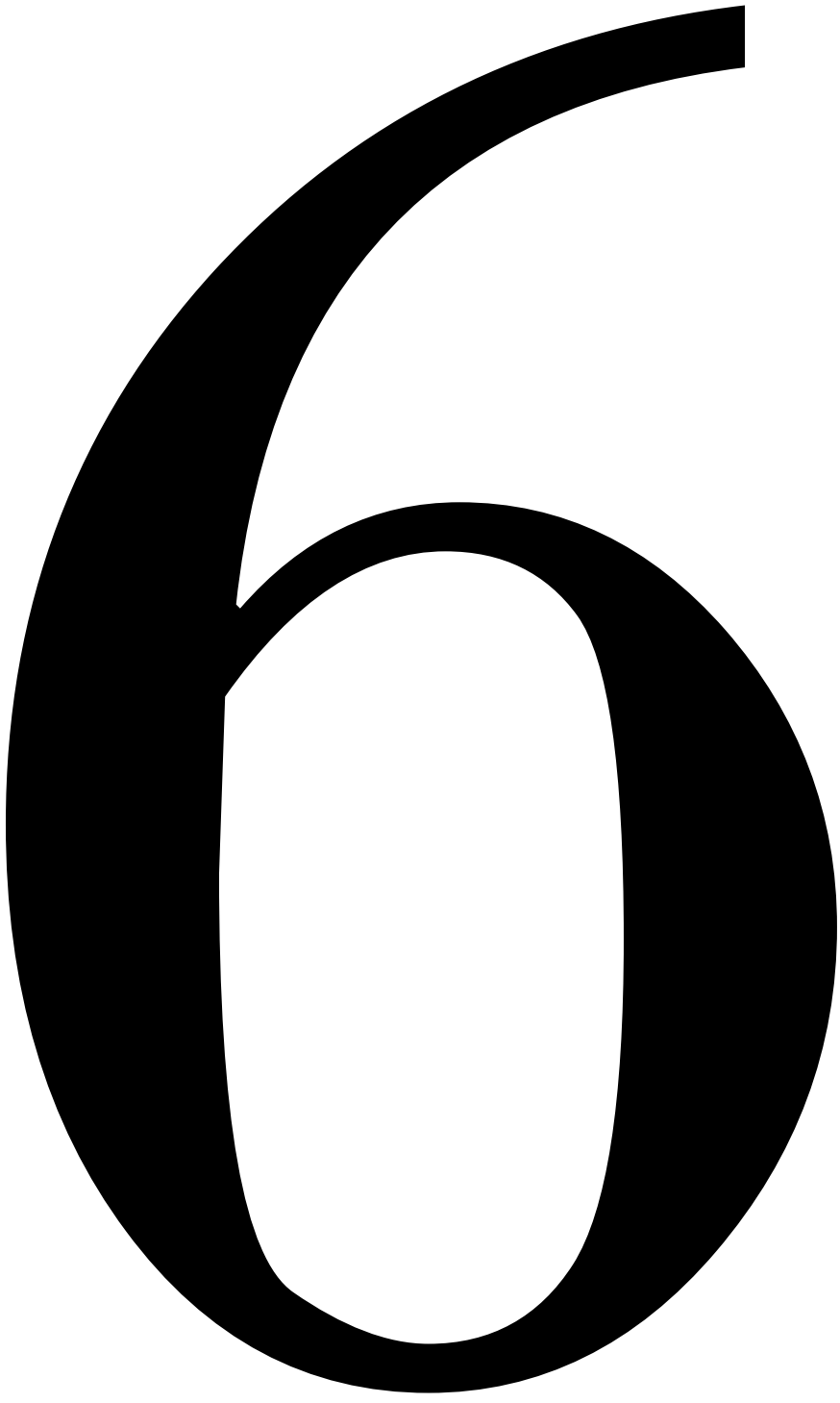
A fair balance: health data protection and the promotion of health data use for clinical and research purposes

Kist, I.R.



Closing the gaps in patients' data protection rights: a glance into the future with a Dutch case study

6. Closing the gaps in patients' data protection rights: a glance into the future with a Dutch case study[397]

This chapter answers sub-question 5 that reads as follows:

In what way does the existing data protection and health legislative framework protect the individual's autonomy, his health data, and his position as a care receiver where commercial companies deliver health services?

Abstract

This chapter discusses the legislative framework of data protection and health law in today's world, where the individual has become an active player in governing his health.[398] The individual's protection within the traditional treatment relationship between care provider and care receiver has been subject to substantial changes amidst technological and health innovations. The traditional, clinical health setting is complemented with actors from a non-clinical background, such as commercial companies that provide health care deliverables. New mechanisms for data protection and safeguarding a data subject's rights are required. The European Health Data Space Regulation is a good starting point, since it enables individuals to obtain a copy of their health data, to share and rectify these. However, we observe three gaps in the individual's data protection and his position vis-à-vis commercial companies: in the domain of legislation, in governance, and in the interaction between care provider and care receiver. The individual plays a role as a patient, but also as an individual with a particular lifestyle who uses wearables and buys commercial DNA tests. The individual's monitoring of his own health with devices does not necessarily fall within the scope of existing European and Dutch legislation on data protection and health.

[397] R. Dekker & I.R. Kist, Closing the gaps in patients' data protection rights: a glance into the future with a Dutch case study, *European Data Protection Law Review* 3 (2022) (8), 331-345. Keywords: European Health Data Space, fundamental rights, individual and informational self-determination, technological innovations

[398] In this chapter, words importing the masculine shall include the feminine and words importing the singular shall include the plural or vice versa. For easier readability, we continue with words importing the masculine.

6.1. Introduction

We elaborate on the new role played by the individual in his relationship with commercial companies that provide health deliverables. Health deliverables include any medical device as defined in the medical device regulation (MDR).[399] However, not all devices fall within the scope of the MDR since some of these devices focus on general health and well-being rather than on a medical purpose. In any event, the MDR includes a reference to data protection, i.e., the current General Data Protection Regulation (GDPR).[400] The individual must give his explicit consent for the processing of health data on health deliverables. In practice, research has shown that the companies of health deliverables do not always comply with the GDPR provisions.[401] Furthermore, though the individual seemingly exercises more control over his health and health data in monitoring this himself, his data may be further processed by other parties with a different purpose. As a result, his control over his data is compromised.[402]

In this chapter, the individual's role is illustrated with an innovative example followed by a glance into the future. We consider that some forms of data processing by these commercial companies have not yet been fully covered by law, either at an international or European or national level.[403] Consequently, the individual runs the risk that his data will be processed for other purposes than the original purpose or that they will be transferred to third parties, whereas the individual has neither given his consent nor has he been properly informed about this further processing.[404] His health data could be spread worldwide without his knowledge.[405]

[399] Article 2 of Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance), Medical Device Regulation, hereinafter MDR.
[400] 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), hereinafter GDPR. The MDR explicitly refers to data protection in article 110 (1).
[401] H.B. van Kolfschooten, The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union. In I. G. Cohen, T. Minssen, W. N. Price II, & C. Robertson (eds.), *The Future of Medical Device Regulation: Innovation and Protection* (Cambridge University Press, 2022), 63-76.
[402] European Data Protection Board (EDPB) – European Data Protection Supervisor (EDPS) Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, adopted on 12 July 2022. EDPS, Preliminary Opinion 8/2020 on the European Health Data Space, 2020. P. Quinn, The EU commission's risky choice for a non-risk based strategy on assessment of medical devices, *Computer Law & Security Review* 33.3 (2017), 361-370.
[403] C.S. Schneble et al., All our data will be health data one day: the need for universal data protection and comprehensive consent, *Journal of Medical Internet Research* 22 (2020) (5), e16879. And, Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document Green Paper on mobile Health ("mHealth"), 2014, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52014SC0135. Accessed 7 September 2022.
[404] C.M.L. Zegers et al., Mind your data: privacy and legal matters in eHealth, *JMIR Formative Research* 5 (2021) (3), e17456.
[405] M. Becker, Understanding users' health information privacy concerns for health wearables, 2019 https://pdfs.semanticscholar.org/c4a5/206eafcf533565f936ce5a70b8b11226f43d.pdf. Accessed 14 July 2022.

