Alma Mater Studiorum - Università di Bologna

in cotutela con UNIVERSITÄT WIEN

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo 35

Settore Concorsuale: 12/H3 - FILOSOFIA DEL DIRITTO

Settore Scientifico Disciplinare: IUS/20 - FILOSOFIA DEL DIRITTO

INTERNET OF HEALTHCARE (LAW): PRIVACY AND DATA PROTECTION ASPECTS IN AN INTERNET OF EVERYTHING

Presentata da: Richard Rudolf Rak

Coordinatore Dottorato

Monica Palmirani

Supervisore

Monica Palmirani
(Alma Mater Studiorum - Università di Bologna)

Supervisore

Nikolaus Forgó
(Universität Wien)

Co-supervisore

Michele Graziadei
(Università di Torino)

Esame finale anno 2023

universität wien

DISSERTATION / DOCTORAL THESIS

Titel der Dissertation / Title of the Doctoral Thesis

Internet of Healthcare (Law): Privacy and Data Protection Aspects in an Internet of Everything

verfasst von / submitted by

Dr. Richárd Rudolf Rák, LL.M.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Doktoratsstudium der Rechtswissenschaften (Dr. iur.)
Doctoral program in Law (Dr. iur.)

Wien, 2023 / Vienna, 2023

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 783 101
Dissertationsgebiet lt. Studienblatt / field of study as it appears on the student record sheet:	Rechtswissenschaften / Law
Betreut von / Supervisors:	Prof. Nikolaus Forgó Prof. Monica Palmirani Prof. Michele Graziadei

TABLE OF CONTENTS

INTRODUCTION

1.) Policy context

1.1.) EU policy initiatives catalysing digital transformation in healthcare

In its 2014 'Communication on effective, accessible and resilient health systems', the Commission outlined that the health systems of EU Member States face complex challenges, namely:[1]

- a growing demand for healthcare due to ageing populations, rise of chronic diseases and multi-morbidity patterns;
- sharply increasing costs;
- limited availability of financial resources;
- shortages and uneven distribution of health professionals;
- health inequalities; and
- inequities in access to healthcare.

In order to cope with these challenges, health systems require reforms to become more effective, accessible and resilient. To achieve complex and system-wide changes, the general view is that health systems should be doing more to embrace digital transformation by harnessing data and digital technologies.[2]

Considering that healthcare is an information- and knowledge-intensive industry, the rapidly growing volume of data relating to health and the possibility of extracting valuable information and knowledge therefrom offer immense potential to improve patient care, manage health systems, analyse public health and facilitate health research.[3] In spite of the considerable potential of digitalisation, healthcare (together with the pharmaceutical)

[1] Communication from the Commission on effective, accessible and resilient health systems, COM/2014/215 final, Brussels (4 April 2014). CELEX: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52014DC0215>.

[2] OECD (2019) *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*. OECD Health Policy Studies. OECD Publishing, Paris, 15. DOI: <https://doi.org/10.1787/e3b23f8e-en>.

[3] OECD (2015) *Data-Driven Innovation: Big Data for Growth and Well-Being*. OECD Publishing, Paris, 332. DOI: <https://doi.org/10.1787/9789264229358-en>.

industry remains among the least digitised sectors.[4] To address this problem, the Commission has aimed to increase coordination efforts relating to the digital transformation of health and care in the EU. In its 2017 'Mid-Term Review on the implementation of the Digital Single Market Strategy', the Commission set out its intention to take further measures in the area of digital health and care, in line with legislation on the protection of personal data, patient rights and electronic identification, in the following three areas:[5]

(a) citizens' secure access to and sharing of health data across borders;

(b) better data to advance research, disease prevention and personalised health and care; and

(c) digital tools for citizen empowerment and person-centred care.

With a view to achieving these objectives, the Commission emphasised in its 2018 'Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society' that the health systems of Member States have to find innovative solutions through new technologies, products and organisational changes.[6] The Commission highlighted that digital solutions can provide the means to support the transformation of health and care systems, if they are designed purposefully and implemented cost-effectively. According to the Staff Working Document accompanying the Communication, digital transformation requires the uptake of digital technologies and tools (e.g. mobile communication devices, sensors, cloud and high-performance computing, distributed data ledgers, big data mining and analytics, and artificial intelligence), and the provision of healthcare services that make use of these digital solutions (e.g. telehealth, telecare, wellness applications and ePrescriptions).[7]

---

[4] European Commission Directorate-General for Communications Networks, Content and Technology (2020) *Shaping the Digital Transformation in Europe*. Publications Office of the European Union, Luxembourg, 26. DOI: <https://data.europa.eu/doi/10.2759/294260>.

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, COM(2017) 228 final, Brussels (10 May 2017). CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017DC0228>.

[6] 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, COM/2018/233 final, Brussels (25 April 2018). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:233:FIN>.

[7] Commission Staff Working Document Accompanying the Document '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 COM(2018) 233 final', SWD(2018) 126 final, Brussels (25 April 2018). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0126>.

In the aforementioned Communication and accompanying Staff Working Document, the Commission outlined the opportunities that digital health solutions offer to transform health systems, and improve their effectiveness, accessibility and resilience. According to these documents, digital health solutions enable the capturing, management and processing of large volumes of diverse data generated from multiple sources in order to create new knowledge. They enable new person-centred approaches in the organisation of healthcare by offering new insights for individuals to assume responsibility for their health, improve their well-being, and contribute to more sustainable health systems. They also enable new approaches to personalised medicine, accelerating scientific progress, early diagnosis and prevention of diseases, as well as effective treatments. Digital health solutions can address staff shortages in rural areas and certain specialties. They can connect various actors across the healthcare sector, thus ensuring effective sharing of data and collaboration, in more effective healthcare delivery models. The analysis of electronic health data and patient-reported data may lead to improved procedures, reduce inefficiencies, support outcome-oriented healthcare, promote evidence-based assessment of innovative health technologies, and improve emergency preparedness and response to epidemics. However, the Commission reminded that success in these endeavours depends on the availability and interoperability of vast amounts of high-quality data. The other key success factor is the adoption of appropriate regulatory frameworks that are capable of stimulating innovation while safeguarding the interests of society and the rights of the individual.

1.2.) The impact of the COVID-19 public health crisis on the uptake of digital health solutions and telehealth services

The COVID-19 public health crisis exposed the latent fragilities of health systems and exacerbated the abovementioned structural problems.[8] However, at the same time, the pandemic triggered a remarkable leap of innovation in healthcare and induced the rapid uptake of digital health solutions. Most EU Member States introduced new policies to incentivise the use of digital health solutions. In terms of legislation, several Member States relaxed rules on the possibility to arrange teleconsultations with first-visit patients, while

[8] OECD, European Union (2020) *Health at a Glance: Europe 2020: State of Health in the EU Cycle*. OECD Publishing, Paris, 13. DOI: <https://doi.org/10.1787/82129230-en>.

another group of Member States adopted provisions to permit the remote renewal of repeat prescriptions.[9] Regarding financial aspects, most Member States increased reimbursement levels for remote patient consultations closer or even up to those normally paid for standard in-person visits.[10] Indeed, the public health crisis showed that effective health spending is an investment, not a cost to be contained: stronger, more resilient health systems protect both populations and economies.[11] In general, these legal and financial incentives fostered the use of digital health solutions to boost public health measures during the pandemic in four critical areas:[12]

(a) communication and information (e.g. dissemination of information on COVID-19 issues to the public);

(b) monitoring and surveillance (e.g. mobile apps for contact tracing, symptom tracking and/or enforcement of quarantine);

(c) provision of healthcare services (e.g. teleconsultations, ePrescriptions, use of AI to identify infections or potential treatments); and

(d) vaccination, immunity and pharmacovigilance (e.g. issuance of digital immunity certificates, remote monitoring of adverse reactions to vaccinations).

In addition to the uptake of digital health solutions, another lesson from the COVID-19 crisis is that data is not just a critical enabler for developing more efficient, higher quality, safer and more personalised healthcare services, but it is also an essential asset in tackling public health emergencies. Prompt sharing of data helped to speed up the implementation of contingency measures and expedite research on new tests and treatments. This happened not only in academia, but also within industry, which accelerated cooperation and collaboration among entities in the health research and innovation ecosystem.[13] The pandemic also

---

[9] European Commission Directorate-General for Health and Food Safety (2022) *State of Health in the EU: Companion report 2021*. Publications Office of the European Union, Luxembourg, 24. DOI: <https://data.europa.eu/doi/10.2875/835293>; *see also* CMS (2020) *CMS Expert Guide to digital health apps and telemedicine*. CMS. Available from: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-digital-health-apps-and-telemedicine>.

[10] *Ibid*.

[11] OECD (2021) *Health at a Glance 2021: OECD Indicators*. OECD Publishing, Paris, 13. DOI: <https://doi.org/10.1787/ae3016b9-en>.

[12] European Observatory on Health Systems and Policies *et al*. (2021) *Use of digital health tools in Europe: before, during and after COVID-19*. World Health Organization Regional Office for Europe, Copenhagen, 18. Available from: <https://apps.who.int/iris/handle/10665/345091>.

[13] MedTech Europe (2020) *Innovation in Medical Technologies: Reflection Paper*. MedTech Europe, Brussels (October 2020), 7. Available from <https://www.medtecheurope.org/wp-content/uploads/2020/10/2020_mte_innovation-in-medical-technologies_reflection-paper.pdf>.

highlighted the imperative of having "FAIR" (i.e. findable, accessible, interoperable and reusable)[14] electronic health data in order to ensure preparedness to health threats, and for improving diagnoses, treatments, and open up new horizons enshrined in the secondary use of health data. If society would have had a stronger sense of urgency to deal with these issues before, then timely access to data would have contributed, through efficient public health surveillance and monitoring, to a more effective management of the public health crisis, and ultimately, would have helped to save lives and mitigate health problems.

From a market perspective, the COVID-19 crisis accelerated the formation of a 'New Health Economy', a concept that describes the transformation of health systems into a modular ecosystem of innovation, delivery and wellness, more closely tied to consumers (patients) and increasingly dependent on the provision and use of telehealth services.[15] When the pandemic undermined traditional face-to-face patient–doctor encounters, especially in general practitioner services, this change brought telehealth to the forefront of primary care on a scale as never before.[16] In the wake of the pandemic, healthcare providers scaled the provision of ICT-enabled healthcare services rapidly, while client adoption of telehealth solutions increased at an unprecedented pace.[17] By way of illustration, in the US, overall telehealth utilisation for doctor visits and outpatient care was 78(!) times higher in April 2020 than in February 2020.[18] In the next 12 months, the volume of telehealth claims reached a 30–40 times higher level than the pre-COVID baseline. In Europe, survey data shows that the share of EU citizens who had a remote (online or telephone) consultation with a general practitioner increased from 28.7% in June/July 2020 to 38.6% in February/March 2021.[19] The COVID-19 crisis also boosted the use of mHealth apps as consumers looked to keep fit

---

[14] Wilkinson M, Dumontier M, Aalbersberg I *et al*. (2016) The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data* 3(16018):1–9. DOI: <https://doi.org/10.1038/sdata.2016.18>.

[15] PwC (2020) *Accelerating the health economy of tomorrow: Transforming health systems and embracing innovation amid a pandemic*. PwC, 2–3. Available from: <https://www.pwc.com/gx/en/industries/healthcare/publications/assets/pwc-new-health-economy.pdf>.

[16] Garattini L, Badinella Martini M, Mannucci PM (2021) Improving primary care in Europe beyond COVID-19: from telemedicine to organizational reforms. *Internal and Emergency Medicine* 16:255–258. DOI: <https://doi.org/10.1007/s11739-020-02559-x>.

[17] Negreiro M (2021) *The rise of digital health technologies during the pandemic*. European Parliamentary Research Service Member's Research Service, 2–3. Available from: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690548/EPRS_BRI(2021)690548_EN.pdf>.

[18] Bestsennyy O, Gilbert G, Harris A, Rost J (2021) *Telehealth: A quarter-trillion-dollar post-COVID-19 reality?* McKinsey & Company (9 July 2021). Available from: <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>.

[19] Eurofound (2021) *Living, working and COVID-19 dataset*. Eurofound, Dublin (5 July 2021). Available from: <https://www.eurofound.europa.eu/data/covid-19/quality-of-public-services>.

and stay mindful during lockdowns. According to estimates, downloads of health and fitness apps surged by 46% in Europe to 829.5 million, while spending on this category of apps jumped by 70.2% year-over-year in 2020, accounting for 30.3% of total global spending.[20]

Although there are significant differences in the uptake of telehealth between countries, evidence suggests that there is a positive role for telehealth to play in improving the performance and outcomes of health systems (where the necessary digital resources are available).[21] The pandemic has shown that telehealth can function as a "safety net" while mitigating the devastating impact of a public health crisis, and has become an essential tool in building resilient health systems that are able to adapt to changing circumstances. Telehealth can also become a force multiplier for health systems given its ability to scale healthcare services, expand healthcare providers' reach to underserved areas and improve the efficiency of workflows.[22] Remote and real-time monitoring of the physiological and/or biochemical parameters of individuals (patients), in combination with other data, could enable timely diagnoses and treatments. New workflows, enhanced by artificial intelligence, could support integrated transition between virtual and in-person healthcare. In general, the growing social acceptance of digital health solutions and telehealth services is an opportunity to exploit and translate their capabilities into advancing the smart transformation of healthcare.[23]

In order to see the big picture, it is important to point out that healthcare providers scaled up the implementation of digital health solutions (especially telehealth services) so rapidly during the pandemic, because they were critical to ensure the delivery of healthcare services in a context where minimising face-to-face contacts between patients and health professionals was a priority. As health systems emerge from "non-regular" operations, there is a need to reassess regulation, compliance and processes with regard to telehealth services.

---

[20] Chapple C (2021) *Mobile Health & Fitness App Spending Jumped 70% Last Year in Europe to a Record $544 Million*. Sensor Tower (January 2021). Available from: <https://sensortower.com/blog/european-health-and-fitness-app-growth-2020>.

[21] Bhaskar S, Bradley S, Chattu VK *et al*. (2020) Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). *Frontiers in Public Health* 8(556720):1–15 at 11. DOI: <https://doi.org/10.3389/fpubh.2020.556720>.

[22] Temesgen ZM, DeSimone DC, Mahmood M, Libertin CR, Varatharaj Palraj BR, Berbari EF (2020) Health Care After the COVID-19 Pandemic and the Influence of Telemedicine. *Mayo Clinic Proceedings* 95(9):S66–S68 at S66–S67. DOI: <https://doi.org/10.1016/Fj.mayocp.2020.06.052>.

[23] Healthcare Information and Management Systems Society (2020) *eHealth Study: Non-clinical Telehealth Services Are Most Prevalent, but COVID-19 Accelerates New Trends*. HIMSS, Chicago (7 July 2020). Available from: <https://www.himss.org/news/ehealth-study-non-clinical-telehealth-services-are-most-prevalent-covid-19-accelerates-new>.

Regarding regulation, there is great expectation that the abovementioned, "relaxed" rules on the provision of telehealth will remain, which would help to sustain, expand and build on this new dimension of healthcare.[24] As for compliance, healthcare providers must take responsibility to ensure that they update the legal aspects of their "pandemic-borne" services to be in conformity with a "normal" (non-emergency) environment.[25] From the perspective of processes (business operations), some aspects of newly implemented or scaled digital health solutions will require recalibration, so that they can serve a broader set of objectives. On the long run, digital health solutions and telehealth services could realise their potential, if their design and configurations can meet the so-called 'SMART' criteria (an acronym derived from the following objectives):[26]

- straightforward to use;
- measurably impactful;
- agile and affordable;
- reliant on collaboration in research and innovation; and
- tailored to end-users' needs.

1.3.) Digital transformation of healthcare in the EU: policy initiatives in recovery from the COVID-19 public health crisis

In 2020, the European Parliament, the Council of the European Union and the European Commission adopted its 'Joint Conclusions on Policy Objectives and Priorities for 2020-2024 to drive the Union's recovery from the COVID-19 pandemic', while seizing the opportunity of digital transformation.[27] According to the document, the EU will facilitate cooperation on health and civil protection, building a European Health Union, while

---

[24] Temesgen *et al*., *supra* note 22 at S66.

[25] Giacalone A, Marin L, Febbi M, Franchi T, Tovani-Palone MR (2022) eHealth, telehealth, and telemedicine in the management of the COVID-19 pandemic and beyond: Lessons learned and future perspectives. *World Journal of Clinical Cases* 10(8):2363–2368 at 2366. DOI: <https://doi.org/10.12998/wjcc.v10.i8.2363>.

[26] Deloitte Centre of Health Solutions (2020) *Digital transformation: Shaping the future of European healthcare*. Deloitte Centre of Health Solutions, London, 44. Available from: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-shaping-the-future-of-european-healthcare.pdf>.

[27] Joint Conclusions of the European Parliament, the Council of the European Union and the European Commission on Policy Objectives and Priorities for 2020-2024. 2021/C 451 I/02 (OJ C, C/451, 29.12.2020, 4). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020Y1229(01)>.

respecting national competences. In connection with digital transformation, the document acknowledges that the COVID-19 crisis accelerated hyper-connectivity and the integration of new technologies. Consequently, the EU needs to focus simultaneously on access to and protection of data, development of innovative technology and upgrading of infrastructure. Building on these commitments, the European Parliament, the Council of the European Union and the European Commission has annually issued Joint Declarations of EU Legislative Priorities. In their 2022 Joint Declaration, the three EU institutions agreed to give priority to achieve a Europe fit for the digital age and lead the way globally in developing trustworthy, secure and human-centric technology.[28] To achieve this, the institutions made commitments to prioritise their work on digital services and digital markets, artificial intelligence, data, and secure space-based communication.

In this regard, EU actions are guided by the 2020 'Communication on "A European strategy for data"' in which the Commission outlined its vision to develop a common single market for data and establish EU-wide common data spaces in strategic sectors and domains of public interest.[29] These common data spaces aim at overcoming legal and technical barriers to data sharing, data access and data use across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example by way of developing common rules for a given space. The objectives of common data spaces include: (i) the deployment of data-sharing tools and platforms; (ii) the creation of data governance frameworks; and (iii) improvement of the availability, quality and interoperability of data. In the healthcare sector, the EU aims to establish a Common European health data space, which it considers essential for advancements in preventing, detecting and curing diseases, and for making informed, evidence-based decisions in order to improve the accessibility, effectiveness and sustainability of healthcare systems.

According to the Appendix to the 'Communication on "A European strategy for data"': while EU data protection law has created a level playing field for the use of personal data concerning health,[30] data governance models are diverse and the landscape of digital

---

[28] Joint Declaration of the European Parliament, the Council of the European Union and the European Commission EU Legislative Priorities for 2022 2021/C. 514 I/01 (OJ C 514I, 21.12.2021, 1–4). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.CI.2021.514.01.0001.01.ENG>.

[29] 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, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066>.

[30] For counter-arguments *see* Chapter 3 Part 1.3.1.

health services remains fragmented, especially when in the provision of cross-border healthcare services. For this reason, the Commission aims to develop sector-specific legislative and non-legislative measures for the Common European health data space by:

- strengthening citizens' access to health data and portability of these data, and tackling barriers to cross-border provision of digital health services and products;
- facilitating the establishment of a Code of Conduct relating to the processing of personal data in the health sector;
- deploying data infrastructures, tools and computing capacities, and supporting the development of national electronic health records (EHRs) and interoperability of health data through the application of the Electronic Health Record Exchange Format; and
- scaling cross-border exchange, linkage and usage of health data and specific kind of health information, such as EHRs, genomic information and digital health images, through secure, federated repositories.

The Commission presented this data strategy together with its 'Communication on "Shaping Europe's digital future"', which summarised the key actions that the Commission plans to take in order to ensure that digital solutions help Europe to pursue its own way towards digital transformation for the benefit of people and with respect to European values.[31] On the same day, the Commission also published its 'White Paper on Artificial Intelligence - A European approach to excellence and trust'[32], and accompanying 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics'[33]. The White Paper established a policy framework setting out measures to align European efforts for trustworthy and secure development of the AI ecosystem. It also laid out a risk-based approach with regard to a future regulatory framework for AI (which later

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Shaping Europe's digital future", COM(2020) 67 final, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52020DC0067>.

[32] White Paper "On Artificial Intelligence - A European approach to excellence and trust", COM(2020) 65 final, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065>.

[33] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics", COM(2020) 64 final, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0064>.

materialised in the proposal for an AI Act). According to the White Paper, this approach entails that an AI application should be high-risk, if it meets the following criteria:

(a) the AI application is employed in a sector (e.g. healthcare) where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur; and

(b) the AI application in the sector in question is, in addition, used in such a manner that significant risks are likely to arise (but for example, a flaw in the AI-enabled appointment scheduling system in a hospital will normally not pose risks of such significance to justify distinct regulatory intervention).

The Commission presented its aforementioned strategies just before the public health crisis in Europe, but then, the pandemic radically changed the role and perception of 'digital' in society and economy, and accelerated digital transformation. This rationale led to the joint declaration by the European Parliament, the Council and the Commission of the 'European Declaration on Digital Rights and Principles for the Digital Decade' in which the three institutions outline the EU's common vision for digital transformation.[34] The Declaration defines a set of principles for human-centred digital transformation based on European values. The Commission warned in its accompanying Communication that the burgeoning availability of new digital technologies and data comes with undesirable risks.[35] To ensure a protected, secure and safe online environment, the Declaration, therefore, strengthens privacy and individual control over data, and reinforces their implementation through policy initiatives and application with existing rights and principles for the overall public interest. In addition to proclaiming that "[e]veryone has the right to the protection of their personal data online", the Declaration adds that "that right includes the control on how the data are used and with whom they are shared." The EU also commits to "ensuring the possibility to easily move personal data between different digital services". In healthcare, the EU is committed to "facilitating and supporting seamless, secure and interoperable access across the Union to digital health and care services, including health records, designed to meet people's needs." Regarding interactions with algorithms and AI systems, the Declaration sets forth that the EU is committed to "ensuring transparency about the use of algorithms

[34] European Declaration on Digital Rights and Principles for the Digital Decade, COM(2022) 28 final, Brussels (26 January 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2022:28:FIN>.

[35] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Establishing a European Declaration on Digital rights and principles for the Digital Decade", COM(2022) 27 final, Brussels (26 January 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0027>.

and artificial intelligence, and that people are empowered and informed when interacting with them." This includes "providing for safeguards to ensure that artificial intelligence and digital systems are safe and used in full respect of people's fundamental rights."

Finally, in terms of sector-specific policy measures, the Commission presented (with its proposal for a Regulation on the European Health Data Space) its 'Communication on "A European Health Data Space: harnessing the power of health data for people, patients and innovation"'.[36] The European Health Data Space (EHDS) is the first common EU data space to emerge from the European strategy for data. The Communication explained that the EHDS is a key pillar of the European Health Union that aims to strengthen preparedness and response to cross-border health threats, and deliver resilient health systems.[37] The EHDS intends to address the problem that healthcare delivery and innovation are hampered by often incompatible digital health solutions, fragmented standards and specifications, and different legal and administrative rules, including variations in the implementation of the GDPR. For this reason, the objectives of the EHDS are to:

- empower individuals to control their health data;
- foster a single market for digital health services and products;
- ensure interoperability and security of health data and a level playing field for manufacturers;
- unleash the power of the health data economy; and
- ensure a consistent and efficient framework for the re-use of health data for research, innovation, policy-making and regulatory activities.

The EHDS would complement the EU's data-related legislative initiatives by providing tailor-made rules for the health sector. The overall aim of the EHDS is to provide a trustworthy setting for secure access to and processing of a wide range of health data based on data protection, cybersecurity, legality of processing data and personal control of data.

---

[36] Communication from the Commission to the European Parliament and the Council "A European Health Data Space: harnessing the power of health data for people, patients and innovation", COM(2022) 196 final, Strasbourg (3 May 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0196>.

[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Health Union: Reinforcing the EU's resilience for cross-border health threats", COM(2020) 724 final, Strasbourg (11 November 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0724>.

2.) Research design and methodology

2.1.) Problem statement, delimitations and research question

New enabling technologies and interconnected health data ecosystems could drive the "smart transformation" of healthcare from a merely reactive system to a data-driven system that provides personalised healthcare, real-time response solutions and prospective insights through the integration of clinical ("in-person") services and telehealth ("virtual") services. This transformation could improve the effectiveness, accessibility and resilience of health systems, and unlock the potential benefits outlined in the Commission's 'Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society' and accompanying Staff Working Document.[38] However, the EU and Member States must address a number of legal and operational issues in order to ensure that stakeholders can make the best use of digital technologies and data for health and well-being purposes.

According to the Synopsis Report of the public consultation survey carried out by the Commission in relation to the drafting of the aforementioned Communication, the majority of survey respondents stated that they did not have access to digital health services (e.g. remote monitoring, consultation with doctors or any kind of service provided through digital means).[39] However, of those who did not, two out of three respondents indicated that they would like to have access to digital health services. When the survey inquired about the possible reasons for this shortcoming, most respondents (79% of individuals and 62% of organisations) answered that they consider 'risks of privacy breaches' as the most significant barrier to electronic access to health data.[40] Similarly, most individuals (73%) answered that 'risks of privacy breaches' are the most significant barrier to electronic sharing of health data.[41] Overall, the conclusion of the public consultation was that individuals (as consumers

[38] See *supra* notes 7–8.

[39] European Commission Directorate-General for Communications Networks, Content and Technology (2018) *Consultation: Transformation health and care in the digital single market. Synopsis report*. Publications Office of the European Union, Luxembourg, 15. DOI: <https://data.europa.eu/doi/10.2759/18589>.

[40] *Ibid*., 8.

[41] *Ibid*., 9.

of healthcare) should have confidence and trust in digital health services that they will not be subject to unlawful processing of their personal data or interferences with their privacy.

The results of a public consultation presented in the 'EU initiative on a European Health Data Space (EHDS): Public Consultation Factual Summary Report' aggregated public opinion on digital health services and products, and the use of AI in healthcare.[42] The majority of respondents (65%) believed that telehealth entails additional risks for patients and doctors, such as risks linked to data security, misdiagnosis, unclear reimbursement systems, as well as the dehumanisation and depersonalisation of medical treatment. 63% of respondents stated that these risks should be addressed at EU level, primarily through the adoption of minimum standards for telehealth equipment (63%). Respondents suggested that a certification scheme granted by third parties would be the most appropriate measure to foster the uptake of digital health products and services at national and EU level (52%). In terms of AI, 69% of respondents believed that the introduction of AI in healthcare creates a new type of relationship between the AI system, the health professional and the patient (69%). While some thought this relationship was positive (bringing positive changes, such as acceleration and optimisation of healthcare, as well as fostering research and innovation), others stated that this would have downsides (e.g. worsening the level of trust between health professionals and patients, or decreasing patient confidence in the proposed solutions). An overwhelming majority (80%) believed that there are specific ethical issues involved in the use of AI in healthcare. For example, respondents answered that the use of AI creates risks related to the possibility that AI might draw wrong conclusions or create biases, which might lead to discrimination and inequalities. Respondents also expressed their concerns relating to the use of AI about data protection, transparency issues, and the dehumanisation of medicine.

