022

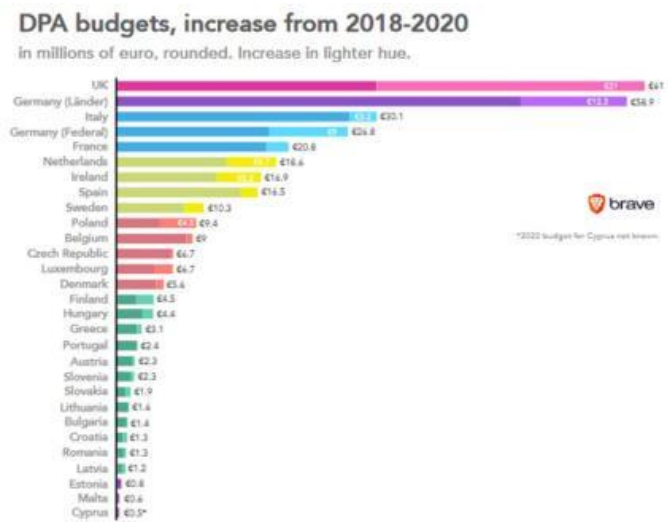
Towards European Health Data Space (TEHDAS), 'Why health is a special case for data governance', 23 June 2021, <Joint Action Towards the European Health Data Space – TEHDAS - Tehdas>, accessed 15 May 2022

Williams G and others, 'Regulating the Unknown: A Guide to Regulating Genomics for Health Policy-Makers' (2021) European Observatory on Health Systems and Policies <https://www.euro.who.int/en/about-us/partners/observatory/publications/policy-briefs-and-summaries/regulating-the-unknown-a-guide-to-regulating-genomics-for-health-policy-makers-2021Williams G and others, 'Regulating the Unknown: A Guide to Regulating Gen> accessed 20 February 2022

Woollacott E*, '*Under-Resourced Data Protection Authorities Fail to Enforce GDPR' (Forbes, 26 May 2020) <Under-Resourced Data Protection Authorities Fail To Enforce GDPR (forbes.com)> accessed 25 May 2022

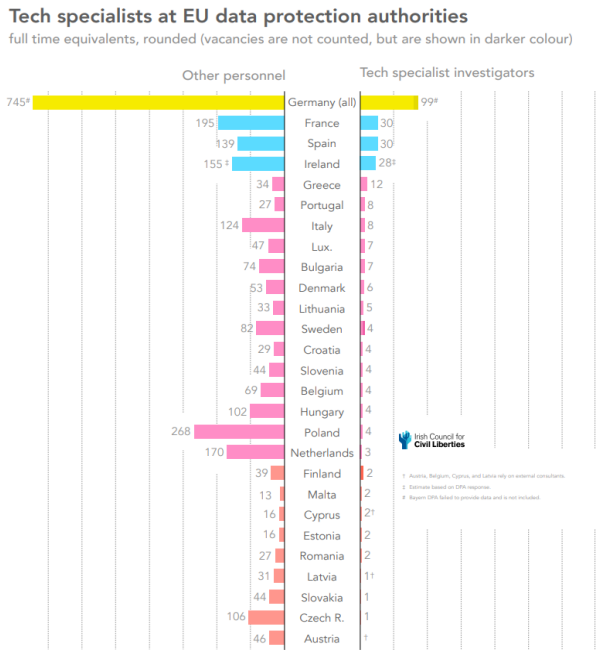
Appendices

Appendix 1:



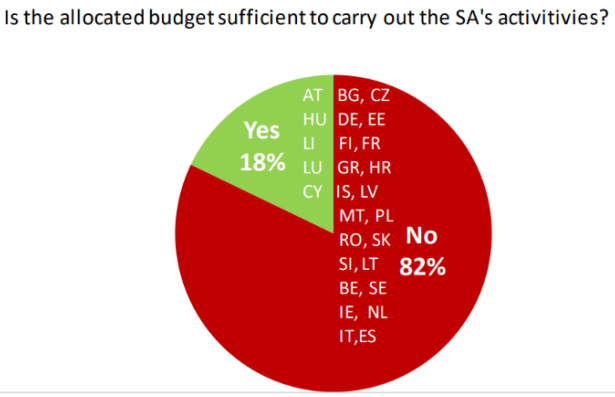
Reference: European Data Protection Board ‘Contribution to the evaluation of the GDPR' (February 2020) 28-9

Appendix 2:



Reference: Alan Toner and Johnny Ryan, ‘Europe’s enforcement paralysis’ (Irish Council for Civil Liberties, April 2022) 10

Appendix 3:



Reference: EDPB, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' 31, 5