The existing data protection and health legislation has been implemented at the EU and national level by and among member states.[406] Health legislation governs the relationship between care provider and care receiver.[407] However, health innovations are often introduced by commercial non-state organizations. These organizations process and transfer health data from individuals, yet a treatment relationship, legally speaking, does not exist between these organizations and the individual. We consider that in these situations, the individual's consent, as a legitimation for processing his health data, may not suffice. The individual needs additional legislative protection, for instance a guarantee that particular data processing activities be prohibited by law, such as the commercial exploitation of his health data.[408]

Similarly, the health care professional finds himself in a new role. He continues to act pursuant to rules pertaining to professional medical secrecy and with his professional autonomy.[409] However, he is unable to exercise control over the personal data that have been collected and processed beyond traditional health care institutions. Whereas the health professional has a duty of care to the patient and his data in the traditional provider–patient relationship, the guardianship of his data has shifted towards the individual himself vis-à-vis commercial companies.

In the light of these innovations, we observe gaps in the existing data protection and health legislation with an impact on the individual's autonomy and control over his data. The GDPR applies but the data processing does not fall within the scope of the treatment relationship between the care provider and the care receiver. Thus, national health law does not automatically govern the data processing by commercial companies outside the traditional clinical realm. We investigate how said technological health services create a legislative and governance gap, both for the individual and the care provider. Furthermore, we analyze how the European Health Data Space

[406] European Commission, Assessment of the EU Member States' rules on health data in the light of the GDPR, Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03. BBMRI-ERIC, Statement by BBMRI-ERIC on "A European Health Data Space", and Response by BBMRI-ERIC to "European Health Data Space" (EHDS) Questionnaire (Public Consultation), https://www.bbmri-eric.eu/. Accessed 11 September 2022.

[407] In this chapter, we consider that the care provider is a healthcare professional pursuant to national health law, in particular the WGBO. However, we focus on commercial companies that also deliver healthcare services but do not automatically fall within the scope of Dutch health law.

[408] Article 4 (13), (14), and (15) together with article 9 of 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), hereinafter GDPR.

[409] Article 7:453 (WGBO); Article 99 Wet op de beroepen in de individuele gezondheidszorg (de wet BIG), Dutch Law on Individual Healthcare Provisions, hereinafter BIG.

(EDHS) constitutes a basis for filling these gaps to ensure that the processing of health data by commercial companies is legally solidified.[410]

6.1.1. Scope

We elaborate on the active role the individual plays in monitoring his health by making use of commercial tools and services. Hence, commercial companies also process and transfer his health data beyond the traditional care provider–care receiver relationship. This also occurs in the light of DNA testing, for instance. Although we do not cover the topic of genetic profiling and automatic decision-making here, we consider that these topics also deserve further analysis in view of the individual's autonomy and data protection.

We focus on data protection law, and we aim to strike a balance between data protection and health law when we consider the individual in two different health contexts. First, the individual is a patient in a clinical setting with the relationship between the care provider and care receiver. Second, the individual is an active participant who monitors his health beyond the traditional clinical realm. We illustrate the legislative and governance gaps and overlap with an example of an individual who lives in the Netherlands within the Dutch legal and health context. The Dutch context serves to highlight the correlation between data protection and health law, as well as the interaction between European and national data protection and health law.

6.1.2. Aim and research question

Individual self-determination and autonomy are two pillars of data protection and health law.[411] Nevertheless, these principles must be scrutinized with the new role the individual plays in the processing of health data provided by commercial companies beyond the traditional, legally safeguarded, care provider–care receiver relationship. Our aim in this chapter is twofold. Firstly, we aim to strike a balance between data protection and health law since we consider that both legal domains serve to safeguard the individual and his health data. Secondly, we elaborate on the European Health Data Space as a starting point to overcoming the legislative and governance gaps and overlap.

[410] BBMRI-ERIC, Statement by BBMRI-ERIC on "A European Health Data Space", 4 February 2021, https://www.bbmri-eric.eu/wp-content/uploads/statement-on-european-health-data-space.pdf. Accessed 14 July 2022. EDPB/ EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, adopted on 12 July 2022, https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf. Accessed 14 July 2022. L. Abboud et al., Towards European Health Data Space, Summary of Milestone 5.1 & 5.2 Annex A | Case studies: different governance and health data systems in Europe, 28 September 2021.

[411] Article 8 Charter of Fundamental Rights of the European Union, 2012/C 326/02. See section 6.2 below for the legal background. Also, A.C. Hendriks et al., Het recht op autonomie in samenhang met goede zorg bezien, *Tijdschrift voor Gezondheidsrecht* (2008) (32), 2-18.

We aim to answer the following sub-question in this chapter: *In what way does the existing data protection and health legislative framework protect the individual's autonomy, his health data, and his position as a care receiver where commercial companies deliver health services?*

In unraveling this question, we will elaborate on the influence of health innovations by commercial companies on the individual's autonomy and control over his health data. Furthermore, we will discuss which gaps and overlaps can be observed in the existing legislative and governance framework. Subsequently, we will elaborate on the role that the European Health Data Space (EHDS) can play in overcoming these gaps and overlap.

We begin this chapter with the legal research methodology (section 6.1.3) followed by the theoretical and legal background of this chapter (section 6.2). We analyze the individual's autonomy and control over his data from a data protection perspective (sections 6.2.1 and 6.2.2), and we elaborate on his autonomy within technological health innovations (section 6.2.3). Next, we introduce a case study (section 6.2.4.) upon which we illustrate the gaps we observe in data protection with the health services provided by commercial companies (section 6.3). We continue with the relationship between the care provider and the care receiver, which has gained new impetus (section 6.3.1). We also focus on the role played by commercial companies that offer health services (section 6.3.2). Subsequently, we analyze the gaps and overlaps, i.e., the legislative gap (section 6.4.1) and the governance gap and overlap (section 6.4.2). In addition, we elaborate on the role of the European Health Data Space as a point of departure to a transition in this field. We conclude by answering the research question of this chapter (section 6.5).