In addition to the risks mentioned by respondents in the public consultations, "unfit-for-purpose" regulations have intensified legal challenges in digital health. The Impact Assessment Report accompanying the Commission's 'Proposal for a Regulation on the European Health Data Space' acknowledged that the regulatory framework has shown a limited effectiveness in supporting patients' control over their health data at national and

[42] EU initiative on a European Health Data Space (EHDS): Public Consultation Factual Summary Report, Ref. Ares(2022)636543 - 27/01/2022. Available from: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Digital-health-data-and-services-the-European-health-data-space/public-consultation_en>.

cross-border level and very low effectiveness on secondary use of health data.[43] As for the reasons, the Impact Assessment Report pointed to the fragmented and divergent legal and administrative rules, frameworks, processes, standards and infrastructures. According to the Impact Assessment Report, there are fragmented and limited tools for timely access to health data in electronic format and their digital transmission. There is also limited legal and technical interoperability, including in relation to cybersecurity and data protection aspects, across Member States that create barriers for providers of digital health services and products when entering the markets of other Member States. Furthermore, the growing diversity of national laws, regulations and administrative actions lead to obstacles to the free movement of data, which has a substantial impact on the free movement of digital technologies in healthcare that contact such data, the free movement of persons, and may lead to distortions in competition.

The EU aims to address the wide range of legal problems in digital health through the adoption of horizontal and sectoral legislative measures (and subsequently, non-legislative measures). However, regarding legislative measures relevant to digital health, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have pointed to inconsistencies and possible conflicts between generic/sectoral legal acts and legislative proposals regulating privacy, data protection and/or data governance matters. Major industrial players and trade associations have widely criticised the regulation of AI, and the potential uncertainties for healthcare. In addition to these, there is a great deal of concern over legal requirements with regard to the "blurring of the line" between medical devices and digital consumer health products (wellness applications). The integration of new technologies (e.g. IoT, AI) in increasingly complex health data ecosystems may intensify practical challenges and expose further regulatory deficiencies. Accordingly, the hypothesis of this research is that the proliferation of legislative measures may lead to uncertainties about their (possible) interaction, legal effects and effectiveness regarding their application in the context of digital health, and specifically, telehealth.

In terms of the scope of the research, the discussion centres on some of the most pressing and topical legal challenges in digital health. Digital health (and care) refers to the

---

[43] Commission Staff Working Document Impact Assessment Report Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final - SEC(2022) 196 final - SWD(2022) 130 final - SWD(2022) 132 final', SWD(2022) 131 final, Strasbourg (3 May 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0131>.

use of information and communication technologies (ICTs) to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health.[44] As the results of the abovementioned public consultations highlighted, privacy (and data protection) risks are the most significant legal challenge hindering the uptake of digital health services. Legal debates relating to privacy and data protection risks in digital health gained wider attention when the EU and Member States discussed the regulation of contact tracing and warning apps, and digital COVID certificates.[45] However, privacy and data protection challenges in other areas of digital health have not been under such scrutiny. The research aims to address this deficit by analysing the privacy and data protection aspects of three high-impact digital health solutions. With reference to a study prepared for the Commission on the health systems of France and Germany, which account for almost half of the EU-27 public health expenditures, digital health solutions could generate a value of €55 billion to these two countries.[46] Three use cases account for 40% of this value: a) remote monitoring of chronic disease patients; b) teleconsultation; and c) unified electronic health record/exchange system. Accordingly, this study focuses on privacy and data protection challenges relating to three corresponding topics (defined in detail below).

The first of these two use cases fall into the context of telehealth. By definition, telehealth solutions utilise information and communications technologies (ICT) to deliver healthcare (clinical) services or promote well-being by transmitting information between patients (users) and healthcare providers (or other stakeholders in the health data ecosystem), who are located at the communication endpoints and are separated by distance. Telehealth activities may encompass synchronous (real-time) or asynchronous (delayed) interactions between actors.[47] The main benefits of telehealth are typically associated with: (1) improved access to healthcare; (2) enhanced efficacy/quality/delivery/efficiency of healthcare

---

[44] European Commission (n.d.) *Public Health: Overview*. European Commission website. Available from <https://ec.europa.eu/health/ehealth-digital-health-and-care/overview_en> (accessed 1 October 2022).

[45] *See* European Commission (n.d.) *eHealth and COVID-19*. European Commission website. Available from <https://health.ec.europa.eu/ehealth-digital-health-and-care/ehealth-and-covid-19_en> (accessed 1 October 2022).

[46] European Commission Directorate-General for Communications Networks, Content and Technology, *supra* note 5, 26–27.

[47] International Organization for Standardization (2021) *ISO 13131:2021: Health informatics — Telehealth services — Quality planning guidelines*. International Organization for Standardization, Geneva, para. 3.5.2. Available from <https://www.iso.org/standard/75962.html>.

services; (3) equality of distribution of healthcare services; and (4) reduction of costs.[48] It is particularly valuable for those in remote areas, vulnerable groups and ageing populations.[49] It is relevant to point out that the terms 'telemedicine' and 'telehealth' are often used interchangeably, but this study opts to use the latter term (unless a legal reference states otherwise) to express the inclusion of non-clinical services (e.g. digital well-being applications). This is in line with a growing body of literature which argues that 'telemedicine' is reserved for the use of ICT to deliver clinical services at a distance, while 'telehealth' is a more generic term that also includes the delivery of non-clinical services to promote health and well-being.[50]

The technological dimension of this research focuses on new enabling technologies in telehealth. By way of explanation, an 'enabling technology' bears high transformative potential for the system in which it is deployed for a variety of uses and provides means to generate huge leaps in performance and capabilities for the user.[51] Enabling technologies may also trigger paradigmatic changes over time. The key enabling technologies discussed in this study (IoT, AI and video APIs) not only enable the delivery of new types of telehealth services, but they have begun to transform the very concept of healthcare by driving its digital transformation and shifting many aspects of it to the Internet. At the same time, the Internet (of Things) is expanding into an Internet of Everything (described in the next chapter). The title of this study (which was pre-determined by the call for the project) gives emphasis to these developments.

---

[48] Sood S, Mbarika V, Jugoo S *et al*. (2007) What Is Telemedicine? A Collection of 104 Peer-Reviewed Perspectives and Theoretical Underpinnings. *Telemedicine and eHealth* 13(5):573–590 at 575. DOI: <https://doi.org/10.1089/tmj.2006.0073>.

[49] World Health Organization (2016) *Global diffusion of eHealth: Making universal health coverage achievable. Report of the third global survey on eHealth*. World Health Organization, Geneva, 56. Available from: <https://apps.who.int/iris/handle/10665/252529>.

[50] *See* World Health Organization Global Observatory for eHealth (2010) *Telemedicine: Opportunities and developments in Member States. Report on the second global survey on eHealth*. Report of the third global survey on eHealth. World Health Organization, Geneva, 8–9. Available from: <https://apps.who.int/iris/handle/10665/44497>; European Commission Directorate-General for Health and Food Safety (2018) *Market study on telemedicine*. Publications Office of the European Union, Luxembourg, 25–26. DOI: <https://health.ec.europa.eu/system/files/2019-08/2018_provision_marketstudy_telemedicine_en_0.pdf>; Hashiguchi TCO (2020) *Bringing health care to the patient: An overview of the use of telemedicine in OECD countries*. OECD Health Working Paper No. 116, OECD Publishing, Paris, 10–11. DOI: <https://doi.org/10.1787/8e56ede7-en>.

[51] *See* OECD (2017) *New Health Technologies: Managing Access, Value and Sustainability*. OECD Publishing, Paris, 18. DOI: <https://doi.org/10.1787/9789264266438-en>; Martinelli A, Mina A, Moggi M (2021) The enabling technologies of industry 4.0: examining the seeds of the fourth industrial revolution. *Industrial and Corporate Change* 30(1):161–188 at 162. DOI: <https://doi.org/10.1093/icc/dtaa060>.

Considering that digital transformation in healthcare requires the implementation of resource-intensive and complex technologies, infrastructures and system architectures on the supply side, many healthcare providers opt to use cloud-based applications offered by healthcare online marketplaces and SaaS (Software-as-a-Service) platforms. In general, healthcare online marketplaces implement a B2C (business-to-customer) e-commerce business model to inform customers (patients) about the range of medical (and digital consumer health) products and services offered by providers on the market.[52] An online doctor marketplace is a specific type of healthcare online marketplace that connects patients with health professionals by pooling information about the supply side of the healthcare market. More specifically, the search engine functionality of an online doctor marketplace provides patients with prompt and structured information about the healthcare services on offer, available timeslots with various health professionals, the location of doctors' office (or the possibility to conduct teleconsultation with them), prices, as well as ratings and comments left by other patients.[53] Online doctor marketplaces may integrate communication application programming interfaces (APIs), such as video APIs offered by third parties, to enable teleconsultation between patients and health professionals. Online doctor marketplaces may also integrate SaaS applications, such as cloud-based electronic health records (EHR) and hospital information systems (HIS), into the functionalities and service offerings of their platform. In these cases, SaaS users (patients and healthcare providers) store data in the underlying cloud infrastructure of the platform, and use a client interface, such as a web browser or mobile application, to access them.[54] Given the cost, security and scalability benefits, healthcare SaaS is expected to become more prevalent and develop further in the future. Potential directions of development include: integration of AI to enable self-learning and autonomous SaaS applications; transfer to PaaS (Platform-as-a-Service)

---

[52] Aggarwal AK, Travers S (2001) E-commerce in healthcare: changing the traditional landscape. *Journal of Healthcare Information Management* 15(1):25–36 at 30. Available from: <https://pubmed.ncbi.nlm.nih.gov/11338906>.

[53] Emerline (2020) *Marketplace Platforms for Healthcare to Foster Medical and Insurance Processes*. Emerline, Mountain View (16 June 2020). Available from: <https://emerline.com/blog/marketplace-platforms-for-healthcare-to-foster-medical-and-insurance-processes>.

[54] Khalil S, Bou Abdo J (2022) Healthcare 4.0: Technologies and Policies. *In*: Makhoul A, Demerjian J, Bou Abdo J (eds) *5G Impact on Biomedical Engineering: Wireless Technologies Applications*. CRC Press, Boca Raton, 3–17 at 4–5. DOI: <https://doi.org/10.1201/9781003058434-1>.

business model that allows healthcare providers to develop customised applications; or the positioning of data centers closer to the edge of the network.[55]

With regard to these overarching legislative, technological and market developments, the main research question asks:

"What are the key privacy and data protection-related regulatory and compliance challenges that may undermine the use of new enabling technologies (IoT, AI) and B2C healthcare platforms (online doctor marketplaces) in telehealth?"

2.2.) Research disciplines, methods and sources

This interdisciplinary legal research study integrates legal and non-legal disciplinary methods to provide an informed and balanced narrative on privacy and data protection challenges relating to new enabling technologies and platformisation in telehealth. The underlying consideration to this is that privacy and data protection rules are 'context-relative informational norms'.[56] This means that their analysis depends on the distinct social context (e.g. healthcare) and/or technological context (e.g. IoT environment, AI ecosystem) in which they are interpreted and applied in. The general value of conducting interdisciplinary legal research is that it can help to grasp the forces (e.g. technological advancements, impact of COVID-19, social perceptions of privacy and data protection) that influence the legal system and how the law operates in action, in contrast to just by being interested only in the 'law as such'.[57] Furthermore, by combining legal science with other disciplines (computer science, health informatics, health management and ethics), an interdisciplinary narrative may provide ground for recommending future-proof rules, which could help to ensure normative certainty and effective implementation of policy objectives. "Law and ..." approaches (i.e. the combination of legal science with supplementary disciplines) can also shed light on

---

[55] Peranzo P (2022) *10 Healthcare SaaS Trends That Can Revolutionize the Medical Industry*. Imaginovation, Raleigh (7 February 2022). Available from: <https://imaginovation.net/blog/healthcare-saas-trends-that-revolutionize-medical-industry>.

[56] Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, 3.

[57] *See* Siems MM (2009) The Taxonomy of Interdisciplinary Legal Research: Finding the Way Out of the Desert. *Journal of Commonwealth Law and Legal Education* 7(1):5–17 at 12. DOI: <https://doi.org/10.1080/14760400903195090>.

different positions in the normative context with regard to various considerations, relationships, rights and interests.[58]

In terms of the research design and corresponding research methods and sources, Chapter 1 ('Towards an Internet of Healthcare: New Enabling Technologies and Their Integration in Telehealth') provides a state-of-the-art overview on how new enabling technologies are transforming digital health and opening up new opportunities in telehealth. Based on a literature review of academic and non-academic sources, the chapter conceptualises 'Internet of Healthcare' (based on the operationalisation of the concept of 'Internet of Everything'), and draws inferences about its implications to telehealth. The collection of sources followed a Boolean search logic based on the application of relevant terms and logical relationships between them. The chapter refers to a wide range of sources: books; articles published in scientific journals or conference proceedings; studies and white papers prepared by international organisations, ICT companies or consultancy services; and telecommunications standards issued by international or European standardisation bodies. The references address mostly technical-operational, systems engineering, medical physics, security and ethics issues relating to the use of new enabling technologies in healthcare. The study considers especially sources that feature cutting-edge solutions, good practices or widely recognised standards. The purpose of referring to these materials is to obtain additional scholarly and expert insights of recent developments in data-driven technologies and data governance arrangements in the field of health informatics. By definition, health informatics is the interdisciplinary study of the design, development, adoption and application of information and communications technologies in the delivery and management of healthcare services.[59] (In some circles, the broader term "biomedical and health informatics" is preferred to fully cover the scope of this rapidly changing field.[60])

Chapter 2 ('Internet of Health Things and Interconnected Software (AI Systems) Under EU Law: Qualification Rules and Data Protection Implications') applies the findings of the previous chapter to analyse the normative framework that determines the regulatory affairs and data protection aspects of two key enabling technologies (IoT and AI) in

---

[58] Smits JM (2014) Law and Interdisciplinarity: On the Inevitable Normativity of Legal Studies. *Critical Analysis of Law* 1(1):75–86 at 83. DOI: <https://resolver.scholarsportal.info/resolve/22919732/v01i0001/nfp_laiotinols.xml>.

[59] Healthcare Information and Management Systems Society (2017) *HIMSS Dictionary of Health Information Technology Terms, Acronyms, and Organizations* (Fourth Edition). CRC Press, Boca Raton, 101.

[60] Hersh W (2009) A stimulus to define informatics and health information technology. *BMC Medical Informatics and Decision Making* 9(24):1–6 at 1. DOI: <https://doi.org/10.1186/1472-6947-9-24>.

telehealth. The doctrinal component of the chapter encompasses analysis of the essential features of legislation and case law with the purpose of combining and synthesising all relevant normative elements in order to establish an arguably correct and complete statement of the law on the subject matter.[61] The legislative sources cover EU legal acts (and proposals) regulating the safety, health and quality requirements of (digital consumer health) products, medical devices and AI systems in healthcare. The analysis also touches upon Germany's national law regulating digital health applications on prescription, because it is a "blueprint" regulatory model that other EU Member States are expected to replicate in the near future. The underlying reason for the study of these legal regimes is that they have direct or indirect effects on the application of privacy, data protection, cybersecurity and AI governance rules. Considering that there are ongoing EU legislative procedures relevant to the subject matter, the analysis takes into account the latest available version (as of 1 October 2022) of compromise/resolution texts of legislative proposals. This implies references to the Council's mandate for negotiations with the European Parliament on the General Product Safety Regulation proposal[62] and to the Council's second Presidency compromise text on the AI Act proposal[63]. The study does not refer to draft resolution texts that the European Parliament did not vote on. In addition to these, the analysis incorporates the feedback of stakeholders in public consultations held in the course of these legislative procedures, which contain valuable recommendations on what the law should be (*lex ferenda*). Additional sources of the legal analysis include authoritative legal interpretations of EU legal acts: the relevant judgments and Advocate General opinions of the Court of Justice of the European Union (CJEU), as well as guidelines, opinions and other documents issued by the EDPB, the EDPS and the Medical Device Coordination Group (MDCG). Where authoritative interpretations are not available, the analysis interprets the law based on theoretical-legal reasoning with consideration to the technological and industrial realities.[64] Overall, the chapter considers problems affecting relevant legal acts (and proposals), thereby evaluating

[61] *See* Hutchinson T (2017) Doctrinal research: Researching the jury. *In*: Watkins D, Burton M (eds) *Research Methods in Law* (Second Edition). Routledge, Abingdon, 7–33 at 13. DOI: <https://doi.org/10.4324/9781315386669>.

[62] GPSR proposal, *infra* note 198.

[63] AI Act proposal, *infra* note 205.

[64] *See* Vaquero AN (2013) Five Models of Legal Science (Bertrán EG, trans.). *Revus* 19:53–81 at 76. DOI: <https://doi.org/10.4000/revus.2449>.

the adequacy of existing rules, highlighting flaws and recommending possible reforms to the law.[65]

Chapter 3 ('Privacy and Data Protection Aspects of Internet of Health Things') discusses privacy and data protection issues relating to one of the three high-impact digital health solutions examined in this research work (based on the potential value that those solutions represent to society, as mentioned above[66]). This chapter focuses on the assessment of privacy and data protection-related risks, rights and requirements associated with the use of IoT devices in telehealth. The chapter analyses what the implications of international human rights law (adopted within the UN and Council of Europe frameworks) and of EU privacy and data protection law are to IoT-enabled telehealth. Regarding EU law, the analysis focuses on the GDPR[67], the (Commission's) Data Act proposal[68], the (adopted) Data Governance Act[69], and their interaction in order to assess the legal bases for processing data concerning health generated by the use of Internet of Health Things, related rights, and the allocation of responsibilities in IoT-enabled telehealth ecosystems. In terms of related case law, the analysis refers to relevant decisions and legal interpretations of the UN Human Rights Committee, the European Court of Human Rights, the CJEU, the Article 29 Data Protection Working Party (predecessor of the EDPB), the EDPB, and the domestic courts of EU Member States. Additionally, references to academic commentaries and expert studies help to trace where the shortcomings are in the interaction of legal acts (and proposals), and to identify certain trends in case law.

Chapter 4 ('Data Protection Roles in Teleconsultation') analyses data protection challenges in teleconsultation (as the second high-impact digital health solution). Based on an industrial PhD collaboration with a company group providing healthcare platforms with telemedicine services, the chapter builds on empirical legal research findings to assess the functioning of data protection law in telemedicine. The case study begins by mapping the technical features of teleconsultation services offered by the four analysed healthcare platforms to their users via two video communications API services. As a matter of note,

---

[65] *See* Bhat PI (2019) *Idea and Methods of Legal Research*. Oxford University Press, New Delhi, 11. DOI: <https://doi.org/10.1093/oso/9780199493098.001.0001>.

[66] *See* European Commission Directorate-General for Communications Networks, Content and Technology, *supra* footnote 45.

[67] GDPR, *infra* note 313.

[68] Data Act proposal, *infra* note 73.

[69] Data Governance Act, *infra* note 585.

three platforms use the same video API service, while the fourth one uses a different video API service provider. The author collected empirical evidences through direct industrial collaboration with those four healthcare platforms. The technical analysis of the chapter builds on tutorials and developer guides published by the video communications API service providers. The structure of the legal analysis follows the relevant EDPB Guidelines; while content-wise, it is based on the publicly available privacy and data protection policy documents of the healthcare platforms and of the video communications API service providers. The purpose of this case study is to navigate through the complexities of determining data protection functional roles and allocation of responsibilities relating to the processing of personal data in the context of teleconsultation. The analysis provides an example of the various considerations that may emerge when a healthcare platform carries out a data protection impact assessment for teleconsultation.

Finally, Chapter 5 ('Online Doctor Marketplaces in the European Health Data Space') investigates the data protection implications of the European Health Data Space (EHDS) proposal[70] on the product development and business preparedness of online doctor marketplaces that offer telemedicine services. The analysis focuses on the general provisions of the EHDS proposal and its rules governing the primary use of electronic health data. The limitation of a purely doctrinal analysis of the EHDS proposal would be that it could not answer as comprehensively and accurately whether the law will be effective in practice, or whether any deficiencies may affect its implementation.[71] The assessment of the law, the evaluation of the underlying policy considerations, and the possible need for law reforms (amendments) require an empirical approach.[72] Therefore, this chapter combines doctrinal and empirical methods to evaluate the adequateness of the proposed legal provisions, and the possible actions that the online doctor marketplace is required to take in order to comply with the requirements of the EHDS proposal, or to exploit any related opportunities. Similarly to the previous chapter, the empirical findings of this chapter were collected in the course of an industrial PhD collaboration with an online doctor marketplace, and its data protection officers and technical development team.

---

[70] EHDS proposal, *infra* note 623.

[71] *See* Roberts P (2017) Interdisciplinarity in Legal Research. *In*: McConville M, Chui WH (eds) *Research Methods for Law* (Second Edition). Edinburgh University Press, Edinburgh, 90–133 at 105. DOI: <https://www.jstor.org/stable/10.3366/j.ctt1g0b16n.10>.

[72] *See* Dobinson I, Johns F (2017) Legal Research as Qualitative Legal Research. *In*: McConville M, Chui WH (eds) *Research Methods for Law* (Second Edition). Edinburgh University Press, Edinburgh, 18–47 at 20. DOI: <https://www.jstor.org/stable/10.3366/j.ctt1g0b16n.7>.

CHAPTER 1:
TOWARDS AN INTERNET OF HEALTHCARE: NEW ENABLING TECHNOLOGIES AND THEIR INTEGRATION IN TELEHEALTH

1.) Broader developments: the expansion of the Internet of Things to the Internet of Everything

1.1.) Internet of Things (IoT)

Healthcare is just one of the major domains in which the Internet of Things (IoT) has begun to spur a digital revolution. Despite the global buzz around IoT, there is no universally accepted definition for the term. Instead, various definitions describe or promote a particular view of the key attributes and purposes of IoT. Recital 14 of the Data Act proposal[73] defines 'IoT' as "physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service". On a large-scale, IoT envisions a pervasive, adaptive and self-configuring network that interconnects uniquely identifiable objects of the physical world (physical 'things') and of the information world (virtual 'things') with the use of standard and interoperable communication protocols.[74] IoT adds a new dimension to information and communications technologies by providing connectivity to digital telecommunications networks not only anytime, anywhere and for anyone, but also for any 'thing'.[75] The revolutionary feature of IoT is that 'things' make themselves recognisable and obtain intelligence by making or enabling context-related decisions due to their capability to communicate information about themselves.[76]

---

[73] 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 (23 February 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN> (henceforth: 'Data Act proposal').

[74] Minerva R, Biru A, Rotondi D (2015) *Towards a Definition of the Internet of Things (IoT)*. IEEE Internet Initiative (Rev. 1) (27 May 2015), 74. Available from: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>.

[75] International Telecommunication Union (2005) *ITU Internet Reports 2005: The Internet of Things*. International Telecommunication Union, Geneva, 3. Available from: <http://handle.itu.int/11.1002/pub/800eae6f-en>.

[76] Vermesan O, Friess P, Guillemin P *et al.* (2013) Internet of Things Strategic Research and Innovation Agenda. *In*: Vermesan O, Friess P (eds) *Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, Aalborg, 7–142 at 8. Available from: <http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf>.

Interactions with 'things' are facilitated by interfaces in the form of services, which can also query and change the state of 'things' and information associated with them.[77]

IoT builds on three pillars relating to the ability of 'smart objects' ('IoT devices'): (a) to be identifiable ("anything identifies itself"), (b) to communicate ("anything communicates") and (c) to interact ("anything interacts") either among themselves, building networks of interconnected objects, or with end-users or other entities in the network.[78] An IoT device is a piece of equipment that possesses the mandatory capabilities of communication and optional capabilities of sensing, actuating and/or data processing (such as data collection, data storage or data analysis).[79] An IoT device can collect data and convey it across digital communications networks to enable the performance of other processing operations; but it may also be capable of executing operations based on data received from digital communications networks.[80] Their inbound data and/or outbound commands are pipelined into or issued by an application system using (a relatively high degree of) human and/or computer-based intelligence.[81] According to their functionalities, IoT devices may fall into one or more of the following categories:[82]

(a) sensing and actuating device, which can detect or measure information relating to its surrounding environment and convert it into digital electronic signals, and may also convert digital electronic signals from the information networks into operations;

(b) data-carrying device, which is attached to a physical thing to indirectly connect the physical thing with the communication networks;

(c) data-capturing device, which refers to a reader/writer device with the capability to interact with physical things; and

---

[77] European Commission Directorate-General for the Information Society and Media (Sundmaeker H, Guillemin P, Friess P, Woelfflé S (eds) (2010) *Vision and Challenges for Realising the Internet of Things*). Publications Office of the European Union, Luxembourg, 43. DOI: <https://data.europa.eu/doi/10.2759/26127>.

[78] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10(7):1497–1516 at 1498. DOI: <https://doi.org/10.1016/j.adhoc.2012.02.016>.

[79] International Telecommunication Union (2012) *Overview of the Internet of things. Recommendation ITU-T Y.4000/Y.2060 (06/2012)*. International Telecommunication Union, Geneva, 1. Available from: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>.

[80] *Ibid*., 4.

[81] Minoli D (2013) *Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications*. John Wiley & Sons, Hoboken, 33. DOI: <https://doi.org/10.1002/9781118647059>.

[82] International Telecommunication Union, *supra* note 79, 4–5.

(d) general device (e.g. smartphone), which has embedded processing and communication capabilities and may communicate with the communication networks via wired or wireless technologies.

In order to identify the peculiar aspects of IoT devices (and associated challenges) in the healthcare domain, this work refers to IoT devices in the narrow sense (categories (a)–(c)), and considers general devices only to the extent that they possess any of the functionalities of devices belonging into categories (a)–(c).

1.2.) Internet of Everything (IoE)

The Internet of Everything (IoE) is a concept that describes the next wave of Internet growth and aims to look at the context in which IoT fits from a broader and more holistic perspective. The concept of expanding the Internet (the "INTERconnected NETwork of computers") to everything (every 'thing') describes the societal effort of expanding digital technologies and infrastructure in order to connect all objects in the world that we can identify and observe.[83] The term 'IoE' was coined by Cisco and defined as "*a network of networks*" that "*brings together people, process, data, and things to make networked connections more relevant and valuable than ever before – turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries.*"[84] This idea transcends the relatively passive perspectives on which IoT is founded ("data captured by sensors") to a far more active view, whereby actions in the physical world are what really matter ("data captured by sensors for the purpose of physical action as a consequence").[85]

The power of IoE derives from the vastly expanding possibilities of everything becoming a part of the global digital communications network. By connecting people,

---

[83] Dinc E, Kuscu M, Bilgin BA, Akan OB (2019) Internet of Everything: A Unifying Framework Beyond Internet of Things *In*: Cardoso PJS, Monteiro J, Semião J *et al*. (eds) *Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities*. IGI Global, Hershey, 1–30 at 2. DOI: <https://10.4018/978-1-5225-7332-6.ch001>.