6.1.3. Legal research methodology

Firstly, the methodology applied in this chapter is doctrinal legal research.[412] The chapter analyzes the letter of the law, and both primary and secondary sources of law are scrutinized. Case law is also included. Secondly, the chapter analyzes the interpretation and implementation of the law in practice.[413] To this end, a Dutch case study serves to exemplify the challenges to health data protection amidst technological innovations. We have explicitly chosen a case study in one of the EU member states, i.e., the Netherlands, to elaborate on the interaction between international, European and national law on the one hand, and the relationship between data protection and health law on the other. In principle, Dutch data protection and health law provide

[412] J.B.M. Vranken, Methodology of legal doctrinal research, in M.A.A. Hoecke (ed.), *Methodologies of legal research. Which kind of method for what kind of discipline* (Hart Publishing, 2010), 111-121.
[413] P. Langbroek et al., Methodology of Legal Research: Challenges and Opportunities, *Utrecht Law Review* 13 (2017) (3), 1-8.

for the lawful basis of explicit consent for the use of health data.[414] The patient's implied consent applies when one or more health care provider(s) is (are) also directly involved in the care and cure of the patient.[415] The Netherlands has a long-standing history of the patient's informed consent for processing and transferring his health data and is a European pioneer in patients' rights.[416] The Dutch WGBO dates to 1994 and the case study sheds light on the interaction between national health law and the GDPR. The WGBO was implemented at a time when the internet had just been introduced to humankind, while the GDPR was implemented in a world surrounded by technological innovations.[417] Currently, the European Health Data Space aims to facilitate the creation of a European Health Union, as well as to enable the EU to make full use of the potential offered by a safe and secure exchange, use and re-use of health data.[418]

6.2. Legal background

We consider that health innovations influence the patient's autonomy and the control over his data.[419] Before we analyze the position of the individual and his health data, we outline the concept of self-determination in the context of health law and data protection law. We do so from the perspective of the care receiver. We note that the individual's autonomy and control over his personal data are subject to change since he engages in legal relations with commercial companies that deliver health care services. National health law does not automatically apply to these (international) commercial companies. At the same time, the care receiver can no longer rely on the professional medical secrecy for safeguarding his health data in a situation beyond the traditional care provider–care receiver relationship for the following two reasons. Firstly, the care receiver gives his consent to the processing of his personal data outside the realm of traditional health care and hence beyond the traditional legal framework where the health provider may not share the patient's data with others unless a specific legal ground applies. Secondly, the care provider–care receiver relationship with

[414] Article 24 UAVG, https://wetten.overheid.nl/BWBR0040940/2021-07-01. Article 7:450 WGBO.
[415] Article 7:457 (1) WGBO.
[416] European Commission, Patients' Rights in the European Union Mapping eXercise, PRE-MAX Consortium March 2016, 26.
[417] W. Schäfke-Zell, Revisiting the definition of health data in the age of digitalized health care, *International Data Privacy Law* 12 (2022) (1), 33-43.
[418] European Health Data Space Regulation, https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en. And, https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en#governance-of-the-european-health-data-space. Legislative train schedule on https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space. And, A Commission's presentation for the European Public Service Union of 3 February 2022: https://www.epsu.org/sites/default/files/article/files/EHDS%20presentation.pdf. Accessed 13 April 2022. Hereinafter: EHDS.
[419] M. Karampela et al., Connected health user willingness to share personal health data: questionnaire study, *Journal of Medical Internet Research* 21 (2019) (11), e14537.

shared decision-making is absent in the relationship between the individual and the commercial companies.[420] We turn to this impact in section 6.2.3 below.

6.2.1. Individual self-determination: the individual's autonomy

In health care, the notion of individual self-determination is closely related to the patient's freedom, i.e., the protection against the limitation of his autonomy and his (physical and mental) integrity, and, subsequently, the freedom to choose and to determine for himself which health care he receives. Additionally, self-determination with regard to his medical records is described as his capacity to determine, in principle, to what extent his personal data may be processed and transferred to foster a self-determined life.[421]

At an international and European level, individual self-determination is affirmed, inter alia, in article 8 Charter of Fundamental Rights of the European Union, article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and in article 1 International Covenant on Economic, Social and Cultural Rights.[422] The European Court of Human Rights has also acknowledged that article 8 ECHR includes the positive obligation of the individual's autonomy, rather than solely the negative right to freedom of the individual.[423] Explicit reference to individual self-determination is included in the Oviedo Convention and the UN Convention on the Rights of Persons with Disabilities.[424] However, these conventions are specifically directed at state actors, whereas commercial companies are non-state actors.[425]

[420] M.J. Taylor & J. Wilson, Reasonable expectations of privacy and disclosure of health data, *Medical Law Review* 27 (2019) (3), 432-460.
[421] T. Hooghiemstra, *Informationele zelfbeschikking in de zorg* (2018), 15.
[422] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe Treaty Series 005, Council of Europe, 1950. Hereinafter ECHR. United Nations (General Assembly). International Covenant on Economic, Social, and Cultural Rights. Treaty Series, 999, 171, 1966. See E. Milligan & J. Jones, Rethinking Autonomy and Consent in Health Care Ethics, 2017, Intech Open. V.A. Entwistle et al., Supporting Patient Autonomy: The Importance of Clinical-Patient Relationships, *Journal of General Internal Medicine* 25 (7), 741-745. Also, D. Hallinan, The Genomic Data Deficit: on the Need to Inform Research Subjects of the Informational Content of Their Genomic Sequence Data in Consent for Genomic Research, *Computer Law & Security Review* 37 (July 2020), 105427, 1-10.
[423] ECHR 7 July 1989, 10454/83 (Gaskin/United Kingdom); ECHR 13 February 2003, 42326/98 (Odièvre/France). Cordula Dröge, 'Positieve Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention', Beitrage zum ausländischen öffentlichen Recht und Völkerrecht, Band 159, 2003, pp. 379-392. European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence. Updated on 31 August 2021.
[424] Council of Europe, Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164). The Netherlands have not ratified the Oviedo convention. United Nations General Assembly, Convention on the Rights of Persons with Disabilities: resolution / adopted by the General Assembly, 24 January 2007, A/RES/61/106. See H. Nys et al., Patient rights in EU Member States after the ratification of the Convention on Human Rights and Biomedicine, *Health Policy* 83 (2007) (2-3), 223-235.
[425] F. Thouvenin, Informational Self-Determination: A Convincing Rationale for Data Protection Law? *JIPITEC* 12 (2021) (4), 246-256, https://www.jipitec.eu/issues/jipitec-12-4-2021/5409. Accessed 12 April 2021.

6.2.2. Informational self-determination: the individual's control over his data

We consider the following in light of the European legal framework on informational self-determination. The concept of consent, as a corollary to self-determination, is not expressly included in the Council of Europe Convention 108 or in the non-binding OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.[426] The OECD Guidelines only indirectly refer to the principle of consent in article 7, whereas Council of Europe Convention 108 refers to consent once in article 14 as regards the assistance to data subjects who are residents abroad. However, article 5 of this convention includes the requirement of fair and lawful processing and, thus, that a legitimate purpose and a lawful basis exist. The European Charter on Fundamental Rights has not formulated the right to data protection as a right to informational self-determination.[427]

The Data Protection Directive (DPD) connects the individual's privacy as well as other fundamental rights and interests of the individual, and echoes the right to informational self-determination to some extent.[428] However, the directive does not explicitly anchor a principle or a right to informational self-determination. The principle can be observed via the principle of consent by the individual and the rights he can invoke to express his control over his data. Examples are the right of access, the right of rectification, and the right to object.[429] Thus, the individual is able to exercise a certain degree of control over his personal data.

The GDPR also promotes the individual's control over his data, but like the DPD does not include an absolute, enforceable right to self-determination.[430] The GDPR combines the free flow of data and the necessity of trust by an individual in the data controller.[431] The individual must have control over his own personal data and he is

[426] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108. OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, 2002, OECD Publishing, Paris.
[427] P. Hustinx, European Leadership in Privacy and Data Protection. *Hacia un nuevo regimen europeo de protección de datos/ Towards a new European Data Protection Regime* (Valencia, 2015). E. Dove, The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era, *Journal of Law, Medicine & Ethics* 46 (2018) (4), 1013-1030.
[428] 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 OJ L 281, 23 November 1995.
[429] Article 7 (a) DPD (on consent), article 12 (a) DPD (on the right of access), article 12 (b) DPD (on the right of rectification) and article 14 DPD (on the right to object).
[430] Recital 7 GDPR. E.M.L. Moerel & J.E.J. Prins, Het recht op zelfbeschikking is een illusie, *Homo Digitalis* (NJV 2016-1) 2016/1.4.3. F. Thouvenin, Informational Self-Determination: A Convincing Rationale for Data Protection Law? *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 12 (2021), section 1.
[431] B. van der Sloot, Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation, *International Data Privacy Law* (2014) (4), 315. B. van der Sloot, Privacy as a human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? *JIPITEC* 5 (2014), 230. Also M. Mostert et al., Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach, *European Journal of Human Genetics* 24 (July 2016) (7), 956-60.

autonomous in his decision-making.[432] He expresses his free will with his explicit consent.[433] Furthermore, the individual has a number of rights he can invoke, i.e., the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing.[434] However, individuals are not always aware of or informed about their data protection rights when purchasing a wearable.[435] Thus, while the GDPR provides for a general data protection framework in theory, practice shows that the actual protection of the individual's privacy and health data protection is prone to the risk of further data processing beyond the original purpose, his own knowledge, and without his consent. Though the GDPR applies to those organizations outside the EU that render services and data to individuals in the EU, practice shows that organizations offering wearables on the EU market do not always comply with the EU legislative framework.[436]

Informational self-determination is closely related to the individual's autonomy.[437] In 1983, the German Constitutional Court developed the notion of informational self-determination as stemming from the core value of human dignity (article 1 of the German Constitution) and the so-called personality right (article 2 of the German Constitution).[438] This ruling presumes the capacity of the individual to determine, in principle, the processing and sharing of his personal data. Based on the newly defined right to informational self-determination, the individual himself, and only himself, shall decide when and within which limits the information about his private life may be communicated to others.[439]

[432] Recitals 5, 6, 7 and article 1 GDPR. European Data Protection Supervisor, https://edps.europa.eu/data-protection_en. Accessed 12 April 2022:

[433] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, adopted on 4 May 2020; European Data Protection Supervisor, Preliminary Opinion 8/2020 on the European Health Data Space, 17 November 2020.

[434] Chapter 3, articles 12 – 23 GDPR: rights of the data subject.

[435] T. Mulder & M. Tudorica, Privacy policies, cross-border health data and the GDPR, *Information & Communications Technology Law* 28 (2019) (3), 261-274. Also F. Lucivero, K.R. Jongsma, A mobile revolution for healthcare? Setting the agenda for bioethics, *Journal of Medical Ethics* 44 (October 2018) (10), 685-689.

[436] H.B. van Kolfschooten, The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union, in I. G. Cohen, T. Minssen, W. N. Price II, & C. Robertson (eds.), *The Future of Medical Device Regulation: Innovation and Protection* (Cambridge University Press, 2022), 66 – 68.

[437] T. Hooghiemstra, (2018). *Informationele zelfbeschikking in de zorg*. SDU. Also, A. Rouvroy & Y. Poullet, The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy, in S. Gutwirth et al. (ed.), *Reinventing data protection?* (Springer, 2009), 45.

[438] Judgment of the Bundesverfassungsgericht of 15 December 1983, First Senate, Case 83. ECLI:DE:BVerfG:1983:rs19831215.1bvr020983. G. Hornung & C. Schnabel, Data protection in Germany I: The population census decision and the right to informational self-determination, *Computer Law & Security Report* 24 (2009) (1), 84-88.

[439] The Court considered informational self-determination to derive from the fundamental (German) right to personality, as laid down in the German Constitution. See also C-73/07 Satakunnan Markkinapörssi Oy and Satamedia v. Finland, App. No. 931/13, 2017, ECLI:CE:ECHR:2017:0627JUD000093113, at 137, where the Court recognized that article 8 of the European Convention on Human Rights 'provides for the right to a form of informational self-determination'.

New European legislation is to be implemented as deliverables to the European strategy for data.[440] In short, the legislation comprises the following deliverables. On 25 November 2020, the European Commission published a proposal for a regulation on data governance.[441] The Data Governance Act (DGA) entered into force on 23 June 2022 and became fully applicable in the EU on 24 September 2023, following a transitional period of 15 months The EU aims to create a single European market for data to guarantee the free flow, sharing, and re-use for the benefit of individuals, researchers, corporate entities, and public administrations. The Data Governance Act creates the processes and structures to facilitate data.

The Data Act then clarifies who can create value from data and under what conditions.[442] The Data Act entered into force on 11 January 2024 and it will become applicable in September 2025.[443] The Data Act particularly addresses the use of data generated by Internet of Things (IoT) devices. On 3 May 2022, the European Commission presented a proposal for the European Health Data Space Regulation (EHDS). The EHDS is one of nine European data spaces identified in the European Commission's 2020 European Strategy for Data. It builds on the Data Governance Act and the Data Act. These acts are horizontal in nature, i.e., they also apply to the mutual relationship between consumers and companies, whereas the EHDS Regulation includes specific sectoral measures in the area of health, both as regards the use of data for health care (primary use) and the re-use of health data (secondary use). These deliverables aim to regulate both the free flow and use of data and to expand the rights of citizens to access and portability of health data.

At a national level, Dutch legislation serves to enhance the interoperability and exchange of data in the health sector. The *Wet elektronische gegevensuitwisseling in de zorg* (Dutch Act concerning the flow of electronic data interchange) was addressed by both chambers of Parliament and entered into force on 1 July 2023.[444] However, this act governs the 'when' and 'how' of data exchange, and does not address the position of the individual or the lawful bases of the data processing in particular. In conclusion,

[440] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data, COM/2020/66 Final, 19 February 2020.
[441] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 Final, 25 November 2020.
[442] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM (2022) 68 Final Brussels, 23 February 2022. EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted on 4 May 2022.
[443] https://digital-strategy.ec.europa.eu/en/policies/data-act. Accessed 21 January 2024.
[444] Kamerstukken II 35 824 nr. 2 (Parliamentary Papers II 35 824 nr. 2) Regels inzake het elektronisch delen en benaderen van gegevens tussen zorgverleners in aangewezen gegevensuitwisselingen (Wet elektronische gegevensuitwisseling in de zorg), https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2021Z07327&dossier=35824. Accessed 13 April 2022. Ministerie van Volksgezondheid, Welzijn en Sport, (Dutch Ministry of Health, Welfare and Sport), Herijking Grondslagen voor gegevensuitwisseling in de zorg (Recalibrating the lawful bases for data exchange in health care), 9 May 2022.

a wide array of international, European, and national (implementation) legislation aims to protect the individual and his health data. However, a separate right to informational self-determination has not been acknowledged.[445] New legislation aims at safeguarding both the individual and his data as well as the free flow of data.

6.2.3. Challenges to Individual and informational self-determination in the light of health innovations

With regard to the legal framework as described above, the individual reaches decisions about his health (i.e., he gives expression to his individual self-determination) and exercises control over his health data (i.e., he gives expression to his personal autonomy and informational self-determination).[446] Individual self-determination applies, inter alia, to the relationship between the care provider and care receiver.[447] The right is reflected in the patient's informed consent and safeguarded by the medical professional secrecy.[448] The requirement of the patient's informed consent serves two elements. First, it serves the patient's defensive right to say 'no' to a certain treatment. Second, it serves the patient's positive right to choose a medical treatment. Health services delivered beyond the traditional care provider–care receiver relationship have an impact on the traditional relationship and on the protection of the individual's health data.

Both the individual role and the role of the traditional care provider change with commercial companies that deliver health services. In his traditional role, the care provider is bound by professional secrecy and professional autonomy. He is the guardian of the patient's data and self-determination as regards medical treatment. The patient can voice his rights, for instance to access his medical records or choose a medical treatment. Although the individual may have access to the results of health deliverables from a commercial company, the traditional legal relationship between the care provider and care receiver is absent. In the traditional relationship, national health law protects the patient, whereas the commercial companies do not automatically fall within the traditional health care system.