[84] Evans D (2012) *The Internet of Everything: How More Relevant and Valuable Connections Will Change the World*. CISCO Internet Business Solutions Group, San Jose, 2–3. Available from: <https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf>.

[85] i-Scoop (n.d.) *What the Internet of Everything really is – a deep dive*. i-Scoop (accessed 1 October 2022). Available from: <https://www.i-scoop.eu/internet-of-things-iot/internet-of-everything-2>.

process, data and things, the exponential power of networks (commonly referred to as 'network effects' and associated with 'Metcalfe's law') may create unprecedented opportunities–but also pose new risks.[86] The term 'network effects' describes the phenomenon when the net value or utility that an agent can derive from a good or service is affected by the number of agents using the same good or service within the ecosystem.[87] For example, in healthcare, if the number of patients using a certain type of IoT device increases, then the healthcare provider may obtain more data from patients. In turn, bigger datasets may improve the accuracy of data analyses underpinning medical diagnoses, and enable the healthcare provider to deliver more personalised medical treatments.

The concept of IoE brings together four components, which denote the following phenomena:

(a) people: the connection of people via the Internet in more relevant and valuable ways;
(b) things: the connection of physical objects to the Internet and each other;
(c) data: the generation of big data by people and things, and the transformation of data into meaningful and actionable information, which can facilitate faster and more intelligent decisions and action; and
(d) process: the delivery of the right information to the right person (or machine) at the right time and in the right place in an appropriate format.

These connections consist of the following types of communications:

(a) people-to-people (P2P) communications: technology-enabled interactions which leverage the network infrastructure, devices and applications in order to enable seamless communication and collaboration between people;
(b) machine-to-people (M2P) communications: interactions of technical systems with people for the purpose of providing or receiving information; and
(c) machine-to-machine (M2M) communications: interactions between networked devices courtesy of technology that enables them to exchange information and perform actions without manual intervention.

[86] Evans, *supra* note 84 at 5.

[87] Liebowitz SJ, Margolis SE (1994) Network Externality: An Uncommon Tragedy. *Journal of Economic Perspectives* 8(2):133–150 at 135. DOI: <https://doi.org/10.1257/jep.8.2.133>.

These heterogeneous interactions enable the creation of cyber-physical and cyber-biological systems that interlink the cyber, physical and biological worlds.[88] The interconnection of these three spheres are particularly prominent in the context of healthcare.

2.) Conceptualising an Internet of Healthcare

The promise of an Internet of Healthcare is that the intelligent interconnection of people, things, data and processes in digital health could increase medical intelligence and support decisions affecting health and well-being. Interconnected health data ecosystems could overcome inefficiencies in healthcare, which are often the repercussions of siloed datasets, manual data processing operations and/or uncoordinated/ad-hoc processes.[89] The Internet of Healthcare aims to exploit the new wave of "data in motion" by enhancing and leveraging the availability, interoperability, sharing and analyses of data concerning health. In addition to this, "anytime-and-anywhere connectivity" could shift the delivery of certain healthcare services from clinical settings to remote environments, while the integration of clinical ("in-person") and telehealth ("virtual") services could lead to the establishment of hybrid healthcare models. These developments could drive the "smart transformation" of healthcare from a "traditional" provider-centric and reactive system to a "new" patient-centric, data-driven and partially automated system that provides personalised healthcare, real-time monitoring and response solutions, as well as prospective insights. In turn, this could enable the reorganisation of healthcare from a fee-for-service (capitated) system to a value-based system that measures outcomes and encourages proactive prevention.[90]

---

[88] Bojanova I, Hurlburt G, Voas J (2014) Imagineering an Internet of Anything. *Computer* 47(6):72–77 at 72, 73, 75. DOI: <https://doi.org/10.1109/MC.2014.150>.

[89] Bradley J, Barbier J, Handler D (2013) *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience*. White Paper. CISCO Internet Business Solutions Group, San Jose, 13. Available from: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf>.

[90] NEJM Catalyst (2017) *What Is Value-Based Healthcare?* NEJM Catalyst, Waltham (1 January 2017). Available from: <https://catalyst.nejm.org/doi/full/10.1056/CAT.17.0558>; Chanchaichujit J, Tan A, Meng F, Eaimkhong S (2019) An Introduction to Healthcare 4.0. *In*: Chanchaichujit J, Tan A, Meng F, Eaimkhong S (eds) *Healthcare 4.0: Next Generation Processes with the Latest Technologies*. Palgrave Pivot, Singapore, 1–15 at 10. Available from: <https://doi.org/10.1007/978-981-13-8114-0_1>.

The interconnected perspective of an Internet of Healthcare has implications for individuals, public health and healthcare management. When an individual uses an IoT device to generate data concerning a unique health parameter (e.g. glucometer data), this can help the healthcare provider to understand a narrowly defined health trend (e.g. how a particular diet affects the individual's glucose levels). However, when that individual uses multiple IoT devices (or an IoT device with multiple functions), the healthcare provider may assemble a multifaceted portrait of the individual's health.[91] On a large scale, the combination of the health datasets of a group of individuals can generate new insights into population health, for example, on how particular health or environmental metrics interact with each other to produce certain outcomes. Similarly, healthcare providers may break down processes (e.g. treatment protocols, workflows or administrative duties) into their components, monitored by a device or data stream, in order to eliminate systematic efficiencies, and identify opportunities to improve outcomes.[92]

The emergence and uptake of the following key (new) enabling technologies are catalysing the development of an Internet of Healthcare:[93]

- IoT devices, whose primary/typical purpose is data collection, data transmission and data visualisation;
- cloud and scalable distributed computing, which provide on-demand computing resources, data storage, and advanced software services;
- big data, data science and AI, whose primary/typical purposes are to perform data analysis;
- distributed ledger technologies, whose primary/typical purpose is to ensure secure data exchanges;
- 5G broadband cellular networks, which provide faster, higher throughput, more reliable and enhanced mobile connectivity; and

---

[91] Bresnick J (2016) *Can Healthcare Exploit the $7 Trillion Internet of Everything?* Health IT Analytics (19 December 2016). Available from: <https://healthitanalytics.com/news/can-healthcare-exploit-the-7-trillion-internet-of-everything>.

[92] *Ibid*.

[93] *See also* Aceto G, Persico V, Pescapé A (2020) Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *Journal of Industrial Information Integration* 18:100129 at 2. DOI: <https://doi.org/10.1016/j.jii.2020.100129>; Al-Jaroodi J, Mohamed N, Abukhousa E (2020) Health 4.0: On the Way to Realizing the Healthcare of the Future. *IEEE Access* 8:211189–211210 at 211190–211191, 211200. DOI: <https://doi.org/10.1109/ACCESS.2020.3038858>.

- high-performance computing, which uses supercomputers and computer clusters to solve advanced computation problems.

Given their sector-specific peculiarities and (potential) significance in driving the transformation of healthcare delivery models, the following sections of this chapter provide a state-of-the-art overview on the technological aspects of IoT-enabled telehealth systems and their integration with cloud and scalable distributed computing, big data and data science methods (including AI systems).

3.) The technological aspects of IoT-enabled telehealth systems

3.1.) IoT-enabled telehealth systems

3.1.1.) Internet of Health Things devices

Internet of Health Things (IoHT) devices denote IoT-enabled medical devices and digital consumer health products (wellness applications) that incorporate embodied (body-centred) computing. In addition to the Internet-connectivity and communications capabilities of IoT devices, IoHT devices possess embedded human-physiological and/or -biochemical sensing capabilities.[94] This implies that IoHT devices function in proximity and develop relatively stable cyber-physical or cyber-biological connections with the human body.[95] IoHT devices utilise various embodied computing technologies and materials placed on, around or inside

[94] *See* Williams PAH, McCauley V (2016) Always Connected: The Security Challenges of the Healthcare Internet of Things. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (Reston, 12–14 December 2016)*, 30–35 at 30. DOI: <https://doi.org/10.1109/WF-IoT.2016.7845455>.

[95] *See* Liu X, Merritt J, Tiscareno KK *et al*. (2020) *Shaping the Future of the Internet of Bodies: New challenges of technology governance*. Briefing Paper (July 2020). World Economic Forum, Geneva, 7. Available from: <http://www3.weforum.org/docs/WEF_IoB_briefing_paper_2020.pdf>.

the human body.[96] The sensors of IoHT devices can perform measurements on the physiological and/or biochemical parameters of the human body (and its environment).[97]

Based on this conceptualisation, IoHT devices can be classified as follows:

- wearables (e.g. smart watch[98]);
- implantables (e.g. smart bionic limb[99]);
- embeddables (e.g. smart tattoo[100]);
- ingestibles (e.g. smart pill[101]); and
- non-invasives (e.g. smart health mirror[102]).

Alternatively, IoHT devices can be divided into three generation of devices (with each of the following categories representing a technological leap):[103]

- externally body-affixed devices;
- body-internal devices (where a portion of the device resides inside the body or accesses the body through the skin or an external body orifice); and
- body-melded devices (which melds the human mind with machines by injecting or implanting brain–computer interfaces that act in a bi-directional read/write manner, thereby enabling functional extension and externalisation of portions of the human

---

[96] Pedersen I, Iliadis A (2020) Introduction: Embodied Computing. *In*: Pedersen I, Iliadis A (eds) *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles*. MIT Press, Cambridge (USA), ix–xxxix at xvi. DOI: <https://doi.org/10.7551/mitpress/11564.001.0001>.

[97] Indrakumari R, Poongodi T, Suresh P, Balamurugan B (2020) The growing role of Internet of Things in healthcare wearables. *In*: Balas VE, Solanki VK, Kumar R (eds) *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*. Academic Press, London, 163–194 at 166–169. DOI: <https://doi.org/10.1016/B978-0-12-819593-2.00006-6>.

[98] *See e.g.* Chandel RS, Sharma S, Kaur S, Singh S, Kumar R (2022) Smart watches: A review of evolution in bio-medical sector. *Materials Today: Proceedings* 50(5), 1053–1066. DOI: <https://doi.org/10.1016/j.matpr.2021.07.460>.

[99] *See e.g.* Beyrouthy, T, Al Kork S, Korbane JA, Abouelela A (2017) EEG Mind Controlled Smart Prosthetic Arm – A Comprehensive Study. *Advances in Science, Technology and Engineering Systems Journal* 2(3), 891–899. DOI: <https://doi.org/10.25046/aj0203111>.

[100] *See e.g.* Meetoo D, Wong L, Ochieng B (2019) Smart tattoo: technology for monitoring blood glucose in the future. *British Journal of Nursing* 28(2), 1–7. DOI: <https://doi.org/10.12968/bjon.2019.28.2.110>.

[101] *See e.g.* Cummins G (2021) Smart pills for gastrointestinal diagnostics and therapy. *Advanced Drug Delivery Reviews* 177:113931, 1–22. DOI: <https://doi.org/10.1016/j.addr.2021.113931>.

[102] *See e.g.* Miotto R, Danieletto M, Scelza JR, Kidd BA, Dudley JT (2018) Reflecting health: smart mirrors for personalized medicine. *Npj Digital Medicine* 1(62), 1–7. DOI: <https://doi.org/10.1038/s41746-018-0068-7>.

[103] *See* Matwyshyn AM (2019) The Internet of Bodies. *William & Mary Law Review* 61(1):77–168 at 94–115. Available from: <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3827&context=wmlr>.

mind and possibly, cognitive enhancement on the basis of a merger between biological and machine intelligence).

IoHT devices connect (the digital representation of) people to the Internet. As technology evolves, IoHT devices have enabled people to even become nodes of the Internet themselves (when the person becomes a so-called 'cyborg', which stands for "cybernetic organisms",[104] while the corresponding network phenomenon is described as the 'Internet of Bodies' or 'Internet of Living Things'[105]). However, these advancements are turning the human body into a potential "data platform". The "melding of bits and bodies" (i.e. the entwining of human flesh with hardware, software and algorithms) will challenge the nature and applicability of fundamental legal concepts. For example, IoT-enabled neurotechnology devices pose significant challenges to 'informational privacy' and 'informational self-determination', which are prerequisites to exercising rights derived from 'human (patient's) autonomy'.[106] For this reason, there is a pressing need to deliberate the protection of cerebral activity and data, and to adopt a new set of 'neuro-rights' in order to effectively safeguard individuals' cognitive liberty, mental privacy, mental integrity and psychological continuity in a new technological era.[107]

3.1.2.) Accompanying components to Internet of Health Things devices

RFID (Radio Frequency Identification) is one of the core enabling technologies of IoT. RFID systems are typically composed of three main components: RFID tags, a reader (also referred to as a transmitter/receiver) and an application system (also known as a data processing system, which can be a software application or database).[108] In an IoT-enabled telehealth context, RFID tags can collect data about the human body (and its environment) and

---

[104] Kreutzer RT, Sirrenberg M (2020) *Understanding Artificial Intelligence: Fundamentals, Use Cases and Methods for a Corporate AI Journey*. Springer, Cham, 63. DOI: <https://doi.org/10.1007/978-3-030-25271-7>.

[105] Pauwels E, Denton SW (2018) The Internet of Bodies: Life and Death in the Age of AI. *California Western Law Review* 55(1):221–233 at 225–226. Available from: <https://scholarlycommons.law.cwsl.edu/cwlr/vol55/iss1/5>.

[106] *See* Matwyshyn, *supra* note 103 at 163–164.

[107] Ienca M, Andorno R (2017) Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy* 13:5, 1–27. DOI: <https://doi.org/10.1186/s40504-017-0050-1>.

[108] Jia X, Feng Q, Fan T, Lei Q (2012) RFID technology and its applications in Internet of Things (IoT). *In: 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, (Yichang, 21–23 April 2012), 1282–1285 at 1283. DOI: <https://10.1109/CECNet.2012.6201508>.

communicate these data to the reader.[109] However, due to their cost and resource-constraint limitations, RFID tags and readers do not always have sufficient security protection, which makes them vulnerable to cyberattacks. [110]

One of the key components of IoHT devices are smart transducers.[111] In general, a transducer is either a sensor or an actuator depending on which direction information passes through the device: sensors detect the variations in input energy and convert these into a signal, while actuators operate in the reverse direction.[112] IoHT devices incorporate digital sensors for capturing data. Sensors convert physical, chemical, thermal or biological aspects of biorecognition events into a measurable (electrical) signal.[113] However, sensor data is inherently noisy and uncertain, and therefore requires "cleaning" and validating. This requires the programming of data models ('data integration') in the sensor node before its use.[114] The data that the sensor node generates is stored in its memory. The sensor can capture data through pull-based or push-based approaches. In the pull-based approach, the sensor captures data at a user-defined frequency, whereas in the push-based approach, sensors only send data based on an agreed behaviour between the sensor node and the base station (e.g. only deviating values are transmitted).[115]

IoHT devices consist of a (physical) hardware device and (physically embedded or externally located) interconnected software. Regarding the management of these resources, IoHT devices may have their own operating systems, but often need the support of companion apps running on a smart mobile device operating system to unlock certain

---

[109] Fan K, Jiang W, Li H, Yang Y (2018) Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE Transactions on Industrial Informatics* 14(4), 1656–1665 at 1656. DOI: <https://doi.org/10.1109/TII.2018.2794996>.

[110] Jia *et al*., *supra* note 108, 1285.

[111] Dei M, Aymerich J, Poitto M, Bruschi P, Javier del Campo F, Serra-Graells F (2019) CMOS Interfaces for Internet-of-Wearables Electrochemical Sensors: Trends and Challenges. *Electronics* 8(2):150 at 1. DOI: <https://doi.org/10.3390/electronics8020150>.

[112] *See* Busch-Vishniac IJ (1999) *Electromechanical Sensors and Actuators*. New York, Springer, 4, 8. DOI: <https://doi.org/10.1007/978-1-4612-1434-2_1>; Fraden J (2015) *Handbook of Modern Sensors: Physics, Designs, and Applications* (Fifth Edition). Cham, Springer, 3. DOI: <https://doi.org/10.1007/978-3-319-19303-8_1>.

[113] Naresh V, Lee N (2021) A Review on Biosensors and Recent Development of Nanostructured Materials-Enabled Biosensors. *Sensors*, 21(4):1109 at 3. DOI: <https://doi.org/10.3390/s21041109>.

[114] European Commission Directorate-General for Communications Networks, Content and Technology, Maier N, De Michiel F, Peter V *et al*. (2022) *Study to support an impact assessment for the review of the database directive.* Final report. Publications Office of the European Union, Luxembourg, 165. DOI: <https://data.europa.eu/doi/10.2759/647387>.

[115] *Ibid*.

functions.[116] Companion apps are usually available for users to download from app stores. Many IoHT devices connect through Bluetooth to the user's smartphone in order to make connections via the Internet, which the IoHT device itself might not support in isolation.[117]

3.1.3.) Architecture of IoT-enabled telehealth systems and networks

An IoHT device is a component of an IoT-enabled telehealth systems and network architecture that enables remote connection between a patient and a healthcare provider.[118] IoT-enabled telehealth networks can be conceptualised and classified according to their core aspects, such as:[119]

- topology, which refers to the physical configurations, application scenarios, activities and use cases;
- architecture, which refers to the specifications of the system's physical elements, their functional organisation, working principles and techniques) and
- platform, which refers to the network platform model and the computing service platforms.

The conceptual model of a typical IoT-enabled telehealth system would include the following physical elements and connections:[120]

- the body area network (WBAN) consisting of one or more IoHT devices and a central node (e.g. personal smartphone);
- short-range data transmissions between the IoHT device(s) and the central node;

---

[116] Commission Staff Working Document Accompanying the Document 'Report from the Commission to the Council and the European Parliament: Final report - Sector inquiry into consumer Internet of Things, COM(2022) 19 final', SWD(2022) 10 final, Brussels (20 January 2020), 53. CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0010>.

[117] *Ibid*.

[118] Rodrigues JJPC, Segundo DBDR, Junqueira, HA *et al*. (2018) Enabling Technologies for the Internet of Health Things. *IEEE Access* 6:13129–13141 at 13130. DOI: <https://doi.org/10.1109/ACCESS.2017.2789329>.

[119] Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak, KS (2015) The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* 3:678–708 at 679–683. DOI: <https://doi.org/10.1109/ACCESS.2015.2437951>.

[120] *See* Baker SB, Xiang W, Atkinson I (2017) Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* 5:26521–26544 at 26523–26524. DOI: <https://doi.org/10.1109/ACCESS.2017.2775180>; Elhayatmy G, Dey N, Ashour AS (2018) Internet of Things Based Wireless Body Area Network in Healthcare. *In*: Dey N, Hassanien AE, Bhatt C (eds) *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. Springer, Cham, 3–20 at 5–6. DOI: <https://doi.org/10.1007/978-3-319-60435-0_1>.

- long-range data transmissions between the central node and the application service; and
- the application service.

International and European technical standards organisations, as well as scholars, have defined several other conceptual models (reference models, reference architectures) for IoT-enabled system architectures[121], eHealth system architectures[122], and IoT-enabled telehealth system architectures[123]. However, the sheer number of conceptual models indicate that there are difficulties in establishing common grounds for these architectures. One of the most relevant conceptual models for IoT-enabled telehealth system and network architectures is the generic IoT reference model drawn up by the International Telecommunication Union, which is composed of the following four layers:[124]

- the application layer, which contains the IoT applications;

---

[121] *See* Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials* 17(4):2347–2376 at 2348–2350. DOI: <https://doi.org/10.1109/COMST.2015.2444095>; International Organization for Standardization, International Electrotechnical Commission (2018) *ISO/IEC 30141:2018(en) Internet of Things (IoT) — Reference Architecture*. International Organization for Standardization, Geneva, paras. 8–10. Available from: <https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en>; IEEE Standards Association (2019) *IEEE 2413-2019 - IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*. IEEE Standards Association, Piscataway. Available from: <https://standards.ieee.org/standard/2413-2019.html>.

[122] *See* European Telecommunications Standards Institute (2009) *ETSI TR 102 764 V1.1.1 (2009-02): eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth*. Technical Report. European Telecommunications Standards Institute, Sophia Antipolis. Available from: <https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf>; European Telecommunications Standards Institute (2020) *ETSI TR 103 477 V1.2.1 (2020-08): eHEALTH; Standardization use cases for eHealth*. Technical Report. European Telecommunications Standards Institute, Sophia Antipolis. Available from: <https://www.etsi.org/deliver/etsi_tr/103400_103499/103477/01.02.01_60/tr_103477v010201p.pdf>.

[123] *See* Catarinucci L, Donno DD, Mainetti L *et al*. (2015) An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal* 2(6):515–526 at 517. DOI: <https://doi.org/10.1109/JIOT.2015.2417684>; Sakr S, Elgammal A (2016) Towards a Comprehensive Data Analytics Framework for Smart Healthcare Services. *Big Data Research* 4:44–58 at 54–55. DOI: <https://doi.org/10.1016/j.bdr.2016.05.002>; Azimi I, Rahmani AM, Liljeberg P, Tenhunen H (2017) Internet of things for remote elderly monitoring: a study from user-centered perspective. *Journal of Ambient Intelligence and Humanized Computing* 8:273–289 at 275–276. DOI: <https://doi.org/10.1007/s12652-016-0387-y>; Da Costa CA, Pasluosta CF, Eskofier B, da Silva DB, da Rosa Righi R (2018) Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards. *Artificial Intelligence in Medicine* 89:61–69 at 64–65. DOI: <https://doi.org/10.1016/j.artmed.2018.05.005>; Indrakumari *et al*., *supra* note 97 at 164–166; Sahu SN, Moharana M, Prusti PC, Chakrabarty S, Khan F, Pattanayak SK (2020) Real-time data analytics in healthcare using the Internet of Things. *In*: Das H, Dey N, Balas VE (eds) *Real-Time Data Analytics for Large Scale Sensor Data*. Academic Press, London, 37–50 at 39–40. DOI: <https://doi.org/10.1016/B978-0-12-818014-3.00002-4>.

[124] International Telecommunication Union, *supra* note 79, 6–9.

- the service support and application support layer, which refers to generic support capabilities (such as data processing or data storage, which can be used by different IoT applications) and specific support capabilities (which cater for the requirements of diversified applications);
- the network layer, which refers to networking capabilities (for providing control functions of network connectivity, such as access and transport resource control functions, authentication, authorisation and accounting) and transport capabilities (for providing connectivity for the transport of IoT service- and application-specific data, and of IoT-related control and management information);
- the device layer, which refers to device capabilities (including capabilities to interact with the communications network) and gateway capabilities (including multiple interfaces support and protocol conversion);

and the following cross-layer associated capabilities:

- management capabilities, which refers to essential generic management capabilities (including device management, local network topology management, and traffic and congestion management) and specific management capabilities (coupled with application-specific requirements); and
- generic security capabilities, which are independent of applications, and include:
    - at the application layer: authorisation, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus;
    - at the network layer: authorisation, authentication, use data and signalling data confidentiality, and signalling integrity protection;
    - at the device layer: authentication, authorisation, device integrity validation, access control, data confidentiality and integrity protection) and
- specific security capabilities (coupled with application-specific requirements).

With regard to the IoT basic network model outlined by the International Telecommunications Union, an IoT-enabled telehealth network typically consists of the following components and networks:[125]

(a) the IoHT device;

---

[125] *See* International Telecommunication Union (2016) *Requirements of the network for the Internet of things. Recommendation ITU-T Y.4113 (09/2016)*. International Telecommunication Union, Geneva, 3–4. Available from: <https://www.itu.int/rec/T-REC-Y.4113-201609-I/en>.

(b) the gateway, which is a unit that interconnects the IoHT device(s) with the core network, and performs the necessary translation between the protocols used in the core network and those used by device;

(c) the IoHT body area network (BAN), which is a network of devices for the IoHT and gateways realised through local connections, typically using short-range communication technologies;

(d) the access network, which connects the IoHT devices and gateways to the core network (typically by fibre optics or radio access technologies);

(e) the core network, which is a portion of the delivery system composed of networks, equipment and infrastructures, and connects the service provider domain with the access network;

(f) the IoT platform is a technical infrastructure that provides an integration of the abovementioned generic and specific capabilities (in conjunction with capabilities of the core network), which can be connected with one or more IoT application servers; and

(g) the IoT application server runs applications and communicates with devices, gateways and the IoT platform directly or via the core network in order to deliver application services.

3.1.4.) Communication patterns in IoT-enabled telehealth systems

Data communications in IoT-enabled telehealth systems and networks have typical patterns, each of them possessing peculiar characteristics. These models shed light on the flexibility with which IoHT devices may connect and deliver value for stakeholders in the health data ecosystem. From a technical-operational point of view, there are four basic communication models in the context of IoT-enabled telehealth systems:[126]

1. The device-to-device communications model refers to two or more IoHT devices that directly connect and communicate with one another, rather than through an

[126] *See* Tschofenig H, ARM Ltd., Arkko J, Thaler D, McPherson D (2015) *Architectural Considerations in Smart Object Networking*. Internet Architecture Board (March 2015). Available from: <https://www.rfc-editor.org/rfc/rfc7452.txt>; Rose K, Eldridge S, Chapin L (2015) *The Internet of Things: an Overview. Understanding the Issues and Challenges of a More Connected World*. Internet Society (29 May 2020), 18–23. Available from: <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>.

intermediary application server. Device-to-device wireless networks allow IoHT devices, which adhere to a particular communication protocol (e.g. Bluetooth, Z-Wave, Zigbee), to exchange data in order to perform their functionalities. This model is common in short-range communications where small data packets of information are conveyed between devices with relatively low data rate requirements. In the context of IoT-enabled telehealth systems, an example of this communication model is the connection between Body Area Network (BAN) devices, such as the connection between a cadence sensor and a heart rate monitor. The functioning of IoHT devices under this communication model is usually based on device-specific data models developed by the manufacturer, and IoHT devices are often equipped with built-in security and trust mechanisms. Although the resource-constraint nature of IoHT devices requires many design decisions to accommodate device functionalities, it is desirable for both users and vendors, if two devices developed by two different manufacturers are interoperable.