In the traditional roles, the right to individual and informational self-determination is expressed by means of shared decision-making to create a balance in the provision

[445] In the Netherlands, the right to informational self-determination was subject to debate in 2010, as the Dutch State Committee brought it forward. See G. Overkleeft-Verburg, het grondrecht op eerbiediging van de persoonlijke levenssfeer, in A.K. Koekkoek et al., *De Grondwet, Een systematisch en artikelsgewijs commentaar* (Deventer, 2000), 155-179. B.J. Koops, Digitale grondrechten en de Staatscommissie: op zoek naar de kern, *Tijdschrift voor Constitutioneel Recht* (2011), 168-185.
[446] T. Hooghiemstra, Informational Self-determination, Digital Health and New Features of Data Protection, *European Data Protection Law Review* 2019 (2), 160-174.
[447] Verdict by the Dutch Supreme Court, 18 March 2005, Baby Kelly, NJ 2006, 606. ECLI:NL:HR:2005:AR5213.
[448] O. O'Neill, Some limits of informed consent, *Journal of Medical Ethics* 29 (2003), 4-7. M. Taylor & J. Wilson, Reasonable expectations of privacy and disclosure of health data, *Medical Law Review* 28 (2020) (2).

of care.[449] The following example sheds light on the different roles played by both the care provider and care receiver in the light of commercial companies that deliver health services. Additionally, the challenges to the individual and informational self-determination are addressed.

6.2.4. Dutch case study: Mrs. Johnson's diagnosis

Mrs. Johnson (43 years old) lives in Amsterdam. She watches a commercial about a genetic self-test that may inform her about a potential risk she runs for developing colorectal cancer. She buys the test with commercial technology Company X (a company that operates in various other sectors beyond health and which hosts other services as well) in non-EU country Y. The result shows that she carries a genetic variant with an increased risk of colorectal cancer. Upon receiving the test result, she also receives advice about her health and potential beneficial changes to her lifestyle. Mrs. Johnson learns that Company X has also invented an algorithm that can estimate her chances of developing colorectal cancer, based on her blood levels provided by a wearable.[450] Mrs. Johnson buys the wearable monitor from Company X. Company X asks Mrs. Johnson's consent for data processing of the blood levels to enhance the algorithm and, subsequently, to provide her with even better information about her health status. Based on the results created by the algorithm, she receives feedback that certain biomarkers in her blood have reached a certain level. She is advised to contact her general practitioner (GP). After a few days of emotional turbulence, she contacts her GP to find support and treatment. She also buys a smartwatch from Company X to monitor her health, which information she shares with Company X. Company X processes these data and informs her about adapting her lifestyle when the data give rise to this. A health practitioner, affiliated with but not employed by Company X, occasionally monitors these data. Ever since, Mrs. Johnson receives adverts from other companies about devices to monitor her health. When she shares the data gathered on her device with her GP, the GP expresses his concerns that premature conclusions may have been drawn after all.

This example illustrates the position of the individual and the health care professional within innovations and underpins the relationship between data protection and health law. The traditional care provider–care receiver relationship is subject to change that emerges from the dynamics of innovations. Traditional rights that aim to safeguard the individual's self-determination such as shared decision-making, as well as professional medical secrecy, are inextricably linked to the traditional care provider–care receiver relationship. In these new situations, the individual uses his own devices and draws

[449] H.J.J. Leenen et al., *Handboek Gezondheidsrecht* (The Hague, 2020, 8th ed.), 101.

[450] It may sound like a fictional reality, but in fact, Elisabeth Holmes tried to impress the world with such tests. Though this was in vain and trials followed, the future may bring similar innovations. See https://www.washingtonpost.com/technology/2021/11/16/blood-startups-theranos/Accessed 11 July 2022.

his own conclusions. Therefore, the specific protection of individual rights in the traditional health care relationship is absent. In the following section 6.3, we analyze and identify the changes of these dynamics in health care from a data protection and health law perspective.

6.3. Health data protection: what has changed?

The individual has become an active player in governing his health. We consider that the health innovations, and hence the different roles the care provider and care receiver play, give rise to changes. At an international, European, and national level, legislation provides for the individual's protection in health. The WGBO in particular protects his health care rights as a patient at a national level.[451] The act dictates that the individual is regarded as a patient when the treatment qualifies as a medical treatment, as a result of which he is entitled to a number of patient rights.[452] For instance, he must be informed about his treatment about which he can reach an informed decision based on shared decision-making.[453] Thus, individual self-determination is reflected in the individual's informed consent as regards his medical treatment. However, as an individual, in his relationship with commercial companies that deliver health care, his rights are not safeguarded pursuant to Dutch health law, since the traditional care provider–care receiver relationship is absent.

Moreover, the health care professional fulfills an essential role in determining to what extent the individual is able to express his self-determination via his consent to the data processing. Based on the protection that the individual receives as a patient within the current legal framework, a gap arises when we consider the example of Mrs. Johnson. She independently shares her health information with Company X. It may very well be that these data are processed anywhere around the world by organizations such as Company X without the intervention of a medical professional.

We continue to elaborate on two factors that influence the safeguards for the individual and his health data. The first factor concerns the changing relationship(s) between the care provider and the individual, where more health innovating companies have entered the scene, and where the individual no longer fulfills the role of patient but he is also an active participant in monitoring his health. The second factor follows from the first and concerns the data protection of the individual's health data.

[451] Article 7:446 – 7:468 WGBO.
[452] Article 7:446 WGBO.
[453] Article 7:448 WGBO.

6.3.1. The changing relationship between the traditional care provider and the individual

In the traditional relationship between the care provider and the individual, the patient has access to his medical records and may exercise his rights as a data subject pursuant to the GDPR.[454] In other words, he may express his right to informational self-determination.[455] His rights as a patient are also guaranteed in national health law.[456] Health legislation protects both the patient's position and the confidential relationship between care provider and care receiver. The bond of trust between them is a key factor when the patient seeks medical advice. Within the professional medical secrecy, the care provider guarantees that the care receiver may share his health data without fear of disclosure of this confidential data.[457] In other words, the care provider may not share the patient's health data in the traditional relationship unless a legal ground exists.[458]

A breach in professional medical secrecy is justified a) with the patient's consent, b) pursuant to a legal obligation or task, or c) in case of a conflict of interest while balancing the facts and circumstances by the care provider.[459] When the care provider breaches the professional medical secrecy in case of a conflict of interest, he must ascertain that he has done his utmost to obtain the patient's consent, and that further damage can only be averted by breaching the professional medical secrecy. In all instances, the care provider must perform a balancing test whether or not he breaches the professional medical secrecy.[460] The patient can only rely on these safeguards when the WGBO applies, i.e., when a treatment relationship qualifies as a medical treatment. Furthermore, the care provider carries out the treatment in the execution of his medical profession.[461]

In the example of Mrs. Johnson, we consider the following. First, Company X does not automatically fall under the scope of the WGBO. Secondly, by analyzing the conclusions reached with an algorithm, Company X informs Mrs. Johnson about a health risk based on the data from her wearable. In this example, the 'diagnosis' can be (and perhaps should be) regarded as an act in the field of medicine, but the traditional care provider–care receiver relationship remains absent since Company X does not meet the requirements of a health provider, i.e., a medical professional,

[454] Articles 12 – 23 GDPR.
[455] T. Hooghiemstra (2018). *Informationele zelfbeschikking in de zorg*. SDU, 15.
[456] Articles 7:446 – 7:467 WGBO.
[457] HR 19 November 1985, NJ 1986, 533, with annotation 't Hart. ECLI:NL:HR:1985:AC9105.
[458] Kamerstukken II 21561 nr. 3 (Parliamentary Papers II 21 561 nr. 3 MvT) 39.
[459] Articles 7:448 (3), 7:450, 7:457 (1) and 7:466 WGBO.
[460] KNMG richtlijn (Royal Dutch Medical Association - Guidelines) Omgaan met medische gegevens (KNMG 2021) 23.
[461] Article 7:446 WGBO and H.J.J. Leenen, Handboek gezondheidsrecht, 2020,108.

pursuant to the Dutch WGBO.[462] Consequently. Mrs. Johnson cannot exercise her right to self-determination via her patient's rights. Similarly, she is not protected by the professional medical secrecy from her care provider.