2. In the device-to-gateway (also known as device-to-application layer gateway (ALG)) communications model, the IoHT device connects through an ALG service as a conduit to reach a cloud (or other scalable distributed computing) service. This means that there is an application software operating on a local gateway device, which acts as an intermediary between the IoHT device and the cloud (or other scalable distributed computing) service, and provides security and other functionalities, such as local authentication and authorisation, and data or protocol translation. Most IoT-enabled telehealth systems deploy this communications model. Since the majority of IoHT devices do not have the native ability to connect directly to a cloud (or other scalable distributed computing) service, they usually rely on a companion app or the software of a home "hub" device (typically installed to support ambient assisted living). In these cases, the smartphone or home hub device serves as the local gateway between personal IoHT devices and the cloud (or other scalable distributed computing) service, and may help to bridge the interoperability gap between IoHT devices.
3. In the device-to-cloud communications model, the IoHT device connects directly to a cloud service (as the application service provider) in order to exchange data and control message traffic. This new communications model enables innovation, which could accelerate the deployment of secure IoT solutions at previously unachievable

speeds.[127] However, it is noteworthy to mention that if proprietary data protocols are used between the device and the cloud service, in effect, the device owner or user could be tied to a specific cloud service (known as "vendor lock-in").

4. The back-end data-sharing communications model refers to a communication architecture that enables users to export and analyse data generated by an IoHT device in a cloud service (in combination with data obtained from other sources). This architecture enables the aggregation and analysis of data streams obtained from a single IoHT device. Moreover, this architecture enables users to grant permission to third parties to access their IoHT device data, and may facilitate data portability needs. Effective back-end data-sharing architectures can break down traditional data silo barriers by allowing users to move their data when they switch between IoT-enabled telehealth service providers. The implementation of the back-end data-sharing model requires either a federated cloud service or a cloud-based applications programming interface (API) in order to ensure the interoperability of IoHT device data.

In three of the communications models, IoHT devices may be used to connect to data aggregation, data analytics, data visualization or predictive analytics services in cloud computing. This can help to extract more value out of IoHT device data (compared to traditional data-silo applications). It is also important to point out that there are use cases when more than one of the abovementioned communications models describe the communications patterns of an IoT-enabled telehealth system. For example, this would be the case in an IoT-enabled ambient assisted living service that relies on smartphone-centric Wi-Fi device-to-device sensor communication.[128]

---

[127] *See also* IoT Business News (2019) *World's first IoT 'device-to-cloud' solution announced*. IoT Business News (27 November 2019). Available from: <https://iotbusinessnews.com/2019/11/27/50213-worlds-first-iot-device-to-cloud-solution-announced>.

[128] *See* Wåhslén J, Lindh T (2011) Smartphone-centric Wi-Fi device-to-device sensor communication for user mobility in AAL services. *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (Valencia, 4–8 September 2016)*. DOI: <https://doi.org/10.1109/PIMRC.2016.7794565>.

3.1.5.) IoT-enabled telehealth services and applications

The focus of this study is on IoT-enabled telehealth services, but it is important to point out that IoT devices can also support other healthcare services, such as hospital management or clinical services for hospitalised patients.[129] In general, IoT can enable a variety of healthcare services, each of which provides a set of healthcare applications. By explanation, an IoT-enabled healthcare service is by some means generic in nature, and has the potential to be a building block for IoT-enabled healthcare applications. In other words, services enable the development of applications, whereas applications are used directly by users (patients); services are developer-centric, while applications are user-centric.[130] For example, IoT-enabled remote health monitoring is an IoT-enabled telehealth service, whereas remote blood pressure monitoring is an IoT-enabled telehealth application.

One of the main types of IoT-enabled telehealth services are remote health monitoring services, which are a set of applications that meet four key criteria: (1) data concerning patient's health are collected remotely (e.g. in a home setting without direct medical oversight); (2) the collected data are transmitted to a healthcare provider (often via a third-party data analytics platform); (3) the data is evaluated by/for the healthcare provider; and (4) the healthcare provider communicates data-driven insights and possible health intervention needs to the patient. Depending on the classification criteria, 'remote health monitoring services' may encompass 'remote health prevention' and 'remote medical diagnoses' services. There is also promise for 'remote health treatment services' (e.g. IoT-enabled telesurgery). As regards IoT-enabled telehealth applications, they can be categorised into two sets of applications: single-condition applications (targeting a specific disease, infirmity or health aspect, e.g. glucose level monitoring) and clustered-condition applications (targeting several diseases, conditions or health aspects, e.g. medication management with the use of smart pills).[131]

---

[129] *See* Kulkarni A, Sathe S (2014) Healthcare applications of the Internet of Things: A Review. *International Journal of Computer Science and Information Technologies* 5(5):6229–6232 at 6230. Available from: <http://ijcsit.com/docs/Volume_5/vol5issue05/ijcsit2014050551.pdf>; Dey N, Ashour AS, Bhatt C (2017) Internet of Things Driven Connected Healthcare. *In*: Bhatt C, Dey N, Ashour AS (eds) *Internet of Things and Big Data Technologies for Next Generation Healthcare*. Springer, Cham, 3–12 at 7. DOI: <https://doi.org/10.1007/978-3-319-49736-5_1>.

[130] Islam *et al*., *supra* note 119 at 687.

[131] *Ibid*., 684–685.

In addition to the foregoing, there are further (cross-cutting) categories commonly used to describe certain IoT-enabled telehealth services or applications. For example, IoT-enabled 'ambient assisted living' (AAL) services aim to reinforce the health and well-being of senior and disabled people.[132] Another example is the delivery of IoT-enabled telehealth services via mobile communication devices, which is known as 'mHealth' or 'Internet of m-Health Things' (m-IoHT).[133] The potential synergy between mHealth and smart cities led to the conceptualisation of 'smart health' ('s-health'), which is the provision of healthcare services by use of the context-aware network and sensing infrastructure of smart cities.[134] On the level of applications, there are so-called 'context-aware IoT-enabled telehealth applications', which have visual (camera-based) sensing capabilities and/or are capable of monitoring environmental parameters.[135]

3.2.) Integrating cloud and scalable distributed computing with IoT-enabled telehealth systems

3.2.1.) Initial reasons for integrating cloud and scalable distributed computing with IoT-enabled telehealth systems

The development of IoT-enabled telehealth systems rely on advancements in network infrastructure and delivery of computing resources. In terms of network infrastructure, 5G provides agile connectivity with higher performance through its enhanced Mobile

---

[132] Syed L, Jabeen S, Manimala S, Alsaeedi A (2019) Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques. *Future Generation Computer Systems* 101:136–151 at 137. DOI: <https://doi.org/10.1016/j.future.2019.06.004>.

[133] World Health Organization (2011) *mHealth: New horizons for health through mobile technologies*. Based on the findings of the second global survey on eHealth. Global Observatory for eHealth series - Volume 3. World Health Organization, Geneva, 1. Available from: <https://apps.who.int/iris/handle/10665/44607>; Ahmadi H, Arji G, Shahmoradi L, Safdari R, Nilashi M, Alizadeh M (2019) The application of internet of things in healthcare: a systematic literature review and classification. *Universal Access in the Information Society* 18:837–869 at 839. DOI: <https://doi.org/10.1007/s10209-018-0618-4>.

[134] Solanas A, Patsakis C, Conti M *et al*. (2014) Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine* 52(8):74–81 at 76–77. DOI: <https://doi.org/10.1109/MCOM.2014.6871673>.

[135] Pateraki M, Fysarakis K, Sakkalis V (2020) Biosensors and Internet of Things in smart healthcare applications: challenges and opportunities. *In*: Dey N, Ashour AS, Fong SJ (eds) *Wearable and Implantable Medical Devices: Applications and Challenges*. Academic Press, London, 25–53 at 34–36. DOI: <https://doi.org/10.1016/B978-0-12-815369-7.00002-1>.

Broadband (eMBB), ultra-reliable low latency communications (URLLC), and ubiquitous access services.[136] This can enable the widespread use of IoT-enabled telehealth services, while facilitating their ad hoc orchestration. As regards computing resources, the proliferation and heterogeneity of Io(H)T devices, and significant growth in data and traffic, have led to the understanding that conventional centralised cloud-based data centres are no longer suitable to provide efficient and sustainable solutions to support rapidly developing Io(H)T systems and applications.[137] Instead, there is a trend to shift computing power and resources along the "cloud-to-thing continuum" towards the endpoints (edge) of the network in order to better cope with performance, availability, reliability, manageability and cost requirements.[138]

3.2.2.) Cloud and scalable distributed computing concepts and service models relevant to IoT-enabled telehealth systems

End-user IoT devices and near-user edge devices have created an acute need to carry out, with minimal latency, a substantial amount of data processing and to collaborate flexibly. This has triggered the development of more scalable, distributed and adaptive computational concepts, which aim to extend the capabilities of cloud computing.[139] Cloud and other scalable distributed computing concepts can be classified according to their location and

---

[136] Latif S, Qadir J, Farooq S, Imran MA (2017) How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare? *Future Internet* 9(93):1–24 at 19–20. DOI: <https://doi.org/10.3390/fi9040093>.

[137] Giannoutakis KM, Spanopoulos-Karalexidis M, Papadopoulos CKF, Tzovaras D (2020) Next Generation Cloud Architecture. *In*: Lynn PT, Mooney J, Lee B, Endo P (eds) *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles*. Palgrave Macmillan, Cham, 23–39 at 31. DOI: <https://doi.org/10.1007/978-3-030-41110-7_2>.

[138] *Cf. ibid*., 28; Skala K, Davidović D, Afgan E, Sovic I, Sojat Z (2015) Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing. *Open Journal of Cloud Computing* 2(1):16–24 at 18. DOI: <https://doi.org/10.19210/1002.2.1.16>.

[139] Iorga M, Feldman L, Barton R, Martin MJ, Goren N, Mahmoudi, C (2018) *Fog Computing Conceptual Model. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 500-325. U.S. Department of Commerce, National Institute of Standards and Technology, Washington, 1. DOI: <https://doi.org/10.6028/NIST.SP.500-325>.

distance from the device level and the core network (Internet backbone).[140] The main computing concepts are as follows:[141]

1. Cloud computing enables network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. The parties in cloud computing may act in the role of a cloud service provider, a cloud service (support) partner or a cloud service customer. There are four types of cloud deployments: private cloud, community cloud, public cloud and hybrid cloud. In terms of its functionalities (resources, capabilities), a cloud service may be offered as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). In addition to these, a provider may deploy on-premise, co-location or outsourced hosting models.[142] Co-location hosting refers to the option of renting space in a third-party data centre for IT equipment, while outsourced hosting refers to an outsource partner that provides, hosts and manages a custom-made system.[143]
2. Fog computing bridges the gap between centralised (cloud) services and end-devices (e.g. IoHT devices) by enabling computing, storage, networking and data management to take place in physical or virtual network (fog) nodes along the thing-to-cloud path (preferably in the close vicinity of end-devices) as data traverses to the cloud. The combination of fog and cloud computing may help to optimise services for IoT devices. As fog computing is essentially an extension of the traditional cloud-based computing model, the same architectural service models can be implemented

---

[140] *See* Yousefpour A, Fung C, Nguyen T *et al*. (2019) All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture* 98:289–330 at 289–298, 302. DOI: <https://doi.org/10.1016/j.sysarc.2019.02.009>.

[141] *Cf. ibid*., International Telecommunication Union (2014) *Information technology – Cloud computing – Overview and vocabulary. Recommendation Y.3500 (08/14)*. International Telecommunication Union, Geneva, 4–7. Available from: <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3500-201408-I!!PDF-E&type=items>; Iorga *et al*., *supra* note 139, 1–7; Beregi R, Pedone G, Mezgár I (2019) A novel fluid architecture for cyber-physical production systems. *International Journal of Computer Integrated Manufacturing* 32(4–5):340–351 at 340–347. DOI: <https://doi.org/10.1080/0951192X.2019.1571239>; Vermesan O, Coppola M, Nava MD *et al*. (2020) New Waves of IoT Technologies Research – Transcending Intelligence and Senses at the Edge to Create Multi Experience Environments. *In*: Vermesan O, Bacquet J (eds) *Internet of Things – The Call of the Edge: Everything Intelligent Everywhere*. River Publishers, Gistrup, 17–184 at 71–86. DOI: <https://doi.org/10.13052/rp-9788770221955>.

[142] Thorp J, Fletcher G, Wehnert J, Gessner C, Nicolas L (2015) *Report on the use of cloud computing in health*. Submitted as information to the members of the eHealth Network at their 8th meeting on 23 November 2015. Joint Action to support the eHealth Network, 13. Available from: <https://health.ec.europa.eu/system/files/2018-02/ev_20151123_co06_02_en_0.pdf>.

[143] *See ibid*.

(IaaS, PaaS, SaaS), and there are similar deployment modes (private fog node, community fog node, public fog node, hybrid fog node).

3. Edge computing encompasses various computing concepts in which computing is limited to the edge of the network (in contrast to fog computing, which is hierarchical and enables a wider range of functionalities). The 'edge' is the first hop from end-devices (e.g. IoHT devices), such as the Wi-Fi access point or the gateway.
4. Mist computing is a lightweight form of fog and edge computing that resides directly within the network constellations at the edge of the network. This brings the fog computing layer closer to end-devices. The mist nodes that form the mist computing layer are placed even closer to the peripheral devices than the more powerful fog nodes they collaborate with, often sharing the same locality with the end-devices that they service. These nodes are typically micro-computers and micro-controllers that feed data into fog computing nodes (and potentially, onward to cloud computing services).
5. Dew computing is computing at the extreme edge (in the end-devices themselves). It describes basic, embeddable extensions of the computing capabilities of individual, separate physical devices, independent of internetwork connectivity. Under this concept, IoHT devices have to cooperate on the lowest level to solve processing needs, and be able to transmit (and receive) data from all hierarchical levels of the network. Where heterogeneous devices act together to perform a set of tasks without connecting to cloud (or other "higher level") computing services, they create a so-called 'Dew of Things' environment.
6. Fluid computing is an architectural principle whose infrastructural abstraction provides an end-to-end mechanism that seamlessly provides, deploys, manages and monitors applications, regardless of whether the underlying resource is provided by cloud, fog, edge, mist or dew computing.

3.3.) Integrating data science techniques and AI systems with IoT-enabled telehealth systems

3.3.1.) Initial reasons for integrating data science techniques and AI systems with IoT-enabled telehealth systems

Given that data generated by the use of IoHT devices are large-scale, heterogeneous and mostly real-time, it is essential to ensure appropriate infrastructural resources and applications to process these big data.[144] 'Big data' not only refers to the huge quantity of data, but is a concept that describes the collection, storage, management, analysis and visualisation of extensive datasets with heterogeneous characteristics, where data processing is characterised by scale (volume), diversity (variety) and high speed (velocity).[145] 'Big data in health' encompasses consolidated data obtained from existing fragmented data sources for the purposes of understanding, forecasting and improving personal health status and health system performance.[146] In addition to data collected by IoHT devices, big data in health may originate from a variety of health data domains, such as: health registers, clinical trials, clinical quality registers, biobanks, genomics and other "-omics" datasets, laboratory data, health surveys/cohort studies, or socio-economic registers.[147] Big data sources may come in the following forms: a) structured data (e.g. data stored in a smart EHR or other personal health record); b) semi-structured data (e.g. data collected by an IoHT device about a particular health parameter); or c) unstructured data (e.g. socio-economic data or

---

[144] Anmulwar S, Gupta AK, Derawi M (2020) Challenges of IoT in Healthcare. *In*: Gupta N, Paiva S (eds) *IoT and ICT for Healthcare Applications*. Springer, Cham, 11–20 at 13–14. DOI: <https://doi.org/10.1007/978-3-030-42934-8_2>.

[145] *See* International Telecommunication Union (2015) *Big data – Cloud computing based requirements and capabilities. Recommendation Y.3600 (11/2015)*. International Telecommunication Union, Geneva, 2. Available from: <https://www.itu.int/rec/T-REC-Y.3600/en>.

[146] Csizmadia I, Láng R, Kis M (2020) *D5.1 - Report on policy action on innovative use of big data in health*. Information note: WP5 Innovative Use of Health data (v. 0.3) (2 February 2020). 17th eHealth Network meeting (June 2020). eHAction: Joint Action to support the eHealth Network, 12. Available from: <http://ehaction.eu/wp-content/uploads/2020/08/03.06.2020_eHN-adopted_eHAction-D5.1-Report-on-policy-action-on-innovative-use-of-big-data-in-health_v0.3-1.pdf>.

[147] Auffray C, Balling R, Barroso I *et al*. (2016) Making sense of big data in health research: Towards an EU action plan. *Genome Medicine* 8(71):1–13 at 2. DOI: <https://doi.org/10.1186/s13073-016-0323-y>; NordForsk (2019) *A vision of a Nordic secure digital infrastructure for health data: The Nordic Commons*. NordForsk, Oslo, 20. Available from: <http://norden.diva-portal.org/smash/get/diva2:1376735/FULLTEXT01.pdf>.

environmental data which can be used to improve the delivery of healthcare).[148] By enabling linkages between deep data (i.e. detailed data concerning health), or between deep data and broad data (population health data), big data can provide new insights for healthcare.[149] In healthcare, big data services can be used either for prospective (predictive or prescriptive) health data monitoring or retrospective (descriptive) health data analysis.[150]

3.3.2.) Technical specificities and classification of AI systems integrated with IoT-enabled telehealth systems

Raw, unstructured or semi-structured big data, such as those generated by the use of IoHT devices, can be transformed into 'smart data' (structured, accurate and agile datasets) by use of data science methods, which adds credibility (veracity) and relevance (value) to make data "actionable".[151] In the context of IoT-enabled telehealth services, data science is a multifaceted discipline that utilises statistics and data analytic methods, processes and algorithms to extract and visualise information from data generated by the use of IoHT devices (in combination with data originating from other health data domains). Data science applies specific algorithms to extract patterns from data ('data mining').[152] Machine learning algorithms can automate this data mining process.[153]

By explanation of relevant terms, programming manages rote tasks; 'machine learning' (ML) enables computers to learn how to best perform these rote tasks; and 'automated machine learning' (AML) can enable computers to learn how to optimise the

---

[148] *See* OECD, *supra* note 3, 148.

[149] OECD (Anderson G, Oderkirk J (eds)) (2015) *Dementia Research and Care: Can Big Data Help?* OECD Publishing, Paris, 14. DOI: <https://doi.org/10.1787/9789264228429-en>.

[150] Bresnick, *supra* note 91; Gesundheit Österreich Forschungs- und Planungs (2016) *Study on Big Data in Public Health, Telemedicine and Healthcare*. Final Report. Publications Office of the European Union, Luxembourg, 23. Available from: <https://op.europa.eu/s/w3wW>.

[151] *Cf.* Thovex C (2019) When Big Data and Data Science Prefigured Ambient Intelligence. *In*: Soldatos J (ed) *Smart Data: State-of-the-Art Perspectives in Computing and Applications*. Chapman and Hall/CRC, New York, 319–342 at 336. DOI: <https://doi.org/10.1201/9780429507670>; Luengo J, García-Gil D, Ramírez-Gallego S, Garcia S, Herrera F (2020) *Big Data Preprocessing: Enabling Smart Data*. Springer, Cham, 45. DOI: <https://doi.org/10.1007/978-3-030-39105-8>.

[152] Mayo M (2017) *The Data Science Puzzle, Revisited*. KDnuggets (25 January 2017). Available from: <https://www.kdnuggets.com/2017/01/data-science-puzzle-revisited.html>.

[153] *Ibid*.

outcome of learning how to perform these rote actions.[154] In general, a typical ML pipeline comprises of the following steps: (1) data preparation: data cleaning and pre-processing; (2) feature engineering: feature selection, extraction and construction; (3) model development: model selection and hyper-parameter optimisation; (4) model evaluation; and (5) model deployment.[155] The objective of AML is to simplify and "democratise" this pipeline, so that it can be made accessible to "citizen data scientists".[156] Within the ML sphere, 'deep learning' has gained a lot of attention recently, which uses deep neural network technology (i.e. artificial neural network architecture, as a specific type of ML algorithms, with multiple hidden layers) to handle large and complex datasets.[157] The "deep" in deep learning refers to the depth of layers in a neural network, which must consist of more than three node layers.[158]

'Artificial intelligence' (AI) refers to the ability of a system of algorithms to infer information from machine-generated and/or human-related (structured, semi-structured or unstructured) data with the purpose of generating outputs that influence the real and/or virtual environments with which the system interacts.[159] AI is essentially a "moving target" that is pursued through the implementation of data mining and ML/AML techniques. The novelty of AI is the ability to perform reasoning, planning, learning, communication or perception tasks without a human having to programme every step of the computing

---

[154] Mayo M (2017) *The Current State of Automated Machine Learning*. KDnuggets (25 January 2017). Available from: <https://www.kdnuggets.com/2017/01/current-state-automated-machine-learning.html>.

[155] Masood A (2021) *Automated Machine Learning: Hyperparameter optimization, neural architecture search, and algorithm selection with cloud platforms*. Packt Publishing, Birmingham, 22.

[156] *Ibid*., 23.

[157] Hoyt R, Muenchen R (2019) Artificial Intelligence. *In*: Hoyt R, Muenchen R (eds) *Introduction to Biomedical Data Science*. Informatics Education, Pensacola, 191–214 at 191.

[158] Kavlakoglu E (2020) *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?* IBM (27 May 2020). Available from: <https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks>.

[159] *See* High-Level Expert Group on Artificial Intelligence (2018) *A definition of AI: Main capabilities and scientific disciplines*. European Commission, Brussels (18 December 2018), 1 *et seq*. Available from: <https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf>; OECD (2019) *Scoping the OECD AI principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)*. OECD Digital Economy Papers, No. 291 (November 2019). OECD, Paris, 6 *et seq*. Available from: <https://doi.org/10.1787/d62f618a-en>.

process.[160] With regard to the independence of control, there are three models of systems according to the degree of human-machine interaction:[161]

- 'human in the loop': when the AI system needs human contributions at regular time intervals to be able to carry out its actions;
- 'human on the loop': if the AI system is capable of acting by itself based on previous programming, but the human can intervene by interrupting or modifying its actions at any time;
- 'human outside the loop': when the AI system acts independently during certain periods of time and, in these intervals, the human has no influence on its actions.

In this regard, AI-enabled automation is often portrayed as if a process is either automated or not, but in practice, automation is reflected more accurately by a spectrum of options:[162]

- human only (no AI involved);
- shadow mode (e.g. a human health professional analyses data and decides on a diagnosis, but an AI system shadows the health professional with its own attempt);
- AI assistance (e.g. a human health professional is responsible for the diagnosis, but the AI system may supply suggestions);
- partial automation (e.g. an AI system analyses data and, if it has high confidence in its decision, renders a diagnosis, but when it lacks confidence, it sends a requests to the human health professional to make the decision);
- full automation (e.g. AI makes the diagnosis).

AI is set to play an active role in the management of patients' health outside clinical settings.[163] An EU survey supports this expectation by indicating that healthcare organisations/start-ups are using, or are planning to use or develop AI primarily for patient

---

[160] *See* Samoili S, López Cobo M, Delipetrev B, Martínez-Plumed F, Gómez E, De Prato G (2021) *AI Watch. Defining Artificial Intelligence 2.0. Towards an operational definition and taxonomy for the AI landscape*. JRC Technical Reports. Publications Office of the European Union, Luxembourg, 23. DOI: <https://data.europa.eu/doi/10.2760/019901>.

[161] *See* European Commission Directorate-General for Health and Food Safety, Lupiáñez-Villanueva F, Gunderson L, Vitiello S (2022) *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*. Publications Office of the European Union, Luxembourg, 91. DOI: <https://data.europa.eu/doi/10.2875/702007>.

[162] Ng A (2021) *Face Datasets Under Fire, Baking With AI, Human Disabilities Baffle Algorithms, Ginormous Transformers.* DeepLearning.AI: The Batch (24 February 2021). Available from: <https://www.deeplearning.ai/the-batch/issue-80>.

[163] World Health Organization (2021) *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*. World Health Organization, Geneva, 9. DOI: <https://apps.who.int/iris/rest/bitstreams/1352854/retrieve>.

monitoring.[164] This outlook includes the uptake of an increasingly diverse range of direct-to-consumer AI-enabled IoHT devices (e.g. computer vision-driven ambient intelligence system, personalised virtual trainer).[165] Indeed, the use of AI for extracting knowledge and insights from raw data generated by the use of IoHT (in combination with data obtained from other health data domains) has huge potential to transform the delivery of healthcare.[166] When an IoT-enabled telehealth system integrates an AI system, then that AI system can interact with the human body and its environment through one or more IoHT devices. In other words, in an integrated IoT- and AI-enabled telehealth system, the AI system can extend the capabilities of the IoHT device(s), and *vice versa*.

In general, ML/AML techniques could transform evidence-based medicine (i.e. the use of current best evidence in making health-related decision about a patient's health) to improve diagnostics, predict outcomes and provide personalised healthcare through the analyses of real-world data (RWD) obtained from the use of IoHT devices.[167] However, there are concerns that AI could also foster the growth of "black box medicine", where health-related decision-making and data processing become increasingly opaque, while the outputs of the AI system are typically probabilistic and sometimes inscrutable.[168] This 'black box' phenomenon coupled with the complexities of ML/AML techniques have made the implementation of the concepts of 'eXplainable AI' (XAI) and 'responsible AI' increasingly important. By explanation, XAI refers to the understandability/intelligibility of the outputs

---

[164] European Commission Directorate-General for Communications Networks, Content and Technology, PwC (2021) *Study on eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union Lot 2: Artificial Intelligence for health and care in the EU.* Final Study Report. Publications Office of the European Union, Luxembourg, 39–45. Available from: <https://ec.europa.eu/newsroom/dae/redirection/document/80948>.

[165] Gerke S (2021) Health AI for Good Rather Than Evil? The Need for a New Regulatory Framework for AI-Based Medical Devices. *Yale Journal of Health Policy, Law, and Ethics* 20(2):432–512 at 444. Available from: <https://yaleconnect.yale.edu/get_file?pid=fd7fce9fbc17724a4b17d7f1ce4581a33c87d962fbbae12115c3217cdb56240>.

[166] Raeesi Vanani I, Amirhosseini M (2021) IoT-Based Diseases Prediction and Diagnosis System for Healthcare. *In*: Chakraborty C, Banerjee A, Kolekar M, Garg L, Chakraborty B (eds) *Internet of Things for Healthcare Technologies*. Springer, Singapore, 21–48 at 29–30. DOI: <https://doi.org/10.1007/978-981-15-4112-4_2>.

[167] Panesar A (2019) *Machine Learning and AI for Healthcare Big Data for Improved Health Outcomes*. Apress, New York, 12, 262. DOI: <https://doi.org/10.1007/978-1-4842-3799-1>.

[168] European Commission Directorate-General for Health and Food Safety *et al*., *supra* note 161, 88–89.

of the AI system, while 'responsible AI' is the large-scale implementation of AI methods with fairness, model explainability and accountability at its core.[169]

As regards explainability, it is important to consider the level of expertise of the actors involved, especially in light of the inherent asymmetries of information in healthcare, as well as the type of results produced by an AI system.[170] Based on these aspects, an AI system may perform tasks or provide information to qualified experts (typically health professionals) or non-qualified laypersons (individuals/patients). An example of an IoT-enabled telehealth system that integrates an AI system to perform a task for laypersons is an AI-enabled artificial pancreas.[171] An example of an IoT-enabled telehealth system that integrates an AI system to perform a task for qualified experts is an AI-enabled telesurgical robot.[172] An example of an IoT-enabled telehealth system that integrates an AI system to provide information for laypersons is an AI-enabled wearable device.[173] An example of an IoT-enabled telehealth system that integrates an AI system to provide information for qualified experts is an AI-enabled data analytics platform that supports health professionals in the remote monitoring of patients using IoHT devices.[174]

Finally, in terms of technological advancements, there is a promise to allocate data processing performed by AI systems from the cloud ("outsourced") level towards the edge of the network (device level).[175] Ultimately, as the deployment of AI system moves closer to the edge and becomes embedded into IoT devices (what is known as 'Artificial Intelligence of Things' or 'AIoT', or 'TinyML'), IoT devices may gain intelligence by

---

[169] Arrieta AB, Díaz-Rodríguez N, Del Ser J *et al*. (2020) Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion* 58:82–115 at 84–85, 103 *et seq*. DOI: <https://doi.org/10.1016/j.inffus.2019.12.012>.

[170] European Commission Directorate-General for Health and Food Safety *et al*., *supra* note 161, 92 *et seq*.

[171] *See* BBC (2022) *Cambridge: Artificial pancreas hailed success for diabetic children*. BBC (20 January 2022). Available from: <https://www.bbc.com/news/uk-england-cambridgeshire-60069369>.

[172] *See* McFarland A (2022) *Telerobotic System Helps Surgeons Remotely Treat Strokes*. UniteAI (17 April 2022). Available from: <https://www.unite.ai/telerobotic-system-helps-surgeons-remotely-treat-strokes>.

[173] *See* Carfagno J (2019) *First AI Medical Monitoring Wearable Approved by FDA for Home Use*. DocWireNews (24 April 2019). Available from: <https://www.docwirenews.com/docwire-pick/future-of-medicine-picks/first-ai-wearable-approved-by-fda-for-home-use-monitoring-vitals>.

[174] *See* Sulis E, Amantea IA, Aldinucci M *et al*. (2022) An ambient assisted living architecture for hospital at home coupled with a process-oriented perspective. *Journal of Ambient Intelligence and Humanized Computing* (online first). DOI: <https://doi.org/10.1007/s12652-022-04388-6>.

[175] Greco L, Percannella G, Ritrovato P (2020) Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern Recognition Letters* 135:346–353 at 347. DOI: <https://doi.org/10.1016/j.patrec.2020.05.016>.

acquiring the capabilities to perform self-driven analytics and act autonomously.[176] Developers can achieve this breakthrough through the advancement of microprocessing and the optimisation of how neural networks use the memory of IoT devices.[177] The significance of AIoT/TinyML solutions is that they may contribute to the further development of intelligent healthcare management systems with their capabilities to enhance human–technology interaction, strengthen the security of IoHT devices, and improve the accuracy of data collection and analytics.[178]

3.3.3.) Big data service models relevant to IoT-enabled telehealth systems

Big Data as a Service (BDaaS) is a cloud service category that provides cloud service customers the capabilities to collect, store, analyse, visualise and manage data using big data.[179] Cloud computing-based big data ecosystems include the following key functional roles: a) data provider (data supplier or data broker); b) big data service provider (big data infrastructure provider and big data applications provider); and c) big data service customer.[180] Considering that IoHT devices are resource-constraint (unless they are integrated with a smartphone or AIoT/TinyML solution), IoT-enabled telehealth systems require shared computing resources (typically cloud computing) to function as the middle layer between data generated by the use of IoHT devices and big data analytics. These big data services may provide IaaS, PaaS or SaaS.[181] Big data services offer flexible and scalable resources in order to provide connectivity to (and between) IoHT devices, and possess the

---

[176] Shamim MZ, Parayangat M, Thafasal Ijyas VP (2021) Distributed Intelligent Networks: Convergence of 5G, AI, and IoT. *In*: Usman M, Wajid M, Ansari MD (eds) *Enabling Technologies for Next Generation Wireless Communications*. CRC Press, Boca Raton, 137–148 at 138. DOI: <https://doi.org/10.1201/9781003003472>.

[177] Noone G (2022) *Putting AI in IoT chips? It's a question of memory.* Tech Monitor (10 February 2022). Available from: <https://techmonitor.ai/technology/ai-and-automation/tinyml-putting-ai-in-iot-chips-a-question-of-memory>.

[178] *See also* McGonigle D, Mastrian K (eds) (2021) *Nursing Informatics and the Foundation of Knowledge* (Fifth Edition). Jones & Bartlett Learning, Burlington, 619; Upadhyay D, Sharma S (2021) Convergence of Artificial Intelligence of Things: Concepts, Designing, and Applications. *In*: Sharma L (ed) *Towards Smart World: Homes to Cities Using Internet of Things*. CRC Press, Boca Raton, 119–142 at 133–135. DOI: <https://doi.org/10.1201/9781003056751>.

[179] International Telecommunication Union, *supra* note 145, 2.

[180] *Ibid*., 4–7.

[181] Biswas AR, Dupont C, Pham C (2017) IoT, Cloud and BigData Integration for IoT Analytics. *In*: Soldatos J (ed) *Building Blocks for IoT Analytics*. River Publishers, Aalborg, 11–38 at 12. DOI: <https://doi.org/10.13052/rp-9788793519046>.

capabilities to dynamically manage data generated by the use of IoHT devices. Of these, SaaS IoT applications are notable, which are usually built over a PaaS infrastructure, and use a combination of data from selected sensors within an integrated application.[182] The provision of on-demand access to the services of multiple sensors are known as 'Sensing as a Service' (or 'Sensing and Actuating as a Service'), while the enhancement of this service with more sophisticated analytics functionalities enables the provision of 'IoT Analytics as a Service'.[183]

[182] Soldatos J, Kefalakis N, Serrano M (2017) An Open Source Framework for IoT Analytics as a Service. *In*: Soldatos J (ed) *Building Blocks for IoT Analytics*. River Publishers, Aalborg, 99–138 at 100. DOI: <https://doi.org/10.13052/rp-9788793519046>.

[183] *Cf. ibid*., 100–101; Priya, Pathak I, Tripathi A (2018) Big Data, Cloud and IoT: An Assimilation. *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T) (Allahabad, 21–23 September 2018)*, 34–40 at 36. DOI: <https://doi.org/10.1109/IAC3T.2018.8674024>.

CHAPTER 2:

INTERNET OF HEALTH THINGS AND INTERCONNECTED SOFTWARE (AI SYSTEMS) UNDER EU LAW: QUALIFICATION RULES AND DATA PROTECTION IMPLICATIONS

1.) The significance of the legal qualification of Internet of Health Things (hardware) devices and interconnected software (AI systems)

The previous chapter explained that IoHT devices often require the integration of data science methods (for example, AI systems) to enable the transformation of raw big data into smart actionable data. However, manufacturers (economic operators, providers) of IoHT (hardware) and interconnected software (AI systems) face complex compliance challenges regarding the assessment of their regulatory obligations. Due to technological advancements and increased public demand for digital consumer health products (wellness applications), the "blurring of the borderline" between medical devices and wellness applications has become one of the most controversial issues in telehealth.[184] The crux of the problem is that there is a thin line between whether so-called "technologies for healthy lifestyle" fall under the scope of the highly regulated medical domain or the less regulated consumer products market.[185] Similarly, the line between medical and consumer neurotechnology IoHT devices has "blurred" due to the potential to use the latter to draw inferences about data subjects, and to repurpose them for medical uses.[186]

To underline the magnitude of the problem: by 2022, there were approximately 5,000-20,000 medical devices in the EU that were capable of processing patient's data, and approximately 100,000 mobile wellness applications, which do not fit within the category of 'medical device'.[187] Moreover, according to a projection, the telemedicine market may grow four times as large by 2027 compared to the 2020 base year at a compound annual growth

---

[184] Goraya T (2019) *Border issues: medical devices, wellbeing and lifestyle apps.* Taylor Wessing (1 March 2019). Available from: <https://www.taylorwessing.com/interface/2019/bodytech/border-issues-medical-devices-wellbeing-and-lifestyle-apps>.

[185] Lucivero F, Prainsack B (2015) The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle. *Applied & Translational Genomics* 4:44–49 at 47. DOI: <https://doi.org/10.1016/j.atg.2015.02.001>.

[186] *See* Paek AY, Brantley JA, Evans BJ, Contreras-Vidal JL (2021) Concerns in the Blurred Divisions Between Medical and Consumer Neurotechnology. *IEEE Systems Journal* 15(2):3069–3080. DOI: <https://doi.org/10.1109/JSYST.2020.3032609>.

[187] Commission Staff Working Document Impact Assessment Report Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final - SEC(2022) 196 final - SWD(2022) 130 final - SWD(2022) 132 final', *supra* note 43.

rate (CAGR) of around 25%.[188] These developments call for increased certainty pertaining to the regulation of IoHT (hardware) devices and interconnected software.[189] Considering that legal uncertainty increases compliance (integrity) risks, this may inadvertently affect the protection of the rights of individuals (consumers, patients) whose personal data are processed by IoHT (hardware) devices and interconnected software (AI systems). Against this background, this chapter analyses how the qualification of IoHT (hardware) devices and interconnected software (AI systems) according to general and specific (sectoral) EU legislation on safety, health and quality requirements affect the application of data protection (including cybersecurity, information security and AI governance) rules. The chapter also aims to pinpoint legal provisions that should be amended to clarify legal issues relating to IoHT (hardware) devices and interconnected software (AI systems).

2.) The qualification of Internet of Health Things (hardware) devices and interconnected software (AI systems) as product(s) or medical device(s)

2.1.) Qualification rules for Internet of Health Things (hardware) devices and interconnected software (AI systems) under general product safety legislation

With a view to building trust in digital health technologies, it is essential to ensure high standards of safety, health and quality in conformity with the intended parameters of a given application. However, the question of whether (or not) any safety, health and quality legal

[188] Fortune Business Insights (2021) *Telemedicine Market Size, Share & COVID-19 Impact Analysis, By Type (Products and Services), By Modality (Store-and-forward (Asynchronous), Real-time (Synchronous), and Others), By Application (Teleradiology, Telepathology, Teledermatology, Telecardiology, Telepsychiatry, and Others), By End User (Healthcare Facilities and Homecare), and Regional Forecast, 2020-2027.* Fortune Business Insights. Available from: <https://www.fortunebusinessinsights.com/industry-reports/telemedicine-market-101067>.

[189] *See* Lang M (2017) Heart Rate Monitoring Apps: Information for Engineers and Researchers About the New European Medical Devices Regulation 2017/745. *JMIR Biomedical Engineering* 2(1):e2 at 1–2. DOI: <https://doi.org/10.2196/biomedeng.8179>.

regime applies to IoHT (hardware) devices and interconnected software (AI systems) under EU law and, if yes, which one, is a grey area ridden with legal uncertainty. In order to fall under the scope of the general or specific legal regime prescribing safety, health and quality requirements, an IoHT (hardware) device or interconnected software (AI system) needs to be, legally speaking, either a 'product' or a 'medical device'. These concepts define the material scope of the relevant legal regimes and are fundamental to establishing which set of safety, health and quality requirements is applicable.[190] In case the interconnected software meets the definition of an 'AI system', then the foregoing legal qualification also affects the determination of the safety, health and quality requirements of that AI-enabled IoHT device.

2.1.1.) General Product Safety Directive

In the EU, the general legislation (*lex generalis*) which ensures that products placed on the market are safe is Directive 2001/95/EC on general product safety[191] (General Product Safety Directive, 'GPSD'). The GPSD lays down a broad-based, legislative framework of a horizontal nature by establishing at EU level "a general safety requirement for any product placed on the market, or otherwise supplied or made available to consumers, intended for consumers, or likely to be used by consumers under reasonably foreseeable conditions even if not intended for them."[192] As a jurisdictional rule, Article 3(2) of the GPSD provides that a "product shall be deemed safe, as far as the aspects covered by the relevant national legislation are concerned, when, in the absence of specific Community provisions governing the safety of the product in question, it conforms to the specific rules of national law of the Member State in whose territory the product is marketed."[193] In addition to European and

---

[190] *See also* Purtova N (2017) eHealth Spare Parts as a Service: Modular eHealth Solutions and Medical Device Reform. *European Journal of Health Law* 24:463–486 at 469. DOI: <https://doi.org/10.1163/15718093-12341430>.

[191] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2001, 4. ELI: <http://data.europa.eu/eli/dir/2001/95/2010-01-01> (henceforth: 'GPSD').

[192] *Ibid.*, Recitals (5)–(6).

[193] *Ibid.*, Article 3(2) first indent.

national 'hard law' provisions, "the conformity of a product to the general safety requirement shall be assessed by taking into account" (where they exist):[194]

- voluntary national standards transposing European standards;
- national standards in which the product is marketed;
- Commission recommendations setting guidelines on product safety assessment;
- product safety codes of good practice in force in the sector concerned;
- the state of the art and technology; and
- reasonable consumer expectations concerning safety.

The GPSD functions as a "safety net" for products and related risks that may affect the health and safety of consumers, but do not enter into the scope of specialised (sectoral) legislation. However, it is not clear whether this principle functions intactly in the cases of IoHT (hardware) devices and interconnected software (AI systems) and related health and safety risks, which are not covered by specialised legislation (addressed below). Even the Commission Staff Working Document 'On the existing EU legal framework applicable to lifestyle and wellbeing apps' (issued in 2014) noted that since the GPSD applies to 'manufactured products', "it is not yet clear if and to what extent they apply to lifestyle and wellbeing apps".[195] Considering that apps are a specific type of software, this legal uncertainty extends to all digital health software marketed in the EU, which do not fall under the definition of 'medical device'. In another remark, the Commission Staff Working Document added that "[i]t is not yet clear if and to what extent lifestyle and wellbeing apps could pose a risk to citizens' health". However, the GPSD was adopted *expressis verbis* "with a view to ensuring a high level of protection of safety and health of consumers".[196] Unless there will be a revision or authoritative (judicial) interpretation of the definition of 'product' to include software, it remains dubious whether (or not) the GPSD is applicable to lifestyle and well-being software that are not 'medical devices'.[197]

---

[194] *Ibid.,* Article 3(2) second indent and Article 3(3).

[195] 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"), SWD/2014/0135 final. CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014SC0135>.

[196] GPSD, *supra* note 191, Recital (5).

[197] Purtova, *supra* note 190, 474.

2.1.2.) General Product Safety Regulation proposal

The Proposal for a Regulation on general product safety[198] ('GPSR proposal'), which is intended to replace the GPSD, recognises that the "[t]he rapid development of new technologies also raises questions about the scope of some of the key concepts of the GPSD. The appearance of some new risks linked to connectivity, the applicability of the Directive to software updates and downloads as well as the evolving functionalities of AI-powered products raise the question whether the GPSD is clear enough to provide legal certainty for businesses and protection to consumers." According to the Explanatory Memorandum of the GPSR proposal, the Regulation intends to strengthen the safety net function of the legislative act, which includes clarifying the application of product safety rules to software. Although the GPSR proposal addresses several important challenges for product safety posed by digitalisation, the following arguments demonstrate that legal shortcomings and uncertainties would persist, if the GPSR proposal were applied to determine the qualification of IoHT (hardware) devices and interconnected software (AI systems).[199]

One of the criticisms is that medical devices and in vitro diagnostic medical devices should be among the list of products excluded from the scope of the GPSR proposal, similarly to the envisaged exclusion of medicinal products.[200] According to this argument: "the fundamental concept which underpins the CE marking of medical devices and IVDs is the obligation of manufacturers to ensure that an appropriate risk-benefit analysis is performed for both categories of products, leading to a positive benefit-risk ratio".[201] "Preamble 14 of the proposed General Product Safety Regulation justifies the exclusion of medicinal products on the basis of the fact that these 'are subject to a pre-market assessment that includes a specific risk-benefit analysis'. Since the same risk-benefit analysis exist in

---

[198] Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council (Mandate for negotiations with the European Parliament). General Secretariat of the Council of the European Union (2021/0170(COD), 11469/22) (20 July 2022). Available from: <https://data.consilium.europa.eu/doc/document/ST-11469-2022-INIT/en/pdf> (henceforth: 'GPSR proposal').

[199] For legal consequences of this qualification *see also* under this chapter: '3.1. Data protection and cybersecurity requirements deriving from the qualification of Internet of Health Things and interconnected software (AI systems) as (digital consumer health) product(s)'.

[200] MedTech Europe (2021) *MedTech Europe comment to the proposed Regulation on General Product Safety*. Feedback to General Product Safety Directive – review. MedTech Europe, Brussels (4 October 2021), 1. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review/F2674997_en>.

[201] *Ibid*.

the pre-market assessment of medical devices and IVDs, these health products should similarly be excluded from the scope of this proposed Regulation. Failure to implement this exclusion in the legal text would create immediate ambiguity in interpreting the specificity of the provisions of the IVDR and MDR via-à-vis those of the proposed Regulation."[202]

Regarding the material scope of the GPSR proposal, consumer organisation groups have called for the legal definition of 'product' to explicitly include software which may be incorporated in a connected product or downloaded after its placing on the market.[203] The new definition of 'product' does not mention *expressis verbis* 'software', but the wording 'any item, interconnected or not to other items'[204] may arguably cover IoHT (hardware) devices and interconnected software. In case software is an AI system, there are explicit references to determine the applicable legal regime. According to the Explanatory Memorandum of the GPSR proposal and Recital 82 of the Artificial Intelligence Act proposal[205] ('AI Act proposal'), the GPSR proposal applies as a safety net for 'AI systems related to products'[206] that are not high-risk according to the AI Act proposal (and, thus, are not subject to the corresponding requirements of the AI Act proposal). The Explanatory Memorandum of the GPSR proposal explains that 'with respect to product safety, the [AI Act proposal] will function like sectorial legislation, establishing specific requirements for AI applications, and the [GPSR proposal] will apply as a safety net for products and aspects not covered by other sectorial legislation to provide a legal basis for withdrawing such products to ensure an effective protection of consumers.'

In connection with the material scope, it is important to note that the GPSR proposal (similarly to the GPSD) is applicable only, if the product is supplied or made available "in

---

[202] *Ibid*.

[203] BEUC – The European Consumer Organisation, ANEC – European Association for the Co-ordination of Consumer Representation in Standardisation (2020) *BEUC and ANEC views for a modern regulatory framework on product safety: Achieving a higher level of consumer safety through a revision of the General Product Safety Directive*. Feedback to General Product Safety Directive – review. BEUC–ANEC, Brussels (26 August 2020), 7. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review/F545598_en>.

[204] GPSR proposal, *supra* note 198, Article 3(1).

[205] 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 (Second Presidency compromise text). Presidency of the Council of the European Union (2021/0106(COD), 11124/22) (15 July 2022). Available from: <https://data.consilium.europa.eu/doc/document/ST-11124-2022-INIT/en/pdf> (henceforth: 'AI Act proposal'). (The analysis takes into account the Commission's proposal and the amendments proposed in the latest available compromise text in the Council's co-legislative procedure.)

[206] As a matter of note, the wording 'AI systems related to products' does not necessarily imply that the AI system is the product itself.

the course of a commercial activity".[207] *A contrario*, IoHT (hardware) devices and/or interconnected software (AI systems), which specialised legislation does *not* cover and are *not* supplied or made available "in the course of a commercial activity", may not fall into the safety net of the GPSR proposal. This would entail that there would be a lack of legal protection relating to safety and health risks posed by IoHT (hardware) devices and/or interconnected software deployed in non-profit, 'in-house' or other non-commercial settings (e.g. a university-developed app for student wellbeing).

2.2.) Common qualification rules for Internet of Things (hardware) devices and interconnected software (AI systems) under the Medical Devices Regulation

Under EU law, the legislation on general safety, quality and performance requirements is complemented by specialised legal acts (*lex specialis*), which regulate the safety, quality and performance requirements of specific products or categories of products in a given sector.[208] In the medical sector, the legal acts that bear relevance to IoHT (hardware) devices and interconnected software (AI systems), insofar as certain conditions are satisfied, are the Regulation (EU) 2017/745 on medical devices[209] (Medical Devices Regulation, 'MDR') and the Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices[210] (*In Vitro* Diagnostic Medical Devices Regulation, 'IVDR').[211] The MDR and the IVDR repealed three directives:

---

[207] GPSR proposal, *supra* note 198, Article 3(1).

[208] Sectoral safety, quality and performance requirements are supplemented by horizontal legislation on safety, quality and performance requirements for AI systems (*see* AI Act proposal, *supra* note 205) and cybersecurity requirements for products with digital elements (*see* Cyber Resilience Act proposal, *infra* note 317).

[209] 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, OJ L 117, 5.5.2017, 1. ELI: <https://eur-lex.europa.eu/eli/reg/2017/745/oj> (henceforth: 'MDR').

[210] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117, 5.5.2017, 176. ELI: <https://eur-lex.europa.eu/eli/reg/2017/746/oj> (henceforth: 'IVDR').

[211] These legal acts are in a state of transition. *See* European Commission (n.d.) *Transition Timelines from the Directives to the Regulations: Medical Devices and in vitro Diagnostic Medical Devices*. Available from <https://ec.europa.eu/health/sites/health/files/md_newregulations/docs/md_infographic-timeline_en.pdf> (accessed 1 October 2022).

Directive 93/42 on medical devices,[212] Directive 98/79 on *in vitro* diagnostic medical devices[213] and Directive 90/385 on active implantable medical devices[214]. In order "to provide advice to the Commission and to assist the Commission and the Member States in ensuring a harmonised implementation of the [MDR]" (and IVDR), the MDR established the Medical Device Coordination Group ('MDCG').[215] The opinions and recommendations of the MDCG present a common understanding of how the MDR and IVDR should be applied in practice.[216] Although these documents are legally not binding, the Court of Justice of the European Union ('CJEU') has referred to the MEDDEV guidelines (which the MDCG documents replaced following the adoption of the MDR) as sources supporting its legal interpretation.[217] As Advocate General Campos Sánchez-Bordona explained: "[t]hrough the guidelines, the Commission seeks to provide manufacturers with guidance on the application of [the MDD]. Drawn up in collaboration with the authorities of the Member States, the Commission's services, the healthcare industry and accredited bodies in that sector, the guidelines reflect the interpretation of the legislation which is used in practice."[218]

The material scope of the MDR extends to clinical investigations concerning medical devices and accessories conducted in the EU, while the IVDR also covers performance studies concerning *in vitro* diagnostic medical devices and accessories conducted in the EU.[219] According to its definition, 'clinical investigation' (not to be confused with the term 'clinical trial' regulated under Regulation (EU) No 536/2014 on clinical trials on medicinal

---

[212] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12.7.1993, 1. ELI: <http://data.europa.eu/eli/dir/1993/42/oj> (henceforth: 'MDD').

[213] Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices, OJ L 331, 7.12.1998, 1. ELI: <http://data.europa.eu/eli/dir/1998/79/oj>.

[214] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices, OJ L 189, 20.7.1990, 17. ELI: <http://data.europa.eu/eli/dir/1990/385/oj>.

[215] MDR, *supra* note 209, Recital (82), Articles 103–105; IVDR, *supra* note 210, Articles 98–99.

[216] European Commission (n.d.) *Guidance - MDCG endorsed documents and other guidance*. Available from <https://ec.europa.eu/health/md_sector/new_regulations/guidance_en> (accessed 1 October 2022).

[217] *Brain Products GmbH v. BioSemi VOF and Others* (C-219/11), Judgment of the Court (Third Chamber) (22 November 2012), Court Reports – Court of Justice, ECLI:EU:C:2012:742, para. 24. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-219/11&language=EN>; *Syndicat national de l'industrie des technologies médicales (Snitem), Philips France v Premier ministre, Ministre des Affaires sociales et de la Santé* (C-329/16), Judgment of the Court (Fourth Chamber) (7 December 2016), Court Reports – Court of Justice, ECLI:EU:C:2017:947, para. 33. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-329/16>.

[218] *Syndicat national de l'industrie des technologies médicales (Snitem), Philips France v Premier ministre, Ministre des Affaires sociales et de la Santé* (C-329/16), Opinion of Advocate General Campos Sánchez-Bordona (28 June 2017), Court Reports – Court of Justice, ECLI:EU:C:2017:501, para. 56. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-329/16>.

[219] MDR, *supra* note 209, Article 1(1); IVDR, *supra* note 210, Article 1(1).

products for human use[220]) means "any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device".[221] As regards the term 'performance study', it means a "study undertaken to establish or confirm the analytical or clinical performance of a device".[222] In terms of their purposes, the MDR and the IVDR ensure that medical devices or *in vitro* diagnostic medical devices placed on the market, made available on the market or put into service meet high standards of safety, quality and performance requirements. According to Article 20(1) of the MDR, "[d]evices [...] considered to be in conformity with the requirements of [the MDR] shall bear the CE marking of conformity." This mark enables medical devices to move freely within the internal market and put into service in accordance with their intended purpose.

One of the main advantages of making a specific product available as a medical device is that the manufacturer may list the device in the Eudamed. This ensures transparency (and facilitates trust) among the public about devices placed on the market, the corresponding certificates issued by notified bodies, the relevant economic operators, as well as the unique identification of devices within the internal market and their traceability.[223] In addition, the manufacturer may be entitled to include its medical device in a registry for digital health applications, which some Member States have established to list mHealth apps and browser-based applications that are validated and CE-marked as medical devices.[224] The significance of this is that devices included in these registries are typically reimbursable by the patient's health insurance.

Article 2(1) of the MDR provides that "'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more [...] specific medical purposes" listed in the indents of this provision, and "which does not achieve its principal intended action by pharmacological, immunological or metabolic

---

[220] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, 27.5.2014, 1. ELI: <http://data.europa.eu/eli/reg/2014/536/2014-05-27>.

[221] MDR, *supra* note 209, Article 2(45).

[222] IVDR, *supra* note 210, Article 2(42).

[223] On the purposes of the EUDAMED *see* MDR, *supra* note 209, Article 33(1).

[224] *See* e.g. mHealth Belgium: <https://mhealthbelgium.be/index.php>; Digitalen Gesundheitsanwendungen (DiGA): <https://diga.bfarm.de/de>.

means, in or on the human body, but which may be assisted in its function by such means." Accordingly, a 'medical device' is defined by reference to its:

(a) physical presentation ("any instrument, apparatus, appliance, software, implant, reagent, material or other article");
(b) use ("for human beings");
(c) purpose ("one or more specific medical purposes"); and
(d) means of achieving its principal intended action or mode of action ("which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means").[225]

In practice, the growing number of borderline cases relating to the qualification assessment of devices are related to the (dubious) interpretation and application of the last two points.