We reach the following preliminary conclusions. The new role carried out by the individual in monitoring his health results in a lack of legislative and operational protection. Since the individual is no longer regarded as a patient pursuant to existing Dutch national law, he lacks the legal protection pursuant to health law. In the example in section 6.2.4 above, even though Mrs. Johnson may have consented to the data processing of Company X, she has not consented to the further processing by third parties, or the sale of her data to other companies. We elaborate on the new relationship and the data protection in the following section.

6.3.2. The individual's health data and his position as a care receiver in a commercial context

Innovative health companies offer tests, treatments and monitoring via algorithms.[463] For instance, the number of genetic, direct-to-consumer tests is emerging. These tests serve various purposes related to health and lifestyle.[464] On the one hand, the individual may gather more information about his health, beyond the traditional treatment relationship. This may be considered a positive development. On the other hand, the medical professional is absent, which may jeopardize the individual's health and his data.

In accepting health services, the individual is generally in a disadvantaged position of health knowledge and expertise, and is unaware in what way his data are (further) processed. The bond of trust is not safeguarded in the commercial setting, because professional medical secrecy does not apply in this new relationship. Data protection is a general concern in DNA testing.[465] Consumers, by accepting the general conditions from the commercial company, may be unaware that they have consented to the further use of their data, albeit anonymized.[466] The concept of freely given, specific,

[462] Article 7:446 (2) (3). And M. van der Mersch, Nieuwe E-health toepassingen, zijn de patiëntenrechten aan innovatie toe? (Preadvies Vereniging voor Gezondheidsrecht 2018) 112 & Memorie van Antwoord (Reply to the statement of objections), Kamerstukken II 1989/90 (Parliamentary Papers II), 21561, nr. 6-55.

[463] Digital healthcare: patient first (22 April 2021) https://dealroom.co/uploaded/2021/04/Healthtech-Dealroom-Inkef-Capital-MTIP-final-smol.pdf?x23070. Accessed 9 February 2022.

[464] C. Ploem, M. Cornel & S. Gevers, Commercieel aanbod van DNA-tests: ruim baan voor vrije markt en zelfbeschikking? (2019) 32 *NJB* 2364. T. Rigter et al., Kansen en risico's van DNA-zelftesten (RIVM-2020-0196) 13.

[465] J.S. Roberts et al., Direct-to-consumer genetic testing: user motivations, decision making, and perceived utility of results, *Public Health Genomics* (2017), 36-45. And E.M. Gerrits et al., Direct-to-consumer genetic tests in de spreekkamer, *Nederlands Tijdschrift voor Geneeskunde* (2019) D4131, 163.

[466] Recital 26 GDPR. See AEPD and EDPS Joint Paper, 10 Misunderstandings related to anonymisation, 2021, https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf. Accessed 11 July 2022. G. Schneider, Disentangling health data networks: a critical analysis of Articles 9(2) and 89 GDPR, *International Data Privacy Law* 9 (2019) (4), 253-271.

informed, and unambiguous consent is eroded, aside from the question of whether DNA data can be completely anonymized at all.[467]

Company X does not automatically fall within the scope of national health law, as a result of which a national quality control framework and a specific, sectoral enforcement mechanism do not automatically apply either. The WGBO dictates that the care provider supplies the patient with proper information, based on his estimation what he needs.[468] Enforcement mechanisms, linked to the quality and safety of care, are important pillars for the patient's right to health and self-determination. Sanctions could be applied pursuant to civil law, disciplinary law, administrative law, and criminal law.[469] In the new health context, similar enforcement mechanisms remain absent since this kind of health services are provided beyond the traditional clinical realm.[470] In our view, the EHDS is a point of departure for filling the legislative gap. At the same time, we observe that the EHDS has significant overlap with other European legislation, such as the GDPR, the MDR, the Data Act, Data Governance Act, and AI Act.[471] The EHDS and Data Governance Act introduce a new governance structure, with a European Digital and Health Data Board. In our view, the patchwork of regulations creates both a governance gap and an overlap. We turn to the potential role of the EHDS in this matter in section 6.4.2 below.

We conclude that the health context for the individual has changed. We consider that the individual and his health data deserve equal protection in new relationships, no matter what role he adopts and no matter which care provider or commercial company he addresses. We observe a legislative gap (section 6.4.1) and a governance gap and overlap (section 6.4.2).

6.4. Filling the gaps: data protection in health innovations

The traditional care provider no longer controls the data processing by commercial companies beyond the traditional framework. Additionally, the individual lacks the bond of trust he enjoys in the traditional care provider–care receiver relationship, and the commercial companies are not bound by the professional medical secrecy. We

[467] M. Suriyar, I. Schlünder, Challenges and Legal Gaps of Genetic Profiling in the Era of Big Data, *Frontiers in Big Data* 2019, https://doi.org/10.3389/fdata.2019.00040. Accessed 12 July 2022.
[468] A. Hendriks et al., *Thematische wetsevaluatie Zelfbeschikking in de zorg* (ZonMw 2013) 158-161.
[469] Article 7:457 WGBO, 272 Wetboek van Strafrecht (Dutch Criminal Code), 218 Wetboek van Strafvordering (Dutch Code of Criminal Procedure) and 88 Wet BIG.
[470] T. Rigter et al., Kansen en risico's van DNA-zelftesten, RIVM-2020-0196, 18.
[471] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final, 2021. M. Kop, EU Artificial Intelligence Act: The European Approach to AI, Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, 2/2021. Ministerie van Volksgezondheid, Welzijn en Sport (Dutch Ministry of Health, Welfare and Sport), Kamerbrief Waardevolle AI voor Gezondheid (Letter to Parliament, Valuable AI in Health care), 9 May 2022.

observe a legislative gap as well as a governance gap and overlap in the relationship between the commercial company that provides health services and the individual.

6.4.1. Filling the legislative gap: protecting the individual and his data by commercial companies

We consider that the lawful basis of explicit consent, as one of the legitimations for the processing of health data, does not suffice in the role played by the individual vis-à-vis the commercial company. The individual is not able to assess the consequences of his consent and the risks involved in the data processing. Thus, other lawful bases must be considered that protect the individual in the new context. Next, we propose specific legislation with the following aims. This legislation must set norms for particular forms of data processing that must be prohibited, i.e., the mere exploitation of the (further) use of health data for commercial purposes without a licensing system and qualitative controls. Although we recognize that the individual is already surrounded by the new health context and acts accordingly by purchasing tests and monitoring his health, we argue that the legislative framework must fill the gap with respect to these new forms of data processing.

The individual's protection in the traditional health system has always been extensive, i.e., to protect the individual who finds himself in a dependent position. Thus, the legal system entrusted the state actors with the accountability and transparency towards the individual, where the individual reaches an autonomous decision, where his data are protected and the individual's rights respected.