As regards the last point, the proper understanding of the 'means of achieving its principal intended action or mode of action' has been questioned recently by the blurred division between 'medical devices' and 'medicinal products'. An increasing number of market authorisation applications for drug–device combinations (DDCs) have highlighted regulatory gaps and led to more borderline cases.[226] The MDR prescribes that in cases where a device incorporates a substance, which, if used separately, may be considered a medicinal product, the medicinal products authority must verify the quality, safety and usefulness of the substance.[227] An example was a case in which the European Medicines Agency issued a favourable qualification opinion on an ingestible event marker (ingestible sensor system), an IoT-enabled platform technology that can be co-formulated with active pharmaceutical compounds into a DDC.[228] The ingestible sensor could collect and communicate data conductively through the body to a patch or wearable sensor. The raw data was secure as

---

[225] *Laboratoires Lyocentre v Lääkealan turvallisuus– ja kehittämiskeskus, Sosiaali– ja terveysalan lupa– ja valvontavirasto* (C-109/12), Opinion of Advocate General Sharpston (30 May 2013), Court Reports – Court of Justice, ECLI:EU:C:2013:353, para. 38. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-109/12>.

[226] Medicines and Healthcare products Regulatory Agency, BioIndustry Association (2018) *The Eighth Joint BIA/MHRA Conference Collaborative Working in the UK. Driving Innovation Forward*. Medicines and Healthcare products Regulatory Agency, BioIndustry Association, London (5 July 2018), 18. Available from <https://www.bioindustry.org/uploads/assets/uploaded/2ceb87ee-bd78-4549-94bff0655fffa5b6.pdf>.

[227] MDR, *supra* note 209, Annex IX, 5.2 *et seq*.

[228] *Qualification opinion on ingestible sensor system for medication adherence as biomarker for measuring patient adherence to medication in clinical trials* (EMA/CHMP/SAWP/513571/2015) (15 February 2016), European Medicines Agency Committee for Medicinal Products for Human Use, London. Available from <https://www.ema.europa.eu/documents/regulatory-procedural-guideline/qualification-opinion-ingestible-sensor-system-medication-adherence-biomarker-measuring-patient_en.pdf>.

detection required direct skin contact and built-for-purpose amplifiers and decoders. The patch or wearable sensor could then upload data to a connected device (typically a mobile phone or tablet) using the Bluetooth protocol. The core medical device software running on the mobile phone or tablet stored and displayed data locally, but the patient could also elect to upload data to a cloud-based personal health record.

Generally, the most important threshold of whether a specific product qualifies as a 'medical device' (and therefore whether or not the MDR applies) is the 'intended purpose' of the manufacturer.[229] This means that the manufacturer itself has the initial power to decide whether a specific product is a medical device. The 'intended purpose' can be broken down into two elements, which the following sections analyse in-depth:[230]

(a) the 'objective' element of 'one or more specific medical purposes' (objective medical functions) that a device should fulfil; and
(b) the 'subjective' element of the manufacturer's 'intended purpose' (subjective intention) that the product should be used for human beings for medical purposes.

2.2.1.) Objective functions ('medical purpose') that a device shall fulfil

With reference to Article 2(1) of the MDR, the objective condition of any IoHT (hardware) device and/or interconnected software (AI system) to qualify as a 'medical device' is that it is "intended by the manufacturer to be used for one or more [...] specific medical purposes" (i.e. objective medical functions).[231] This may encompass one or more of the following medical purpose(s) (with indicative examples of the possible scope/borderline of each purpose[232]):

---

[229] For an analysis on the regulatory considerations behind the concept of 'intended purpose' and a possible alternative 'risk-based' regulatory approach *see* Quinn P (2017) The EU commission's risky choice for a non-risk based strategy on assessment of medical devices. *Computer Law & Security Review* 33(3):361–370. DOI: <https://doi.org/10.1016/j.clsr.2017.03.019>.

[230] Sheppard MK (2020) EU Medical Device Legislation and the Safety Implications for App Users. *In*: Iglezakis I (ed): *Legal Issues of Mobile Apps: A Practical Guide.* Kluwer Law International, Alphen aan den Rijn, Chapter 6 at §6.02.

[231] *See also* under this chapter '2.3. Specific qualification rules for software (AI systems) under the Medical Devices Regulation'.

[232] Medicines and Healthcare products Regulatory Agency (2021) *Guidance: Medical device stand-alone software including apps (including IVDMDs) v1.08* (8 August 2021), 19–25. Available from <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/999908/Software_flow_chart_Ed_1-08b-IVD.pdf>.

(a) prevention of disease (e.g. it may qualify as a medical device, if it claims that its output, such as prescribing interaction alerts using patient-specific data, can directly prevent one or more specific diseases; but it may not qualify as such, if it just provides tips or advice on prevention, or claims to prevent injury or handicap);

(b) diagnosis of disease, an injury or handicap (e.g. it may qualify as a medical device, if it claims that the data entered by the user or generated by the sensor of the physical device are supplied for detecting, diagnosing, or to allow direct diagnosing as such, such as in the case of a symptom-checker using an AI-powered chatbot; however, it may not qualify as such, if it only offers signposts or reference information independent of the likelihood of possible medical conditions);

(c) monitoring of disease, an injury or handicap (e.g. it may qualify as a medical device, if it claims that the data entered by the user or generated by the sensor of the physical device can monitor the progress or severity of a specific disease, an injury or handicap in order to affect the treatment of an individual; however, a log of symptoms used when consulting with the patient's doctor will not qualify as such, nor will monitoring for sport or fitness purposes, such as the heart rate of an athlete, unless the intention is to investigate his/her physiological processes);

(d) treatment or alleviation of disease, an injury or handicap (e.g. it may qualify as a medical device, if it claims that it provides data that can be used to enable treatment to be performed, including by use of telesurgery robots, or its output can be used to treat, reduce symptoms or severity of a disease, injury or handicap; but it may not qualify as such, if it is intended just to provide tips or advice, to remind users to take medicine, or to treat non-medical "lifestyle" conditions, such as non-specific stress);

(e) compensation for an injury or handicap (e.g. it may qualify as a medical device, if it claims that its sensors, output or software can compensate for a specific injury or handicap, such as if it is intended to magnify text specifically for people with visual impairment; however, it may not qualify as such, if it is intended for general use, but can *also* be used to compensate for an injury or handicap, such as if it is intended to magnify text, but there is no mention of visual impairment in the manufacturer's claims);

(f) investigation, replacement or modification of the anatomy or of a physiological process (but, for example, an educational anatomy and physiology software may not qualify as a medical device); and/or

(g) control or support of conception (e.g. it may qualify as a medical device, if it claims to be directly capable of making pregnancy more likely, or prevent pregnancy; but it may not qualify as such, if it simply replaces a written diary/log to track or display data related to a woman's menstrual cycle).

If an IoHT (hardware) device and/or interconnected software (AI system) does not perform any of the abovementioned functions, then it will not qualify as a 'medical device'. This is the case in particular, if an IoHT (hardware) device and/or interconnected software (AI system) only has or performs one or more of the following functions (with indicative examples of the possible scope/borderline of each purpose[233]):

(a) monitoring of general fitness, general health and general well-being;

(b) patient medical education;

(c) professional medical education;

(d) provision of merely reference information to support clinical decision-making (unless it is a decision support software that applies automatic reasoning by combining general medical information databases and algorithms with patient-specific data by use of an algorithm or a more complex series of calculations to interpret or interpolate data, e.g. dose calculation, time of treatment or future risk of disease, and the healthcare professional does not review the raw data);

(e) administration of healthcare (e.g. hospital information systems used for booking of appointments, request of prescription or teleconsultation);

(f) information systems storing or transmitting data concerning health without changing the data (e.g. EHR system, clinical information system, patient data management system, pre-hospital electrocardiograph system, picture archive communication system, communications system, laboratory information system, work area manager, image management system; except if the information system has a specific module that contributes to a medical purpose, then that module may qualify as a medical device, e.g. an image viewer software with diagnosis functionalities, an alarm generator AI system based on the monitoring and analysis of patient-specific physiological parameters, or a web server-based application monitoring the performance of medical devices);

---

[233] Medical Device Coordination Group (2019) *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR* (MDCG 2019-11) (11 October 2019), 6–7, 19–23. Available from <https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf> (henceforth: 'MDCG 2019-11'); *ibid*., 12.

(g) a database without internal language/macros/scripting;
(h) a multipurpose product (e.g. communications systems, as well as word processing or spreadsheet software, unless if it has a specific intended medical purpose, and uses macros/functions/programming language); or
(i) data retrieval by "simple search" library functions (unless the data is modified or its representation is altered for an intended medical purpose).

If an IoHT (hardware) device and/or interconnected software (AI system) qualifies as a 'medical device', it may qualify as an '*in vitro* diagnostic medical device', if it satisfies the objective conditions laid down in Article 2(2) of the IVDR. This entails that the IoHT (hardware) device and/or interconnected software (AI system) is intended by the manufacturer to be used *in vitro* for the examination of specimens derived from the human body for the purpose of providing information on one or more of the following (with indicative examples of the possible scope/borderline of each purpose [234]):

(a) concerning a physiological or pathological process or state (e.g. it may qualify as an *in vitro* diagnostic medical device, if it provides information about a condition or disease from results generated by the device);
(b) concerning a congenital abnormality (e.g. it may qualify as an *in vitro* diagnostic medical device, if it provides information about an acquired or inherited condition or disease from results generated by the device);
(c) concerning the predisposition to a medical condition or a disease;
(d) to determine the safety and compatibility with potential recipients (e.g. it may qualify as an *in vitro* diagnostic medical device, if it provides information about the compatibility of blood, tissues, organs or cells donated for transplant or transfusion from results generated by the device);
(e) to predict treatment response or reactions; and/or
(f) to define or monitor therapeutic measures (e.g. it may qualify as an *in vitro* diagnostic medical device, if it provides information about the presence or amount of a pharmaceutical substance or other therapeutic measure from results generated by the device).

On the competence of interpreting the abovementioned aspects of the qualification assessment, the MDR provides that it is first and foremost "the responsibility of the Member States to decide on a case-by-case basis whether or not a specific product falls within the

[234] MDCG 2019-11, *supra* note 233, 15–18.

scope of the [MDR]" (and IVDR).[235] However, "[i]n order to ensure consistent qualification decisions [...] across all Member States, particularly with regard to borderline cases, the Commission [is] allowed to, on its own initiative or at the duly substantiated request of a Member State, having consulted the [MDCG], decide on a case-by-case basis whether or not a specific product, category or group of products falls within the scope of the [MDR]" (and IVDR).[236] As a supplementary rule, the MDR adds that: "[d]evices with both a medical and a non-medical intended purpose shall fulfil cumulatively the requirements applicable to devices with an intended medical purpose and those applicable to devices without an intended medical purpose."[237]

2.2.2.) The manufacturer's subjective intention ('intended purpose')

Article 2(12) of the MDR defines 'intended purpose' as "the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation".[238] The 'intended purpose' must describe the intent of the manufacturer as objectively as possible, that is, the manufacturer is obliged to formulate its intended purpose in a clear, precise and unambiguous way in order to preclude different interpretations and without acting arbitrarily to circumvent the (perhaps unfavourable) qualification. The intended purpose should describe the intended medical use—not the specific product features or specifications of an anticipated product.[239] Since this has led to confusion in the past, it is worth noting that the MDR defines 'intended purpose', but not 'intended use'. The MDCG has clarified that 'intended use' should be considered to have the same meaning as 'intended purpose'.[240] As an exception to the rule,

---

[235] MDR, *supra* note 209, Recital (8) and IVDR, *supra* note 210, Recital (8).

[236] MDR, *supra* note 209, Recital (8) and Article 105; IVDR, *supra* note 210, Recital (8) and Article 99.

[237] MDR, *supra* note 209, Article 1(3).

[238] *Ibid*., Article 2(12).

[239] Wyler J (2020) *The intended purpose – or, what does your medical device do?* (4 February 2020), Decomplix, Bern. Available from <https://decomplix.com/intended-purpose-medical-device>.

[240] Medical Device Coordination Group (2020) *Regulation (EU) 2017/745: Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC. A guide for manufacturers and notified bodies* (MDCG 2020-6) (23 April 2020), 6 [section 1.2]. Available from <https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2020_6_guidance_sufficient_clinical_evidence_en.pdf>.

Annex XVI of the MDR lists groups of products, which do not require an intended medical purpose, but the MDR cover them nonetheless. With respect to the subject matter, these exceptions may bear relevance only to certain types of IoHT physical devices (e.g. a smart contact lens with built-in augmented reality (AR) functions, or a brain–computer interface intended for brain simulation).

The intended purpose of the manufacturer is decisive not only in the qualification of a specific product, but it is also the basis for applying the classification rules established in Annex VIII of the MDR, in order to determine the risk class of a medical device, as outlined under Article 51(1) of the MDR. The risk classification then determines the conformity assessment route for the device, including the amount of clinical data required to demonstrate conformity with the relevant safety and performance requirements. In the device description, the 'intended purpose' of a device should include the following (non-exhaustive list of) elements: exact medical indications (if applicable); the disease or condition to be treated, managed or diagnosed; patient populations; intended users (e.g. healthcare professionals / laypersons); repeat applications; precautions required by the manufacturer; as well as any contraindications.[241] The intended purpose helps to identify the clinical data that is relevant to the device, while the depth and extent of the clinical evaluation depend on the intended purpose (as well as on the classification, risks of the device, and the manufacturer's claims in respect of the device). If a manufacturer provides instructions for use of medical devices in electronic form, it must also comply with the conditions laid down by Commission Regulation (EU) No 207/2012.[242]

Considering that the definition of 'intended purpose' under Article 2(12) of the MDR refers only to the direct intention manifested in publicly disseminated documentation and materials issued by the manufacturer, one could argue that the 'intended purpose' should also encompass the manufacturer's indirect intention. If the 'intended purpose' were limited purely to what is provided as information to the public, then this might allow a manufacturer, especially of software (AI system), to circumvent the MDR, by not specifying hidden features or risks of a device, such as disguised data processing operations or the likelihood

---

[241] European Commission (2016) *Clinical Investigation: A Guide for Manufacturers and Notified Bodies under Directives 93/42/EEC or 90/385/EEC. Guidelines on Medical Devices* (MEDDEV 2.7/1 revision 4) (June 2016), 35 [appendix A3.] (see also *ibid*., 18 [appendix I] on sections of MEDDEV 2.7/1 rev. 4 which are still relevant under the MDR). Available from <http://www.ec.europa.eu/DocsRoom/documents/17522/attachments/1/translations/en/renditions/native>.

[242] Commission Regulation (EU) No 207/2012 of 9 March 2012 on electronic instructions for use of medical devices, OJ L 72, 10.3.2012, 28–31. ELI: <http://data.europa.eu/eli/reg/2012/207/oj>.

and severity of certain data security or cybersecurity breaches. In these examples, the significance of taking into account the manufacturer's indirect intention is that it would cover the manufacturer's awareness about what the software (AI system) is capable of, and how it functions in practice.[243] If we accept the legal argument of differentiating between a manufacturer's direct and indirect intention, then sources for discerning the its direct intention may be:[244]

(a) information from marketing materials (e.g. manufacturer's publicly claimed intended purpose);
(b) information from internal documentation (e.g. technical documentation); or
(c) informal information sources (e.g. interview with a representative of the manufacturer).

In addition to these, sources for discerning the manufacturer's indirect intention could be:

(a) data-gathering practices (e.g. if software collects data that are relevant to fulfil a medical purpose);
(b) data analysis (e.g. if software requires the analysis of personal and/or non-personal data in order to achieve results that resemble or fulfil a medical purpose); or
(c) functional specifications (e.g. if software is designed and made to function as a medical device with the aim of either substituting or replacing existing medical devices without being one itself).

2.2.3.) The definition of 'medical device' in the CJEU's case law

In *Oliver Medical*, the CJEU delivered a judgment on the customs classification of devices imported into the EU and intended for the treatment of dermovascular and dermatological problems. As part of its assessment, the CJEU took account of the fact that those devices had a medical purpose and, in this regard, held that "it is necessary to assess the use for which the product is intended by the manufacturer and the methods and place of its use. Thus, the fact that the product is intended to treat one or more different pathologies and that that treatment must be carried out in a medical centre and under the supervision of a

[243] Ludvigsen K, Nagaraja S and Daly A (2021) When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law. *European Journal of Risk Regulation* 1–16 at 12. DOI: <https://doi.org/10.1017/err.2021.45>.

[244] *Ibid*., 12–13.

practitioner are indications capable of establishing that that product is intended for medical use. Inversely, the fact that a product mainly brings about aesthetic improvement, that it may be operated outside a medical environment, for example in a beauty parlour, and without the intervention of a practitioner are indications that that product is not intended for medical use."[245] In the same judgment, the CJEU considered that the CE marking that a product bears is an additional factor in establishing whether that product is intended for medical use.[246] As referred to above, the function of a CE marking is to confer on the product that bears the marking the benefit of the presumption of conformity with the requirements of the MDR.

The proper interpretation and application of the 'medical purpose' was part of a question referred for preliminary ruling of the CJEU in *Brain Products*.[247] The national proceedings before a German court concerned a dispute about the qualification of a product ('ActiveTwo') that is capable of recording electrical signals from the human body (intended for the investigation of a physiological process). The question was whether the product qualifies as a medical device even though the manufacturer explicitly did not intend it for medical use, and hence its marketing without a CE marking of conformity (required for medical devices) was prohibited. According to the Opinion of Advocate General Mengozzi, many factors support taking a systematic and/or teleological approach (over a literal interpretation) to interpreting the relevant provisions of the MDD.[248] (With regard to the similarities between the MDD and the MDR in this area, the underlying arguments seem to remain valid with respect to the MDR.) AG Mengozzi wrote that '[a]ccording to the teleological and systematic approach, only products which are intended to have a medical use are covered by the [MDD].'[249] Regarding the objective of the MDD, the Opinion of AG Mengozzi pointed out that 'the idea was to define a reference framework capable of adequately protecting persons who, whether actively or passively, come into contact with the products in a medical setting.'[250]

---

[245] *'Oliver Medical' SIA v Valsts ieņēmumu dienests* (C-547/13), Judgment of the Court (Tenth Chamber) (4 March 2015), Court Reports – Court of Justice, ECLI:EU:C:2015:139, para. 52. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-547/13>.

[246] *Ibid*., para. 53.

[247] *Brain Products GmbH v. BioSemi VOF and Others*, *supra* note 217.

[248] *Brain Products GmbH v. BioSemi VOF and Others* (C-219/11), Opinion of Advocate General Mengozzi (15 May 2012), Court Reports – Court of Justice, ECLI:EU:C:2012:299, para. 23 *et seq*. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-219/11>.

[249] *Ibid*., para. 30.

[250] *Ibid*.

Furthermore, the Opinion of AG Mengozzi supported the abovementioned dogmatics regarding the distinction between the objective and subjective aspects of the manufacturer's intended purpose. In this regard, the AG Opinion emphasised that "[i]t is important [...] to bear in mind that the manufacturer's intention as regards the use of a given product is not immaterial and that categorisation under the [MDD] cannot be based on objective factors only."[251] The AG Opinion added that the "[MDD] contains various references to the manufacturer's intended use of a product. This reveals that, far from being irrelevant, that 'subjective' element must in fact be taken into account in interpreting the applicable provisions."[252] The conclusion of the AG Opinion was that: "[e]ven if the information provided by the manufacturer is the key factor in determining whether a product is intended to be used for a medical purpose, any product which, by its very nature, is clearly intended to be used solely for a purpose of a medical nature *will have to be regarded as a medical device*, even if the manufacturer does not describe it as such."[253] Indeed, it is important to ensure that the subjective intention of a device manufacturer serves as a trigger for the application of the appropriate safety, quality and performance legal regime, and that a simple disclaimer stating that a device is not intended for medical purposes should not release the device manufacturer of certain legal obligations.[254] As regards the objective functions of the device, the AG Opinion wrote: "[t]hat reference to the manufacturer's intention is not of itself decisive here, because the reference is to the intention that the product should be used for human beings and not that it should be used for human beings for medical purposes."[255]

In terms of the legal approach used to interpret the MDD, the CJEU agreed with the AG Opinion that: "it is necessary to consider not only its wording but also the context in which it occurs and the objectives pursued by the rules of which it is part".[256] Regarding the interpretation of the 'intended purpose', the CJEU held that "[a]s regards software, the legislature [...] made unequivocally clear that in order for it to fall within the scope of [the MDD] it is not sufficient that it be used in a medical context, but that it is also necessary that the intended purpose, defined by the manufacturer, is specifically medical."[257] "Furthermore,

---

[251] *Ibid*., para. 42.

[252] *Ibid*., para. 40.

[253] *Ibid*., para. 63.

[254] Purtova, *supra* note 190, 473.

[255] Opinion of Advocate General Mengozzi, *supra* note 248, para. 42.

[256] *Brain Products GmbH v. BioSemi VOF and Others*, *supra* note 217, para. 13.

[257] *Ibid*., para. 17.

nothing [...] indicates that the legislature intended that a wider scope should apply for 'non-software devices' than for 'software'."[258] However, the CJEU did not follow the reasoning of the AG Opinion on the assessment of the manufacturer's intention, and elaborate on this point. For this reason, it is unclear how this decision would affects situations where a manufacturer of a product not labelled or marketed as a medical device sells the product to a clinic for a medical purpose, notwithstanding product labelling.[259]

In connection with the legal considerations underpinning the distinction between medical devices and non-medical goods in the healthcare sector, the CJEU provided the following reasoning: "[a]s the Advocate General states [...], in the field of medical devices account must be taken not only of the protection of health, but also of the requirements of the free movement of goods."[260] "It follows that [the MDD] may have the effect of limiting the free movement of medical devices, by providing for an obligation for certification and CE marking in respect of those products only where such a limitation is necessary for the protection of public health. Therefore, in situations in which a product is not conceived by its manufacturer to be used for medical purposes, its certification as a medical device cannot be required. That is the case, in particular, of many sports goods which enable the functioning of certain organs in the human body to be measured without any medical use. If such articles were to be classified as medical devices, they would be subject to a certification procedure without any justification for that requirement."[261] As we see, this is a reference to the legal status of digital consumer health products (wellness applications).

---

[258] *Ibid*., para. 19.

[259] Kelly B (2012) *CJEU Clarifies Medical Device Borderline.* Covington: Inside EU Life Sciences (26 December 2012). Available from: <https://www.insideeulifesciences.com/2012/12/26/cjeu-clarifies-medical-device-borderline>.

[260] *Ibid*., para. 27.

[261] *Ibid*., paras. 29–31.

2.3.) Specific qualification rules for software (AI systems) under the Medical Devices Regulation

2.3.1.) Medical device software (MDSW): software as a medical device (SaMD), software in a medical device (SiMD) and atypical medical device software

Although the MDR regulates the qualification of software falling within its scope, it provides neither a definition, nor detailed qualification criteria to software.[262] The MDCG provided clarifications in this regard in its 'Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR' ('MDCG 2019-11').[263] The MDCG 2019-11 defines 'software' "as a set of instructions that processes input data and creates output data."[264] The same guidance also provides a definition specifically for 'medical device software' ('MDSW'): "software that is intended to be used, alone or in combination, for a purpose as specified in the definition of a 'medical device' in the [MDR] or in [the IVDR]."[265]

Before addressing factors determining the qualification of software (including AI systems) interconnected with Internet of Health Things physical device(s) under the MDR, it is important to mention what factors are *not* decisive in this qualification assessment. First, the risk of harm to patients, users of the software, or any other person, related to the use of the software within healthcare, including a possible malfunction is not a criterion for whether the software qualifies as a medical device.[266] Second, Recital (19) of the MDR provides that: "[t]he qualification of software, either as a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device." In relation to this, the MDCG 2019-11 elaborates that: "[t]he type of interconnection between the MDSW and the device (e.g. embedded systems, wires, Wi-Fi, Bluetooth) does not affect the qualification of the software as a device under the MDR and IVDR (e.g. whether the

---

[262] *See also* DIGITALEUROPE (2019) *Reflection Paper on regulatory frameworks for digital health technologies in Europe*. DIGITALEUROPE, Brussels (5 April 2019). Available from <https://www.digitaleurope.org/resources/reflection-paper-on-regulatory-frameworks-for-digital-health-technologies-in-europe>.

[263] MDCG 2019-11, *supra* note 233.

[264] *Ibid*., 5.

[265] *Ibid*., 6.

[266] *Ibid*., 7.

software is incorporated in a device or is at a different location)."[267] What follows from this is that the type of interconnection between a software (AI system) and an IoHT physical device(s) bears no relevance for the qualification assessment of that interconnected software (AI system). Moreover, the qualification of a software (AI system) is independent of where that interconnected software (AI system) operates along the cloud-to-thing continuum. These regulatory considerations ensure (implicitly) that the qualification of software (AI systems) under the MDR remains independent of their design features. This is important to highlight, in particular, concerning AI systems, since they "can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded)."[268]

As mentioned, in order to qualify as a MDSW, a software (AI system) must first fulfil the definition of a 'medical device' according to Article 2(1) of the MDR. The MDCG 2019-11 spells out that MDSW can be placed on the market in two different ways:

(a) as a medical device (or *in vitro* diagnostic medical device) in its own right; or

(b) as an integral component or part of a hardware device.

The first instance is often referred to as 'software as a medical device' ('SaMD'), while the second instance is labelled as 'software in a medical device' ('SiMD').[269] The significance of the qualification of MDSW based on this scheme lies in the different regulatory procedures that a particular MDSW has to undergo. By having its own intended medical purpose (and thus meeting the definition of a 'medical device') on its own right (i.e. alone), SaMD must undergo a conformity assessment procedure that takes into consideration the qualification, classification and intended purpose of the MDSW. In this case, the IoHT physical device interconnected with the MDSW must undergo a separate conformity assessment procedure on its own right. In contrast, SiMD must undergo a conformity assessment procedure as a whole (i.e. the *de facto* combination of the MDSW and the physical hardware device that the MDSW is an integral component or part of).

---

[267] *Ibid*., 16.

[268] AI Act proposal, *supra* note 205, Recital (6).

[269] International Medical Device Regulators Forum (2013) *Software as a Medical Device (SaMD): Key Definitions* (IMDRF/SaMD WG/N10FINAL:2013) (9 December 2013), 4. Available from <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>.