The GDPR provides for a general data protection framework and the WGBO provides for the individual's protection in the traditional care provider–care receiver relationship. In traditional health law, safeguards have been implemented to protect the patient and his data. Commercial companies are not bound, legally speaking, to guarantee similar protection.[472]

We consider that the current legislative framework, at an international, European, and national level, does not fill the legislative gap. We observe that the boundaries of individual self-determination are stretched by the individual with his consent to commercial companies. Although we observe that the individual's health data are protected by national health law and, generally, by the GDPR, we observe that the individual's data protection is incomplete in the relationship between himself and commercial companies. We question whether the accountability and transparency principles in

[472] T. Rigter et al, T. Kansen en risico's van DNA-zelftesten (RIVM-2020-0196), 18.

the GDPR are fully realized in the data protection by commercial companies.[473] In our view, the European Health Data Space Regulation is a point of departure in the integral protection of the individual's position and health data. In the following section, we turn to the role of the EHDS as a starting point to foster human dignity in general, and to further the individual's rights to data protection and control over his health data. We observe both a governance gap and an overlap that require further attention to foster the integral protection of the individual's position.[474]

6.4.2. Filling the governance gap and overlap

The EHDS is part of the Digital Single Market Strategy[475] and the new generation of data regulations, i.e., the Data Act, the Digital Services Act, the Digital Markets Act, the Artificial Intelligence Act, and the Data Governance Act. In providing a framework for the use of electronic health data, the EHDS builds on the Data Governance Act and the Data Act.[476] These acts are horizontal in nature, i.e., they also apply to the mutual relationship between consumers and companies. The EHDS Regulation includes specific sectoral measures in the area of health, both as regards the use of data for health care (primary use) and the re-use of health data (secondary use).[477] As a horizontal framework, the Data Governance Act only lays down generic conditions for the secondary use of public sector data without creating a genuine right to the secondary use of such data. The Data Act enhances the portability of certain user-generated data, which can include health data but does not include rules for all health data. The EHDS complements these proposals and includes specific rules for the health sector. These rules cover the exchange of electronic health data and may affect provider of data sharing services formats that ensure the portability of health data, cooperation rules for data altruism in health, and complementarity on access to private data for secondary use.[478]

[473] T. Karjalainen, All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm, *European Data Protection Law Review* 1 (2022), 19-30.
[474] Expertmeeting on 'Zeggenschap, eigenaarschap en persoonsgegevens. Overwegingen en suggesties voor beleid' (control, ownership and personal data. Considerations and policy advice), 29 October 2021. And Brief van de minister van Volksgezondheid, Welzijn en Sport aan de Voorzitter van de Tweede Kamer der Staten-Generaal (letter from the Minister of Health, Welfare and Sport to the Chairman of the Parliament), 27529, nr. 276 and 277 as regards the legislative proposal Wegiz, 9 and 19 May 2022. Eerste Kamer der Staten-Generaal, Wet elektronische gegevensuitwisseling in de zorg, verslag van een deskundigenbijeenkomst, 2021 – 2022, 31765, 12 November 2021.
[475] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe COM (2015) 192 final. And, A European Strategy for Data: Shaping Europe's Digital Future, https://digital-strategy.ec.europa.eu/en/policies/strategy-data, with reference to: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM/2020/66 final. Accessed 10 September 2022.
[476] EHDS, explanatory memorandum, 4.
[477] EHDS, explanatory memorandum, 4-5.
[478] EHDS, explanatory memorandum, 4-5.

The central goal of the EHDS is to provide the individual with more control over his health data.[479] It builds on the GDPR that provides for safeguards in relation to data subject's rights over their health data. The EHDS aims to foster a genuine single market for digital health services while strengthening the right to data protection.[480] For instance, a further harmonization in the rights by individuals over their data is proposed by including a general right to data portability, as opposed to the GDPR where this right is limited.[481] Additionally, the EHDS includes an explicit right to direct access to one's health data, free of charge.[482]

The proposal is based on the Treaty on the Functioning of the European Union (TFEU).[483] The EU not only aims at protecting the individual's health data and giving the individual more control over his data, but it also fosters a framework with free data flows.[484] The EHDS and the Data Governance Act provide for a new governance structure, to which we turn now. Up until now, a national governance structure has guaranteed the supervision and monitoring of the health care system. With the new governance structure, a European Digital and Health Data Board (EHDS Board) is created which will be entrusted with promoting the collaboration between digital health authorities and health data access bodies.[485] This EHDS board will operate parallel to the existing European and national monitoring system, i.e., the European Data Protection Board (EDPB), European Data Protection Supervisor (EDPS), and the national Data Protection Authorities (DPAs). Additionally, the Data Governance Act introduces the European Data Innovation Board (Board), which serves to interact with the existing framework.[486] This Board shall be established in the form of an Expert Group, consisting of the representatives of competent authorities of all the member states, the European Data Protection Board, the Commission, relevant data spaces, and other representatives of competent authorities in specific sectors.[487] The Board shall encapsulate the data protection as enshrined in article 27 Data Governance Act. To this end, the Board shall advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies processing requests for the re-use of the categories of data referred to in article 3 (1). One or more of these competent bodies shall be designated by member states as a national duty. This competent body may be sectoral, to support the public sector bodies which grant

[479] EHDS, 21.
[480] Article 16 Treaty on the Functioning of the European Union.
[481] EHDS, explanatory memorandum, 6.
[482] Article 1 (subject matter and scope) together with article 3 (rights of natural persons in relation to the primary use of their personal electronic health data) and article 34 (purposes for which electronic health data can be processed for secondary use) of the Commission proposal for a Regulation on the European Health Data Space.
[483] Articles 16 and 114 TFEU.
[484] GDPR, Recitals 1, 2, 4-7 together with article 1 GDPR.
[485] EHDS, 19.
[486] Recital 40 Data Governance Act.
[487] Article 26 (1) Commission Proposal for a Regulation on the European Health Data Space.

access to the re-use of the categories of data referred to in article 3 (1) in the exercise of that task.[488]

Regarding the governance model created by the proposal of the EHDS, the tasks and competences of the new public bodies must be scrutinized, particularly taking into account the tasks and competences of national Supervision Authorities, the EDPB, and the EDPS in the field of processing personal (health) data. The EDPB-EDPS Joint opinion on the Proposal for a Regulation on the European Health Data Space observes the existence of an overlap in competences that should be avoided.[489] Furthermore, the fields and requirements for cooperation should be specified.[490] For instance, a difference is observed in the language between article 1 (4) EHDS, which reads as follows.

> "*(…) This Regulation shall be without prejudice to other Union legal acts regarding access to, sharing of or secondary use of electronic health data, or requirements related to the processing of data in relation to electronic health data (…).*"

And article 1 (2) Data Governance Act, which reads as follows:

> "*(…) [T]his Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements related to processing of personal or non-personal data. Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical, administrative or organizational requirements, including through an authorization or certification regime, those provisions of that sector-specific Union legal act shall also apply.*"[491]

Thus, it can also be argued that the national Data Protection Authorities will retain their oversight competence over commercial companies offering health services, apps and the like to patients. In view of the above, we observe a governance overlap and refer to the need as expressed in the EDPB-EDPS Joint Opinion for a clear coordination between the EDPB, the envisaged EHDS Board chaired by the European Commission and the national Data Protection Authorities.[492]

[488] Article 7 (1) Data Governance Act.
[489] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space.
[490] EDPB-EDPS Joint Opinion 03/2022, 4.
[491] Article 1 (2) Data Governance Act. EDPB- EDPS Joint Opinion 03/2022, paras 28 – 30, at 10.
[492] EDPB-EDPS Joint Opinion 03/2022, paras 117 – 121, at 29-30.