In addition to the foregoing distinction outlining the two major configurations in which MDSW can be placed on the market, there are further atypical cases:

- Software (AI system) may be intended by the manufacturer to be used as an 'accessory for a medical device' (as defined by Article 2(2) of the MDR) in order to enable a medical device to fulfil its intended function. For example, if a mobile app is the only way of interacting with an IoHT medical device, then it may be an accessory for that device.[270] In that case, although the software (AI system) would not qualify as a 'medical device', it would be referred to as a 'device' under the MDR, and thus, all corresponding provisions would apply.[271] In other words, a software (AI system) that is an 'accessory for a medical device' must be treated, for the purposes of the MDR, as a medical device in its own right.[272]
- Software may be provided as part of a 'system' ('kit') or as a 'module' in the system. For example, the interconnection and/or combination of a laptop (that is not a medical device), a software (a medical device), and a wearable heart monitoring hardware (an accessory) is considered to be a 'system', if these are placed on the market together.[273] Alternatively, telehealth systems may be based upon a complex software structure (and multiple correlated applications), which may consist of both medical device and non-medical device software modules. In this regard, the MDCG 2019-11 explains that: "[i]f the modules which are subject to the [MDR] are intended for use in combination with other modules of the whole software structure, other devices or equipment, the whole combination, including the connection system, must be safe and must not impair the specified performances of the modules which are subject to the [MDR]."[274]
- If software drives or influences a (hardware) medical device, and has or performs a medical purpose or creates information on its own for one or more of the medical purposes described in the definition of a 'medical device', then it qualifies as a

---

[270] Inside Tech Media (2019) *IoT Update: Are Wearables Medical Devices Requiring a CE-Mark in the EU?* Covington (18 January 2019). Available from: <https://www.insidetechmedia.com/2019/01/18/iot-update-wearables-medical-devices-requiring-a-ce-mark-in-the-eu>.

[271] MDR, *supra* note 209, Article 1(4).

[272] *See Snitem*, *supra* note 217, para. 24.

[273] Medicines and Healthcare products Regulatory Agency, *supra* note 232, 9.

[274] MDCG 2019-11, *supra* note 233, 18.

MDSW.[275] In this case, it functions as either an integral part or component of a hardware device, or as an accessory for a medical device.

2.3.2.) The qualification of medical device software in the CJEU's case law

The assessment of the qualification of a drug prescription assistance software ('ICCA') was part of a question referred for preliminary ruling by the CJEU in *Snitem*.[276] The national proceedings before the French *Conseil d'État* (Administrative Supreme Court) concerned a dispute about whether the ICCA software, which permits the use of patient's data to help a doctor issue the patient's prescription and bears the CE marking, qualifies as a medical device, even if it does not itself act in or on the human body. According to the Opinion of Advocate General Campos Sánchez-Bordona, "in view of the fact that [...] the ICCA software bears the CE marking (as a result of which it is freely placed on the market in [...] Member States), that software benefits from the presumption of conformity with [the MDD]. Accordingly, it is for the [disputing party] to rebut that presumption".[277] However, the AG Opinion found that "[t]he fact [...] that the ICCA software does not itself act in or on the human body does not preclude its classification as a medical device."[278] The definition of medical device "does not require direct action by the device but rather 'assistance' with the principal action".[279]

On the assessment of whether a software serves a medical function, the AG Opinion explained that: "if the software does not perform an action on data or that action is limited to storage, archival, communication, simple search or lossless compression, it cannot be classified as a medical device. *A contrario*, if the software creates or modifies medical information to assist the healthcare professional with the use of that information, it might be a medical device."[280] In the referred case, the AG Opinion found that "[u]sing data collected about the patient (which may come from other systems and appliances to which that patient is connected), and with the assistance of its calculation engines, the [ICCA] software

[275] *Ibid*., 7–8.

[276] *See Snitem*, *supra* note 217.

[277] Opinion of Advocate General Campos Sánchez-Bordona, *Snitem, supra* note 218, para. 41.

[278] *Ibid*., para. 69.

[279] *Ibid*., para. 70.

[280] *Ibid*., para. 57.

automatically converts that data into useful information for the health professional while at the same time suggesting the correct doses of drugs."[281] "[T]he ICCA software go beyond mere administrative functions, such as the storage and archival of data, and allow it to be classified as a medical device."[282]

The CJEU held that: "[i]t is expressly apparent from [the definition of 'medical device' in the MDD] that software constitutes a medical device [...] where it satisfies the two cumulative conditions which must be met by any device of that nature, relating respectively to the objective pursued and the action resulting therefrom."[283] "As regards, first, the objective pursued, [the definition of 'medical device' in the MDD] provides that a medical device must be intended by the manufacturer for use in humans for the purposes [enumerated in the definition]."[284] The CJEU repeated the reasoning of the AG Opinion that: "[i]n the present case, software that cross-references patient-specific data with the drugs that the doctor is contemplating prescribing, and is thus able to provide the doctor, in an automated manner, with an analysis [...] for the purpose of prevention, monitoring, treatment or alleviation of a disease, [...] pursues a specifically medical objective, making it a medical device within the meaning of [the MDD]."[285] "That is not the case, however, for software that, while intended for use in a medical context, has the sole purpose of archiving, collecting and transmitting data, like patient medical data storage software, the function of which is limited to indicating to the doctor [...] the name of the generic drug associated with the one he plans to prescribe, or [...] the contraindications mentioned by the manufacturer of that drug in its instructions for use."[286] The implication of this part of the judgment is that other decision support software incorporating automated reasoning may also meet the threshold of a 'medical device'. However, this raises the question of where the boundary of liability between the healthcare professional and the medical device manufacturer lies.[287]

In *Snitem*, the CJEU also held that: "as regards the condition relating to the action resulting from the objective pursued", "it should be noted that although that provision

---

[281] *Ibid*., para. 64.

[282] *Ibid*., para. 66.

[283] *Snitem*, *supra* note 217, para. 22.

[284] *Ibid*., para. 23.

[285] *Ibid*., para. 25.

[286] *Ibid*., para. 26.

[287] Friedel E, Goraya T (2018) *CJEU rules on prescription support software as a medical device.* Taylor Wessing (March 2018). Available from: <https://www.taylorwessing.com/synapse/march18.html>.

provides that the main action of the medical device 'in or on the human body', it does not require such a device to act directly in or on the human body."[288] "Thus, it does not matter whether, in order to be classified as a medical device, software acts directly or indirectly on the human body, the essential point being that its purpose is specifically one of those" referred to in the definition of a 'medical device.'[289] It follows that "software, of which at least one of the functions makes it possible to use patient-specific data [...] is, in respect of that function, a medical device, within the meaning of [the definition of 'medical device' in the MDD], even if such software does not act directly in or on the human body."[290] "In respect of medical software comprising both modules that meet the definition of the term 'medical device' and others that do not meet it and that are not accessories within the meaning of [the definition of 'accessory for a medical device' provided by the MDD], only the former fall within the scope of the directive and must be marked CE."[291]

2.4.) Risk classification rules for Internet of Health Things (hardware) devices and interconnected software (AI systems) under the Medical Devices Regulation

Manufacturers (as well as health institutions) must comply with the MDR in each step of the regulatory process (in both commercial and in-house use cases): from early-stage considerations through design and development, and regulatory submission, to post-market (post-product release) surveillance.[292] The classification rules of the MDR determine the applicable provisions of the MDR for each step of this process. Article 51(1) of the MDR sets forth that "[d]evices shall be divided into classes I, IIa, IIb and III, taking into account the intended purpose of the devices and their inherent risks. Classification shall be carried out in accordance with Annex VIII." As a general rule, for class IIa ('medium risk'), class IIb ('medium-high risk') and class III ('high risk') devices, manufacturers are subject to a

[288] *Snitem*, *supra* note 217, paras. 27–28.

[289] *Ibid*., para. 32.

[290] *Ibid*., para. 34.

[291] *Ibid*., para. 36.

[292] Beckers R, Kwade Z, Zanca F (2021) The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. *Physica Medica* 83:1–8 at 2 *et seq*. DOI: <https://doi.org/10.1016/j.ejmp.2021.02.011>.

conformity assessment procedure in which a notified body ascertains and certifies whether a device fulfils the relevant provisions of the MDR.[293] Depending on the classification and the manufacturer's choice, there are three types of conformity assessment procedures:[294]

(a) conformity assessment based on a quality management system and on assessment of technical documentation;
(b) conformity assessment based on type examination; and/or
(c) conformity assessment based on product conformity verification

By contrast, for class I ('low risk') devices, as a general rule, the manufacturer alone is responsible for declaring the conformity of their product by issuing the EU declaration of conformity and making all relevant technical documentation available during a certain period to the notified bodies for inspection.[295] As a supplementary rule to the foregoing provisions, the MDR ensures that the compliance of devices with widely accepted soft law instruments demonstrate conformity. On one hand, "devices that are in conformity with the relevant harmonised standards [...] shall be presumed to be in conformity with the requirements of [the MDR] covered by those standards or parts thereof."[296] Alternatively, "[d]evices that are in conformity with the [common specifications (CS) adopted by The Commission] shall be presumed to be in conformity with the requirements of [the MDR] covered by those CS or the relevant parts of those CS."[297]

The risk class applicable to IoHT (hardware) devices and software (including AI systems) that fall under the scope of the MDR are determined by the implementation rules set forth in Chapter II of Annex VIII and by the classification rules laid down in Chapter III of Annex VIII of the MDR. Implementing Rule 3.1 of Annex VIII provides that: "[a]pplication of the classification rules shall be governed by the intended purpose of the devices." Implementing Rule 3.2 of Annex VIII states that "[i]f the device in question is intended to be used in combination with another device, the classification rules shall apply separately to each of the devices. Accessories for a medical device shall be classified in their own right separately from the device with which they are used." Implementing Rule 3.3 of Annex VIII clarifies the regime applicable to MDSW driving or influencing the use of an

---

[293] MDR, *supra* note 209, Article 52(3), Article 52(4) and Article 52(6).

[294] *Ibid*., Annexes IX–XI.

[295] *Ibid*., Article 52(7).

[296] *Ibid*., Article 8(1).

[297] *Ibid*., Article 9(2).

IoHT (hardware) device, as well as the regime applicable to independent MDSW: "[s]oftware, which drives a device or influences the use of a device, shall fall within the same class as the device. If the software is independent of any other device, it shall be classified in its own right." This rule is an orientation for determining the correct (minimum) classification of software placed on the market in combination with an IoHT (hardware) medical device. Therefore, MDSW must be classified on its own right, based on the intended purpose achieved, if it achieves its own intended purpose and also drives or influences the use of an IoHT (hardware) device for a medical purpose. However, in that case, the risk class shall not be lower than the risk class of the hardware medical device.[298] Finally, Implementing Rule 3.5 of Annex VIII adds to these that: "[i]f several rules, or if, within the same rule, several sub-rules, apply to the same device based on the device's intended purpose, the strictest rule and sub-rule resulting in the higher classification shall apply."

IoHT (hardware) medical devices and MDSW (including AI-enabled medical devices) must be classified according to Chapter III of Annex VIII of the MDR as an invasive device or non-invasive device depending on whether the "device [...] in whole or in part, penetrates inside the body, either through a body orifice or through the surface of the body".[299] With reference to the definition provided by Article 2(4) of the MDR, both IoHT (hardware) medical devices and MDSW (including AI-enabled medical devices) must be classified as 'active devices'. Therefore, Implementing Rules 10 to 13 of Annex VIII are applicable thereof. MDSW (including AI-enabled medical devices) must be classified according to Implementing Rule 11.

Implementing Rule 11 of Annex VIII of the MDR has received criticism on the ground that it leaves little room for MDSW to be classified as class I. In the previous legal framework (before the MDR), the advantage of a class I device was that it enabled many start-ups and university spin-offs to ship innovative MDSW without having to go through often expensive and slow conformity assessment procedures, to involve a notified body and establish a certified quality management system.[300] Under the MDR, MDSW are generally classified higher than before. However, according to critics, this "upgrading" will hinder

[298] MDCG 2019-11, *supra* note 233, 12.

[299] MDR, *supra* note 209, Article 2(6).

[300] Eidel O (2022) *MDR Class 1 Devices: Do They Exist (as software)?* OpenRegulatory (updated 29 September 2022). Available from: <https://openregulatory.com/do-software-mdr-class-1-devices-exist>.

innovation by smaller manufacturers.[301] Furthermore, the classification of MDSW does not necessarily mirror their risk. The problem is that Implementing Rule 11 only considers the severity (e.g. "might lead to death") or duration (e.g. "irreversible") of potential harms, but it does not take into account the probabilities of the risk occurring.[302] Although Annex III of MDCG 2019-11 presents an indicative orientation on the appropriate risk class applicable to MDSW intended to provide information in order to take decisions with diagnosis or therapeutic purposes, this guidance does not fix the aforementioned problem.

3.) Data protection-related requirements deriving from the qualification of Internet of Health Things and interconnected software (AI systems)

3.1.) Data protection and cybersecurity requirements deriving from the qualification of Internet of Health Things and interconnected software (AI systems) as (digital consumer health) product(s)

3.1.1.) General Product Safety Directive

The definition of safety ('safe product') under Article 2(b) of the GPSD does not mention data protection, privacy or cybersecurity risks, or other safety concerns related to specifically the use of (new) digital technologies. Moreover, none of the national (Member State) implementation laws transposing the GPSD provides a specific definition of safety in relation to new technologies.[303] For this reason, there is inconsistency and widespread

[301] Johner C (2017) *MDR Classification Rule 11 for Medical Device Software.* Johner Institute (22 July 2017). Available from: <https://www.johner-institute.com/articles/regulatory-affairs/and-more/mdr-rule-11-software>.

[302] *Ibid*.

[303] European Commission Directorate-General for Justice and Consumers, Civic Consulting (2021) *Study for the preparation of an Implementation Report of the General Product Safety Directive.* Final report. Part 1: Main report. European Commission, Brussels (29 September 2021), 8. Available from <https://ec.europa.eu/info/sites/default/files/final_report-gpsd-part1-main_report-final-corrected2.pdf>.

uncertainty within the EU about whether and how general safety, health and quality requirements apply to products enabled by new technologies or to products that are themselves the new enabling technology.[304] Consequently, there is uncertainty as to whether and how the GPSD applies to IoHT devices and software (AI systems) in healthcare. In particular, this includes the problem of whether the GPSD covers (adequately) the following threats to safety:

- cybersecurity risks to consumer products that may lead to physical harm (e.g. the hacking of an wellness application causes damages to the consumer's health);
- cybersecurity risks to consumer products that may lead to loss of usability or loss of data (e.g. through the infection of the wellness application by ransomware);
- cybersecurity risks to consumer products that may expose privacy-related information causing a risk to personal security (e.g. the jogging route mapped by a smart watch is shared without the consumer's consent);
- cybersecurity risks of products that may expose a network to potential attacks (e.g. a router in an IoT-enabled telehealth system is infected with malware);
- malfunctioning of software that is embedded or non-embedded (e.g. downloadable as a separate application) that may affect the safety of a wellness application for consumers (e.g. technical problems affecting the transmission of signals between the software and the hardware device);
- software content that may pose safety risks to consumers (e.g. scientifically unproven wellness/lifestyle guidance that a software displays on the interface of an IoHT physical device); or
- products with machine learning (AI) capabilities that may affect the safety of consumers.

According to the study that underpinned the Implementation Report of the GPSD, there is a general trend in the national transposition of the GPSD (and related interpretations) that data protection, privacy and security risks are subject to the GPSD as far as they have implications for the physical safety or health of consumers.[305]

In addition to the abovementioned risks, the GPSD also lacks clarity on risks posed by new technologies to safety that are "not immediately obvious". Although Article 5(1) of the GPSD imposes obligations on producers to "provide consumers with the relevant

[304] *Ibid*., 40–42.

[305] *Ibid*., 42–43.

information to enable them to assess the risks inherent in a product throughout the normal or reasonably foreseeable period of its use", the risks of post-marketing defects arising increases with new technology. For example, risks may arise from latent technological bugs or failure to provide appropriate security updates to software. Risks may also arise from adaptive systems as they continue to 'learn' (i.e. automatically adapt how functions are carried out) after being placed on the market or put into service. Therefore, it would be important that authorities be adequately empowered to take appropriate action with regard to IoHT devices or interconnected software, which become dangerous products. For this, it would be essential for national legislators to define and allocate competences effectively among national authorities responsible for the market surveillance and product safety enforcement of products taking advantage of new technologies.[306] With respect to the cross-border nature of information and communications networks, enhanced cooperation between the national authorities of Member States would also be necessary to mitigate risks posed by dangerous digital consumer health products (wellness applications) in the European digital market.

3.1.2.) General Product Safety Regulation proposal

As mentioned before, in order to address the legal uncertainty of the GPSD on the application of its requirements regarding new technologies, the GPSR proposal introduces new provisions aimed at new technologies (such as IoT and AI) and related risks. With regard to the subject matter, one of the novelties of the GPSR proposal is that it includes new 'aspects for assessing the safety of products' (i.e. a new definition of 'safety') to address possible risks related to products based on new technologies. New safety aspects listed by the GPSR proposal include, in particular, the "technical features [of the product]", "the effect on other products, [...] including the interconnection of products among them", as well as "the evolving, learning and predictive functionalities of a product". These safety aspects may be relevant to assess risks posed by the use of IoHT (hardware) devices and interconnected software that fall outside the scope of specialised legal regimes governing safety, health and quality requirements.[307] However, a group of stakeholders "caution[ed] policymakers to not

[306] *Ibid*., 61, 142.

[307] GPSR proposal, *supra* note 198, Article 7(1)(a), Article 7(1)(b) and Article 7(1)(i).

introduce these new and unspecified safety assessment requirements which will be better addressed in their own legislative proposals [such as the AI Act proposal], to avoid duplication and inconsistencies".[308] "For example, vague wording such as 'take into account' [connectivity/IoT risks] shouldn't be used if the practical and legal implication isn't made clear", therefore the stakeholders recommended that "the duties [...] be limited to assessment of the impact of products that are *intended* to be used together or connected."[309] With respect to the present context, this would indeed bring clarity in the application of general safety, health and quality requirements to IoHT (hardware) devices and interconnected software, because it would resemble the fundamental concept of the 'intended purpose of the manufacturer' in the specialised legislation (i.e. the MDR).

The new enumeration of aspects to consider for assessing the safety of products also includes "appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product".[310] The inclusion of cybersecurity features among the aspects to consider for assessing the safety of products would be a significant legal development. It would establish a legislative "safety net" for taking into account any cybersecurity risks, which would fall outside the scope of specialised legislation but may have an impact on setting safety, health and quality requirements for IoHT (hardware) devices and interconnected software. According to the Explanatory Memorandum of the GPSR proposal, this is a necessary clarification, because although the Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification[311] ('Cybersecurity Act') "introduces an EU-wide cybersecurity certification framework for ICT products, services and processes [,] it does not include minimum cybersecurity legal requirements for ICT products." Indeed, the addition of cybersecurity aspects to the safety considerations in the GPSR proposal would allow national market surveillance authorities to take specific measures, including the

---

[308] DIGITALEUROPE (2022) *DIGITALEUROPE comments on the proposed General Product Safety Regulation*. DIGITALEUROPE, Brussels (18 January 2022). Available from <https://www.digitaleurope.org/resources/digitaleurope-comments-on-the-proposed-general-product-safety-regulation>.

[309] *Ibid*.

[310] GPSR proposal, *supra* note 198, Article 7(1)(h).

[311] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, 15. ELI: <http://data.europa.eu/eli/reg/2019/881/oj> (henceforth: 'Cybersecurity Act').

possibility to send notifications to the EU Safety Gate (the EU rapid alert system for dangerous non-food products). This would also allow the withdrawal of any IoHT (hardware) devices or interconnected software from the market on the grounds of cybersecurity flaws that have an impact on safety.

The proposed addition of cybersecurity aspects to the definition of safety has received mixed reactions. As a proponent, the EDPS recommended that the GPSR proposal's definition of 'safety' could go even beyond to also include 'data protection aspects in case the products involve personal data processing operations'.[312] If the legislator would incorporate this recommendation, it would establish a clear link between consumer protection law (general product safety legislation) and data protection law. It would supplement Article 35(1) of the GDPR[313] under which the controller has an obligation to carry out a data protection impact assessment "where a type of processing in particular using new technologies [...] is likely to result in a high risk to the rights and freedoms of natural persons". However, several stakeholders have rejected the inclusion of cybersecurity aspects among the aspects to consider for assessing the safety of products.[314] According to a counter-argument: "such a stretch of product safety legislation would not be necessary", because "product safety legislation is intended only to protect consumers from physical harm immediately caused by a product itself", "[s]ecurity and safety considerations should thus only converge when the security threat (i.e., the hacking) causes a direct safety risk (i.e., physical injury to a consumer").[315] The counter-argument adds that "regulatory interventions conflating security and safety risks outside of these two situations is unnecessary, and would

---

[312] Formal comments of the EDPS on the Proposal for a Regulation on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, 4. Available from: <https://edps.europa.eu/system/files/2021-08/21-08-18_comments_product_safety_en.pdf>.

[313] 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), OJ L 119, 4.5.2016, 1–88. ELI: <http://data.europa.eu/eli/reg/2016/679/oj> (henceforth: 'GDPR').

[314] *See* General Product Safety Regulation (GPSR) proposal: summary of the public feedback received after the adoption of the proposal. European Commission letter to the General Secretariat of the Council (26 January 2022), 4. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5720_2022_INIT&from=EN>.

[315] Google (2020) *Google's response to the Inception Impact Assessment (IIA) on the General Product Safety Directive*. Feedback to General Product Safety Directive – review. Google, Brussels (1 September 2020), 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review/F547535_en>.

cause confusion as to what regulation applies when consumers experience a security issue versus a safety issue."[316]

3.1.3.) Cyber Resilience Act proposal

The Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020[317] ('Cyber Resilience Act proposal') lays down essential cybersecurity requirements for placing software and hardware products on the Union market. According to Article 7 of the Cyber Resilience Act proposal and with reference to Article 2(1)(b) of the GPSR proposal, the Cyber Resilience Act proposal shall function as *lex specialis* to the GPSR proposal in terms of cybersecurity requirements and related safety risks for products that are not covered by Union harmonised legislation. Accordingly, Recital 12 of the Cyber Resilience Act proposal explains that the Cyber Resilience Act proposal does not cover (*in vitro* diagnostic) medical devices, because the MDR (and the IVDR) address related cybersecurity risks by establishing essential requirements for (*in vitro* diagnostic) medical devices that function through an electronic system or that are software themselves.[318] *A contrario*, the Cyber Resilience Act proposal covers IoHT devices that are not 'medical devices'; or to put it simply, the Cyber Resilience Act applies to digital consumer health products (wellness applications). The significance of this is that when placing a digital consumer health product (wellness application) on the market, "manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I" of the Cyber Resilience Act proposal.[319] In addition to this, "manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I" of the Cyber Resilience Act proposal.[320]

---

[316] *Ibid*.

[317] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022) 454 final), Brussels (15 September 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454> (henceforth: 'Cyber Resilience Act proposal').

[318] Due to this scope of application, Article 8 of the Cyber Resilience Act proposal (regulating the cybersecurity requirements of 'products with digital elements classified as high-risk AI systems') does not apply to AI-enabled medical devices.

[319] Cyber Resilience Act proposal, *supra* note 311, Article 10(1).

[320] *Ibid*., Article 10(5).

Furthermore, "the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V" of the Cyber Resilience Act proposal.[321]

Article 3(1) of the Cyber Resilience Act proposal defines 'product with digital elements' as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately". The Cyber Resilience Act proposal seems to take for granted that software and hardware fall under the notion of 'product' under general product safety legislation, but this is far from evident.[322] As a further shortcoming, the Cyber Resilience Act proposal does not classify digital consumer health product (wellness application) as a 'critical product with digital elements'. According to Article 3(3) of the Cyber Resilience Act proposal, "'critical product with digital elements' means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III". However, Annex III does not list consumer health products (wellness applications) as critical products with digital elements despite the fact that they have an "intended use of performing critical or sensitive functions, such as processing of personal data".[323]

3.2.) Data protection and cybersecurity requirements deriving from the qualification of Internet of Health Things and interconnected software (AI systems) as medical device(s)

The provisions of the MDR may affect the protection of privacy and personal data in a number of ways. The MDR contains a direct reference to data protection law: Article 110 of the MDR requires that Member States shall apply the GDPR (in place of the repealed Directive 95/46/EC referred to by the MDR) to the processing of personal data pursuant to the MDR. As for the processing of personal data carried out by the Commission pursuant to the MDR, Regulation (EU) 2018/1725 on the protection of natural persons with regard to

[321] *Ibid*., Article 10(3).

[322] *See* European Commission Directorate-General for Justice and Consumers *et al*., *supra* note 303, 142 [footnote 252].

[323] Cyber Resilience Act proposal, *supra* note 311, Article 6(2)(c).

the processing of personal data by the EU institutions, bodies, offices and agencies[324] applies (in place of the repealed Regulation (EC) No 45/2001 referred to by the MDR). The MDR regulates the processing of personal data in relation to several issues, such as the European database on medical devices ('Eudamed'), clinical investigations and clinical performance studies, vigilance, and market surveillance and record-keeping.[325] These data processing operations are considered necessary to achieve the goals that the MDR aims for.[326] The most relevant legal basis for these operations is Article 9(2)(i) of the GDPR, which sets forth that: "processing is necessary for reasons of public interest in the area of public health, such as [...] ensuring high standards of quality and safety of health care and of [...] medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".

In addition to this, Annex I of the MDR sets general safety and performance requirements for the design and manufacture of devices that incorporate electronic programmable systems, including software, or software that are devices in themselves. These requirements bear relevance for the implementation of the concept of 'data protection by design and default'. Annex I states that: "[f]or devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation."[327] In addition, "[m]anufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended."[328] This latter requirement must also be included in the information in the instructions for use.[329]

---

[324] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, 39. ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>.

[325] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission proposals for a Regulation on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and a Regulation on in vitro diagnostic medical devices. Brussels (8 February 2013), 2 (para. 4). Available from <https://edps.europa.eu/sites/default/files/publication/13-02-08_in_vitro_devices_en.pdf>.

[326] *Ibid*., 5 (para. 20).

[327] MDR, *supra* note 209, Annex I, Chapter II, para. 17.2.

[328] *Ibid*., Annex I, Chapter II, para. 17.4.

[329] *Ibid*., Annex I, Chapter III, para. 23.4(ab).

With reference to Annex II of the MDR, IoHT (hardware) medical devices and MDSW (including AI-enabled medical devices) must include in their technical documentation a device description and specification. Although the elements of a device description are set forth by the MDR, they have significant implications to data protection requirements. For example, the "intended purpose", the "intended users", "the principles of operation of the device and its mode of action", and "a general description of the key functional elements, e.g. its parts/components (including software if appropriate), its formulation, its composition, its functionality" are all indicative of how data processing operations may take place by use of the device. Moreover, the manufacturer has to provide "the rationale for the qualification of the product as a device", which underpins the entire qualification assessment.[330] Furthermore, in its product verification and validation documentation (which is part of the technical documentation), the manufacturer is required to "detail information regarding test design, complete test or study protocols, methods of data analysis, in addition to data summaries and test conclusions".[331] This information shall include, in particular, "software verification and validation (describing the software design and development process and evidence of the validation of the software, as used in the finished device."[332]

In the following, this analysis highlights three legal challenges stemming from the provisions of the MDR that affect (but also question the adequateness of) data protection requirements for IoHT medical devices and MDSW (including AI-enabled medical devices). The first issue concerns the Eudamed, which is intended to serve a multitude of purposes set out in Article 33(1) of the MDR. With regard to the subject matter, the Eudamed enables the public to be adequately informed about IoHT devices and interconnected software (including AI systems) placed on the market, the corresponding certificates issued by notified bodies and about the relevant economic operators. The Eudamed enables unique identification of such devices within the internal market and facilitates their traceability. The Eudamed also enables the competent authorities of the Member States and the Commission to carry out their tasks relating to the MDR on a well-informed basis. Article 33(9) of the MDR determines that in relation to "the processing of personal data involved therein, the Commission shall be considered to be the controller of Eudamed and its electronic systems."