In principle, health care is governed by the member states and the proposal on the EHDS does not aim to regulate how health care is provided by member states.[493] However, a European health union has become even more apparent with the recent challenge of COVID-19 and global non-state actors in the health field. Additionally, the evaluation of the digital aspects of the Cross-border Health care (CBHC) Directive reviewed the current situation of fragmentation, differences, and barriers to access and use of electronic health data.[494] The evaluation shows that action by member states alone may prove insufficient and hamper the rapid development and deployment of digital health products and services, including artificial intelligence.[495] The EHDS takes a step forward and allows for the use of electronic health data for public health in the public interest, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health and care and of medicinal products or medical devices. It also serves scientific or historical research and statistical purposes.[496]

Although this new generation of data regulations aims at safeguarding the individual and his data as well as the free flow of data, a separate right to informational self-determination has not been acknowledged.[497] Besides, as we concluded earlier, the health context for the individual has changed. Nevertheless, the individual's human rights and his health data deserve equal protection in new relationships, no matter which role he adopts and no matter which care provider or commercial company he addresses. The boundaries of individual self-determination are stretched by the individual in relation to commercial companies. Though we understand that the individual's health data are protected by national health law and, generally, by the GDPR, we observe that the individual's data protection is incomplete in the relationship between commercial companies and the individual. Member states alone cannot counterbalance the commercial companies that operate at a global level to protect the individual, his health data, and his position as a care receiver in the new context. Here, we observe a governance gap that must be overcome.

[493] Commission proposal for a Regulation on the European Health Data Space, 8.
[494] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. And European Commission, Study supporting the evaluation of the Directive 2011/24/EU to ensure patients' rights in the EU in cross-border healthcare, 13 May 2022, https://health.ec.europa.eu/publications/study-supporting-evaluation-directive-201124eu-ensure-patients-rights-eu-cross-border-healthcare_en. Accessed 12 September 2022.
[495] Commission proposal for a Regulation on the European Health Data Space, 8.
[496] Commission proposal for a Regulation on the European Health Data Space, 7.
[497] In the Netherlands, the right to informational self-determination was subject of debate in 2010, as the Dutch State Committee brought it forward. M. Overkleeft-Verburg, Artikel 10. In A.K. Koekkoek et al., *De Grondwet – een systematisch en artikelsgewijs commentaar* (Deventer: W.E.J. Tjeenk Willink 2000), 177. Also, B.J. Koops, Digitale grondrechten en de Staatscommissie: op zoek naar de kern, *Tijdschrift voor Constitutioneel recht*, March 2011.

To analyze this gap, we took a conceptual look at the EHDS. Though the EHDS does not provide for a global answer, it does provide for additional data protection of the individual and his health data beyond the realm of the traditional care provider–care receiver relationship. In our opinion, the EHDS is a starting point to foster human dignity in general, including addressing the individual's rights to data protection and control over his health data. A European governance structure is created with the EHDS and can be seen as a starting point to bridge the gap between the national autonomy of member states also in health law. The EHDS aims to protect the health data of individuals, and is not limited to protecting the patient's data only.

We reach the following preliminary conclusions. Firstly, both the EHDS and the Data Governance Act create opportunities for the protection of the individual and his health data beyond the traditional care provider–care receiver relationship. Secondly, although member states are given the opportunity to designate a sectoral monitoring body or bodies, we observe a missing link in the relationship between data protection in general and the individual's protection of his health data and safeguarding of his rights. We would argue that a next step is necessary, one that combines individual self-determination (as enshrined in health law) and informational self-determination (as enshrined in data protection law). In this respect, we consider that data protection authorities should cooperate more closely with (cross-) sectoral bodies to strike a balance between the individual and informational self-determination, and to reach a solution to the governance overlap.[498]

6.5. Conclusion

In this chapter, we elaborated on the fifth sub-question:

> *"In what way does the existing data protection and health legislative framework protect the individual's autonomy, his health data, and his position as a care receiver where commercial companies deliver health services?"*

Firstly, the WGBO protects the patient in existing health law, i.e. in the relationship between the care provider and care receiver. The care provider guarantees that the care receiver can share his health data without the fear of disclosure of his confidential data, as part of the professional medical secrecy. The care provider may not share the patient's health data in the traditional relationship unless a breach to the professional medical secrecy is justified. Additionally, the traditional health system is based on the patient's informed consent in the context of shared decision-making.

[498] Recital 41 and article 1(2) Data Governance Act, article 1 (4) EHDS.

The situation is quite the opposite in the new health context where the individual plays a different, active role in monitoring his health beyond the traditional care provider – care receiver relationship. In this new situation, the bond of trust between the care provider and care receiver is absent. The individual uses his own devises and draws conclusions about his health. In this context, he gives his consent to the processing of his personal data outside the realm of traditional health care, beyond the traditional legal framework. Since the individual is no longer safeguarded as a patient, the boundaries of individual self-determination are stretched by the individual and by the commercial companies that deliver health services. We conclude that the legislation must set norms for these forms of data processing beyond the traditional clinical realm. In addition, some forms of data processing must be prohibited where the individual runs a serious risk, such as the mere exploitation of the (further) use of health data for commercial purposes without a licensing system and qualitative controls.

Secondly, the individual's autonomy is not fully protected because of a legislative gap in the current legal framework. The individual's health data are protected by Dutch health law in the traditional care provider–care receiver relationship and, generally, by the GDPR. The individual's data protection is incomplete in the relationship between the commercial company and the individual. The legislation was set up by and between member states, whereas these developments take place beyond the traditional clinical realm by commercial companies. The member states alone cannot safeguard the individual's autonomy and control over his health data with the new, active role he himself plays. The individual runs the risk that his health data are processed for other purposes and by third parties.

Thirdly, we observe a governance gap and overlap in the individual's protection in health law – which safeguards the individual's self-determination and autonomy – and the individual's data protection – which safeguards the control over his personal data and informational self-determination. A next step is necessary to safeguard the individual's self-determination (as enshrined in health law) and his informational self-determination (as enshrined in data protection law). In our view, the European Health Data Space (EHDS) can play a pivotal role in the individual's protection of his health data for reasons as outlined below.

The EHDS creates a European governance structure and can be a driving force behind the aim of protecting the individual and his health data in a broader sense. Thus, the EHDS is a good point of departure for a) enhancing data protection, b) striking a balance between data protection and health law, and c) setting the agenda for a European governance framework in health. However, we also observe some difficulties

in the European ambitions, since health law – within the traditional clinical realm – is governed by member states. When it concerns national health matters, the EHDS must leave room for the supervisory systems within member states. We recommend a further analysis of the interaction between European data protection and national health law.

Additionally, we observe that the EHDS and Data Governance Act do not provide for sectoral supervision. We consider that national data protection authorities should cooperate more closely with sectoral health bodies to strike a balance between the individual's protection in data protection and health law, based on the governance structure offered by the EHDS. Thus, the governance structure should be broadened to safeguard both the individual's position and his data both in the traditional and innovative health contexts. Furthermore, clarity must exist as regards those bodies handling data protection issues. When both European supervisory authorities and national bodies address data protection issues, then the risk of conflicting contributions arises – with the possible result of legal uncertainty.

To conclude, the innovations call for joint action at the European and national levels to safeguard the individual's position and his data in health beyond the traditional care provider–care receiver relationship. We recommend a further legal analysis of the interaction between individual self-determination (in health law) and informational self-determination (in data protection law). We also recommend a sectoral supervisory body that monitors the individual's self-determination in health and his control over his health data. The EHDS creates a European governance structure that can be considered a starting point to bridge the gap between the national autonomy of member states in health law as well. Member states cannot counterbalance the commercial companies that operate at a global level. The EHDS can close the gaps in the individual's data protection rights in health, beyond his role as a patient in the traditional clinical setting.