---

[330] *Ibid*., Annex II, section 1.1.

[331] *Ibid*., Annex II, section 6.

[332] *Ibid*.

The provisions of Article 33(6) of the MDR incorporate, in essence, the data protection principles of 'purpose limitation', 'data minimisation' and 'storage limitation'. However, the MDR did not follow the EDPS's recommendation that "the exclusion of directly identified patient health data from the database should be introduced as a rule for the Eudamed database."[333]

The second data protection-related issue concerns the Unique Device Identification system ('UDI system') that "allow[s] the identification and facilitate[s] the traceability of devices".[334] With reference to Article 27(1)(a) of the MDR, the UDI comprises of:

(a) a UDI device identifier ('UDI-DI') specific to a manufacturer and a device, providing access to the information laid down in Part B of Annex VI of the MDR; and
(b) a UDI production identifier ('UDI-PI') that identifies the unit of device production and if applicable the packaged devices.

For MDSW, Part C of Annex VI of the MDR prescribes that the UDI must be assigned at the system level of the software. It also requires that a UDI carrier (automatic identification and data capture ('AIDC') technology and human-readable interpretation ('HRI') representation of the UDI) is placed on the label or on the device itself. It defines AIDC as "a technology used to automatically capture data. AIDC technologies include bar codes, smart cards, biometrics and RFID". As mentioned in the previous chapter, RFID is one of the core enabling technologies of IoHT devices.

In its standards on establishing a unique identification scheme for IoT, the ISO/IEC 29161:2016 points out that "for [a] "thing" to communicate, it should possess an identifier of "which" it is."[335] In connection with this, it is important to recall Recital 30 of the GDPR: "[n]atural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them." What follows from the foregoing is that data generated by the use of an IoT device may *de facto* render the individual identifiable, if they can be associated with the UDI (or RFID) of the

---

[333] European Data Protection Supervisor, *supra* note 325, 5 (para. 22).

[334] MDR, *supra* note 209, Article 33(1)(b).

[335] International Organization for Standardization (2016): *ISO/IEC 29161:2016(en) Information technology — Data structure — Unique identification for the Internet of Things*. International Organization for Standardization, Geneva. Available from <https://www.iso.org/obp/ui/#iso:std:iso-iec:29161>.

device by means that are reasonably likely to be used to identify the individual. For this reason, privacy and data protection measures must take into consideration the potential impact of the implementation of the UDI and its traceability. For example, the explicit consent of patients/users shall be required, if their personal data is used to generate an UDI or track an IoHT medical device or MDSW.[336]

The third data protection-related issue concerns clinical investigations (clinical performance studies for *in vitro* diagnostic medical devices), vigilance and market surveillance. The MDR divides the system of reporting incidents relating to medical devices into two sets of provisions: provisions on clinical investigations governing reporting during the pre-market phase and provisions on vigilance and market surveillance governing the reporting that takes place after placing the medical device on the market. These operations require the processing of personal data at different (local, national and EU) levels. Consequently, the EDPS was on the opinion that personal data of identified or identifiable patients participating in such operations can be considered as data concerning health since they reveal information about the health status of individuals (or 'subjects') participating in medical procedures.[337] The MDR sets data protection safeguards with respect to these operations, but there seem to be shortcomings in this shield of protection. Only the provisions on clinical investigations include a specific requirement to prevent personal data of the subjects of clinical investigations to become publicly available.[338] However, there are no similar restrictions with respect to vigilance and post-market surveillance operations conducted by manufacturers, health practitioners or competent authorities. This is a problem considering that reporting of data may make patients/users of IoHT medical devices or MDSW (AI-enabled medical devices) identifiable.

As regards clinical investigations conducted to demonstrate conformity of devices, Article 62(4)(h) of the MDR sets forth that the rights of the subject to physical and mental integrity, to privacy and to the protection of the data concerning him or her must be safeguarded. Article 72(3) of the MDR provides that: "[a]ll clinical investigation information shall be recorded, processed, handled, and stored [...] in such a way that it can be accurately reported, interpreted and verified while the confidentiality of records and the personal data

---

[336] Bianchini E, Francesconi M, Testa M, Tanase M, Gemignani V (2019) Unique device identification and traceability for medical software: A major challenge for manufacturers in an ever-evolving marketplace *Journal of Biomedical Informatics* 93:103150 at 6. DOI: <https://doi.org/10.1016/j.jbi.2019.103150>.

[337] EDPS, *supra* note 325, 3 (para. 10).

[338] MDR, *supra* note 209, Article 73(4).

of the subjects remain protected". Article 72(4) of the MDR supplements this provision by prescribing that "[a]ppropriate technical and organisational measures shall be implemented to protect information and personal data processed against unauthorised or unlawful access, disclosure, dissemination, alteration, or destruction or accidental loss, in particular where the processing involves transmission over a network." Accordingly, the Clinical Investigation Plan (CIP) must set out a "[d]escription of the arrangements to comply with the applicable rules on the protection and confidentiality of personal data", in particular:[339]

(a) organisational and technical arrangements that will be implemented to avoid unauthorised access, disclosure, dissemination, alteration or loss of information and personal data processed;
(b) a description of measures that will be implemented to ensure confidentiality of records and personal data of subjects; and
(c) a description of measures that will be implemented in case of a data security breach in order to mitigate the possible adverse effects.

In connection with the foregoing, it is worth noting that the notion of 'subject' under the MDR is different to the notion of 'data subject' under the GDPR. Similarly, the scope of 'informed consent' under the MDR (to participate in a particular clinical investigation) does not overlap with the scope of '(informed) consent' under the GDPR (to agree to the processing of personal data relating to the data subject).

Finally, it is important to highlight that the MDCG issued its 'Guidance on Cybersecurity for medical devices' ('MDCG 2019-16 Rev.1') to provide manufacturers (and other actors in the supply chain) with guidance on how to fulfil all the relevant essential requirements of Annex I of the MDR with regard to cybersecurity across the life cycle of medical devices.[340] MDCG 2019-16 Rev.1 is relevant for all medical devices that incorporate electronic programmable systems and software that are medical devices in themselves. Conceptually, the document considers the relationship between (cyber)security and safety as they relate to risk. It also outlines "secure by design" practices that may contribute to a "defence in depth" strategy for the organisation during the product lifecycle. Moreover, it acknowledges that the MDR sets legal obligations only with regard to manufacturers, but it is important to recognise the role of other stakeholders (such as

[339] *Ibid*., Annex XV, Chapter II, para. 4.5.

[340] Medical Device Coordination Group (2020) *Guidance on Cybersecurity for medical devices* (MDCG 2019-16 Rev. 1) (July 2020). Available from <https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf>.

healthcare providers, integrators and operators) in the provision of secured healthcare services. For example, agreements concluded between parties are one way to ensure shared responsibility for secure management of coexisting medical devices in an IoT environment.

3.3.) Data protection and data/information security requirements under Germany's "blueprint" legislation on the reimbursability of digital health applications

In parallel with the significant changes in EU law shaping the legal framework for IoHT devices and interconnected software (AI systems), a new legal regime has emerged in the legal systems of some Member States, which aims to facilitate the market access and reimbursability of legally compliant digital health applications. Germany is spearheading these regulatory developments, while other Member States may follow suit. Optimally, the harmonisation of healthcare systems through the establishment of comparable requirements for digital health applications could drive the development of a more aligned European healthcare sector. This could facilitate a more coherent interpretation of sector-specific data protection and data/information security requirements. In the following, this part provides an overview of the relevant sections of the Germany's regulation of digital health applications, and its wider implications.

Germany's Digital Healthcare Act (*Digitale-Versorgung-Gesetz*) established the notion of 'digital health applications' (*Digitale Gesundheitsanwendungen*, 'DiGA'), which may be prescribed for patients by a physician or psychotherapist, and are reimbursable by the health insurance.[341] The prerequisite for this is that a DiGA must have successfully completed the assessment of the Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte*, 'BfArM') leading to a listing in the directory of reimbursable digital health applications (DiGA directory). The Federal Ministry of Health (*Bundesministerium für Gesundheit*) has regulated the details of this assessment

[341] Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) vom 09.12.2019 (BGBl. I 2019 S. 2562) (henceforth: 'DVG'), § 33a.

procedure in a supplementary legal regulation, the Digital Health Applications Ordinance (*Digitale Gesundheitsanwendungen-Verordnung*, 'DiGAV').[342]

The BfArM assessment procedure is an accelerated 'fast-track'[343] regulatory path for manufacturers to take their digital health applications to market: within a three-month period starting with the filing of the complete application, the BfArM has to assess the DiGA.[344] The essence of the BfArM assessment procedure assessment is the examination of the manufacturer's statements about the product qualities – including compliance with data protection and data security requirements – and the examination of the evidence provided by the manufacturer of the positive healthcare effects of the DiGA. In case scientific evidence lacks on whether the DiGA provides positive healthcare effects, then it may be preliminary listed, which means that the manufacturer receives 12 months to deliver evidence of the positive healthcare effect. The establishment of the fast-track procedure is based on the fundamental assumption that digital applications must be safe and easy to use to be successfully marketed (and become reimbursable) in healthcare. It aims for a successful link between privacy and information security on the one hand, and user-friendliness and high performance on the other hand.[345]

With reference to Article 33a of the DVG, a DiGA has the following properties:[346]

- medical device classified as risk class I or IIa (according to the MDR);
- main function is based on digital technologies;
- medical purpose is achieved through the main digital functions;
- supports the recognition, monitoring, treatment or alleviation of a disease or the recognition, treatment or alleviation or compensation of an injury or disability;

---

[342] Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020 (BGBl. I S. 768), die durch Artikel 1 der Verordnung vom 22. September 2021 (BGBl. I S. 4355) geändert worden ist (henceforth: 'DiGAV').

[343] To highlight the 'fast-track' feature of this procedure, the corresponding application process takes typically 9 months in the UK and 12-24 months in France. *See* Walzer S (2021) *The reimbursement models in healthcare & market access in Europe*. Market Access & Pricing Strategy, Weil am Rhein (12 October 2021), 19. Available from <https://www.nweurope.eu/media/15287/4the-reimbursement-models-in-healthcare-market-access.pdf>.

[344] Federal Institute for Drugs and Medical Devices (2020) *The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V: A Guide for Manufacturers, Service Providers and Users*. Federal Institute for Drugs and Medical Devices, Bonn, 7. Available from <https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.pdf;jsessionid=7AA0A5E8D2A62E1ECC39A3BA06AB1779.intranet351?__blob=publicationFile>.

[345] Federal Institute for Drugs and Medical Devices, *supra* note 344, 9.

[346] DVG, *supra* note 341, § 33a.

- does not support primary prevention (avoiding or preventing a disease); and
- used solely by the patient or together by the patient and the healthcare provider.

The BfArM clarified that the patient must interact directly with the application.[347] In principle, a DiGA can be an IoHT hardware device interconnected with software (including native apps, desktop or browser applications), as long as the main function is a "predominantly digital one", and this function has a "decisive influence" on the achievement of the intended medical purpose.[348] In any case, it is important that the manufacturer specifies its intention precisely, and it remains consistent.[349] Although the DiGA is a digital medical device, the healthcare provider (or a third-party, e.g. private health insurance) may offer supplementary services (such as teleconsultation) via the DiGA or in combination with the use of a DiGA.[350] "Telemedicinal applications can generally be part of a DiGA, if the central function is mainly based on digital technologies", but a "purely telemedicinal platform is not permissible."[351]

In order to be listed in the DiGA directory, a DiGA must meet the requirements defined in Sections 3 to 6 of the DiGAV relating to safety and suitability for use, data protection and data/information security, and quality aspects (including interoperability). With regard to the subject matter, it is important to highlight that the DiGAV specifies and supplements the requirements of the GDPR and other data protection rules for the manufacturer, for the DiGA itself, and for all systems in connection with the DiGA (including processors, such as cloud providers).[352] According to (the translation of) Article 4(1) of the DiGAV, "[d]igital health applications must meet the legal requirements of data protection and the requirements for data security according to the state of the art, taking into account the type of data processed and the associated protection levels and protection requirements." Article 4(2) of the DiGAV permits data processing "only on the basis of the consent of the insurer", pursuant to Article 9(2)(a) of the GDPR, exclusively for the following purposes:

(a) for the intended use of the digital health application by the users;

---

[347] Federal Institute for Drugs and Medical Devices, *supra* note 344, 13.

[348] *Ibid*., 13–14.

[349] Schuh M (2020) *Focus on the intended purpose of digital health applications*. Reuschlaw, Berlin. Available from <https://www.reuschlaw.de/en/news/focus-on-the-intended-purpose-of-digital-health-applications>.

[350] Federal Institute for Drugs and Medical Devices, *supra* note 344, 15.

[351] *Ibid*., 16.

[352] *Ibid*., 37.

(b) for the proof of 'positive healthcare effects' (which is defined by Articles 8(1)–8(3) of the DiGAV as a patient-relevant medical benefit, or structural and procedural improvements in healthcare) in the context of a trial (clinical investigation);
(c) for the provision of evidence in price agreements between social health insurance funds and DiGA manufacturers; or
(d) to permanently guarantee the technical functionality, user-friendliness and further development of the digital health application.

The same provision adds that the manufacturer of the DiGA must obtain consent to data processing for the last purpose ("to permanently guarantee the technical functionality, user-friendliness and further development of the digital health application") separately from consent to data processing for the other purposes. Concerning the last purpose, the BfArM explains in its guidance that the display of user questionnaires via the DiGA for the collection and subsequent processing of feedback on user experience or on possible technical problems is permitted, but comprehensive tracking of user activities (e.g. through system logs or operational metrics) is not permitted.[353] The BfArM also notes that consent (for any of the purposes listed above) must be obtained prior to the collection and further processing of personal data, and that it does not have to be in writing, but can be given electronically.[354] Although the legal provisions of the DiGAV require consent as the legal basis, if the purpose of the data processing results from a legal obligation of the manufacturer of the DiGA, then this will be an "acceptable justification" for non-compliance with the prescribed requirements.[355]

Furthermore, it is noteworthy to point out that Article 4(3) of the DiGAV restricts the place of data processing for the abovementioned purposes to the EU, EEA, Switzerland and to third countries for which the Commission has made an adequacy decision (in accordance with Article 45 of the GDPR). Consequently, the transfer of personal data outside the EU pursuant to other legal avenues (Articles 46, 47 or 49) is not permitted for personal data processed by use of a DiGA. In this regard, the BfArM presented a legal position to clarify the admissibility of data processing outside Germany.[356] As the legal opinion notes,

---

[353] *Ibid*., 41.

[354] *Ibid*., 39.

[355] DiGAV, *supra* note 342, Annex 1.

[356] Federal Institute for Drugs and Medical Devices (2021) *Information on the admissibility of data processing outside Germany in connection with the review procedure of the BfArM pursuant to Section 139e German Social Code Book V (SGB V)*. Federal Institute for Drugs and Medical Devices. Available from

this assessment is not binding for data protection authorities. Nevertheless, the BfArM is on the view that, for instance, in case of apps offered via app stores, the DiGA manufacturer must always ensure strict data separation between login data and personal data (concerning health). This implies that the DiGA may send push messages only if they do not contain any data concerning health.

Annex 1 of the DiGAV requires the implementation of state-of-the-art data protection and data/information security measures. When selecting suitable measures, the manufacturer must consider especially the risks specific to the DiGA and its context of use. The questionnaire that the manufacturer of the DiGA must complete for its application contains forty statements that take into account both the technical implementation of the DiGA as well as the organisation of the manufacturer and its processes. Privacy (including data protection) and data/information security requirements are basic requirements with which all DiGAs must comply. In terms of the privacy requirements, the questionnaire addresses matters encompassing:

- quality of consent;
- data minimisation and adequacy;
- integrity and confidentiality;
- necessity (storage limitation);
- data portability;
- information requirements (transparency);
- privacy management;
- data protection impact assessment and risk management;
- obligation to provide evidence (accountability);
- processors;
- international data transfers; and
- data sharing warranty.

Concerning data/information security requirements, the questionnaire covers the following issues:

- information security and service management;
- prevention of data leakage;
- authentication;

<https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/Data_Processing_outside_of_Germany_FAQ.pdf;jsessionid=7AA0A5E8D2A62E1ECC39A3BA06AB1779.intranet351?__blob=publicationFile>.

- access control;
- logging;
- regular and secure update;
- safe uninstall;
- penetration testing;
- hardening (reducing vulnerability);
- use of sensors and external devices; and
- use of third-party service.

One of the main challenges of ensuring data/information security is that a "secure DiGA" is always only a snapshot. In order to meet market dynamics and the fast release cycles of DiGAs, the DiGAV takes the approach of regarding data/information security less as a conglomerate of technical measures, but rather as a process that should be anchored in the organisation.[357] This can be achieved, for example, by operating a management system for information security (ISMS), such as the ISO 27001.[358] Finally, in case there is a "very high protection" need for a DiGA (due to the type of data processed, the addressed care scenarios and/or the context of use[359]), then the DiGA must also comply with the 'Additional requirements for DiGA with very high protection requirements' set forth by Annex 1 of the DiGAV. These requirements include, for example, encryption of stored data, two-factor authentication, and measures against DoS (denial-of-service) and DDoS (distributed denial-of-service) attacks.

Overall, the pragmatism of the DiGAV is commendable. The fast-track assessment procedure permits innovators to release DiGAs and use the first 12 months on the market to gather scientific evidence regarding their safety and efficacy in a real-world setting.[360] The evaluation of digital health applications based on real-world data and evidence (in contrast to only referring to data obtained from randomised controlled clinical investigations) present

---

[357] Federal Institute for Drugs and Medical Devices, *supra* note 344, 45.

[358] *See* International Organization for Standardization (2013) *ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization, Geneva. Available from <https://www.iso.org/obp/ui/#iso:std:54534:en>.

[359] Bundesamt für Sicherheit in der Informationstechnik (2017) *BSI-Standard 200-2: IT-Grundschutz-Methodik*. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 107. Available from <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html>.

[360] Brown D (2020) *Are Germany's DiGAs the Blueprint for DTx Reimbursement in Europe?* Smart Patient (2 December 2021). Available from <https://www.smartpatient.eu/blog/frontiers-health-2020-germanys-diga-as-blueprint-for-european-dtx-reimbursement>.

opportunities, but also pose challenges. In this regard, Germany's performance-based reimbursement scheme provides incentives to assess digital tools on an ongoing basis, which may generate data far beyond the one-time results derived from traditional studies.[361] However, the legislature's decision to not impose comparably high evidence requirements for proof of positive healthcare effects of DiGAs has been criticised as an example of "digital exceptionalism".[362]

Stakeholders emphasise that, on the long-run, it is important to improve public information strategy and the training of physicians regarding the widespread implementation of the DiGAV considering that the establishment of a new legislative and procedural framework is merely the first step in creating an effectively functioning legal framework.[363] These efforts should include improved provision of information to patients, as well as education of health professionals on (new) privacy and data protection requirements in digital health. As regards the future prospects of the DiGAV, the BfArM fast-track assessment procedure will need to be adapted to accommodate the marketing of higher risk digital health applications.[364] In order to achieve legal harmonisation in the European digital health applications market, a possible regulatory solution could be that it is sufficient for manufacturers to generate evidence once, and if the digital health application is approved in one EU Member State and receives CE certification, then the approval in other Member States should become automatic.[365]

The DiGAV has set a blueprint for other countries to see what works (and what does not) in the adoption and diffusion of digital technologies that aim to improve patient outcomes through telehealth solutions. Several Member States have expressed that they may

---

[361] Stern AD, Matthies H, Hagen J, Brönneke JB, Debatin JF (2020) *Want to See the Future of Digital Health Tools? Look to Germany*. Harvard Business Review (2 December 2021). Available from <https://hbr.org/2020/12/want-to-see-the-future-of-digital-health-tools-look-to-germany>.

[362] Olesch A (2021) *Sven Jungmann: "Is the model of reimbursable health apps in Germany a failure?"* ICT&health (1 December 2021). Available from <https://ictandhealth.com/is-the-model-of-reimbursable-health-apps-in-germany-a-failure/news>.

[363] Olesch A (2021) *A Year With Apps On Prescription In Germany*. Sidekick (19 October 2021). Available from <https://sidekickhealth.com/news/a-year-with-apps-on-prescription-in-germany>.

[364] Von Mühlenen E, Melin AS (2021) *Germany's "DiGA" Digital Health Fast Track Process Is Modeling a New Way To Regulate Market Access and Reimbursement*. Sidley Austin (10 December 2021). Available from <https://www.sidley.com/en/insights/newsupdates/2021/12/germanys-diga-digital-health-fast-track-process-is-modeling-a-new-way-to-regulate-market-access>.

[365] Markvarde A (2021) *"Digital health is happening and here to stay". One Year of DiGA Fast-Track in Germany*. Digital Health Global (29 September 2021). Available from <https://www.digitalhealthglobal.com/digital-health-is-happening-and-here-to-stay-one-year-of-diga-fast-track-in-germany/>.

use Germany's regulation as a template in their legislative endeavours.[366] For example, France plans to replicate Germany's fast-track assessment procedure in order to create an immediate market access procedure for innovative digital health products.[367] In addition to this regulatory model, there are other (alternative) advancements in terms of regulating the marketing of digital health applications. For example, the Nordic countries will establish a Nordic-wide Digital Health & Medication Platform for accreditation, dissemination and activation services for digital health apps in the Nordics.[368] Belgium, on the other hand, has already set up a national platform for reimbursable mHealth apps (and other telemedicine solutions).[369] The particularity of mHealth Belgium is that multiple stakeholders are involved in its functioning, and consists of a validation pyramid with three levels. In this pyramid, an app always enters at the lower level (M1), and may climb in the hierarchy (via M2) to the top level (M3) as far it meets the corresponding requirements for each level:[370]

(a) level 1 (M1) determines the basic criteria for an app (CE declaration as a medical device and declaration of compliance with the GDPR);

(b) level 2 (M2) is based on a risk assessment of data protection (taking into account the data category processed by the app), information security (covering identification, authentication and verification), interoperability and connectivity to the basic services of the eHealth platform;[371] and

(c) level 3 (M3) is reserved for apps for which the social-economic added value has been demonstrated and are reimbursable.

---

[366] Simonson M (2021) *Electronic wellbeing apps in Germany – An update on the DiGA journey*. Inno Lab (1 December 2021). Available from <https://innolabllc.com/electronic-wellbeing-apps-in-germany-an-update-on-the-diga-journey.html>.

[367] Lovell T (2021) *France to enable rapid market access for digital therapeutics*. Healthcare IT News (20 October 2021). Available from <https://www.healthcareitnews.com/news/emea/france-enable-rapid-market-access-digital-therapeutics>.

[368] Nordic Innovation (n.d.) *Nordic Digital Health & Medication Platform*. Nordic Innovation. Available from <https://www.nordicinnovation.org/programs/nordic-digital-health-medication-platform> (accessed 1 October 2022).

[369] GlobalData Healthcare (2021) *France to enable rapid market access for digital therapeutics*. Healthcare IT News (5 February 2021). Available from <https://www.healthcareitnews.com/news/emea/france-enable-rapid-market-access-digital-therapeutics>.

[370] mHealth Belgium (n.d.) *Validation pyramid*. mHealth Belgium. Available from <https://mhealthbelgium.be/validation-pyramid> (accessed 1 October 2022).

[371] mHealth Belgium (n.d.) *Technical file that describes the M2 criteria*. mHealth Belgium. Available from <https://mhealthbelgium.be/images/downloads/Criteria-mHealth-apps-ENv5.pdf> (accessed 1 October 2022).

3.4.) Data protection-related requirements deriving from the qualification of an Internet of Health Things device or an interconnected software as an AI system

3.4.1.) The definition of an 'AI system' and its implications to telehealth

The AI Act proposal[372] lays down harmonised rules for the placing on the market, the putting into service and the use of AI systems in the Union. A clear definition of what constitutes an AI system is paramount to ensure the implementation of a trustworthy, flexible and innovation-friendly regulatory approach to AI. However, the definition of an 'AI system' under Article 3(1) of the AI Act proposal has been subject to much criticism. Although the Council (as co-legislator) narrowed the definition proposed by the Commission with the addition of further requirements and added clarifications in Recitals (6)–(6c) of the AI Act proposal, this has not addressed most of the criticism.

Uncertainty persists as to what exactly constitutes a 'system'.[373] For example, when there is integration between an AI system and an IoT-enabled telehealth system, which interacts with a human body and its environment, it is challenging to delimit the scope of where the AI system exerts its influence. Furthermore, there are uncertainties in relation to the objectives of an AI system. Although the Second Presidency Compromise text added to Article 3(1) of the AI Act proposal that an AI system is "designed to operate with a certain level of autonomy", the conjunctive requirement "to achieve a given set of human-defined objectives" excludes objectives that are indeterminate, defined autonomously by an AI system, or by other systems in its environment. However, it would be important that an AI system, which performs indeterminate objectives, should undergo conformity assessment, even if the MDR and Article 6 of the AI Act proposal do not cover its deployment.[374] For example, this might be the case when an AI system is integrated into a digital consumer health product (wellness application).

---

[372] AI Act proposal, *supra* note 205.

[373] AstraZeneca (2021) *Feedback provided by AstraZeneca: Artificial intelligence – ethical and legal requirements*. Feedback to Artificial intelligence – ethical and legal requirements. AstraZeneca, Groot Bijgaarden (4 August 2021), 1. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665331_en>.

[374] Ryan J, Shrishak K (2021) *A serious loophole in Europe's draft AI Regulation?* Irish Council for Civil Liberties (27 October 2021). Available from <https://www.iccl.ie/news/scope-loophole-in-the-eu-ai-act-draft>.

If the AI Act proposal does not clearly define the approaches used by AI systems, then this may lead to uncertainty about the proper differentiation between AI systems and other "more classical" software or other programming applications in the field of medical technology. However, the definition proposed by the Commission contained descriptions of 'AI techniques and approaches' that had no exclusive reference to AI technology.[375] For example, the Commission included "statistical approaches, Bayesian estimation, search and optimization methods" under the umbrella of the definition. The problem with these is that they are frequently used approaches in non-AI-supported software, such as statistical software calculation generation of clinical evidence.[376] Although the Second Presidency Compromise text deleted explicit references to these approaches from the binding part of the legislative text, Recital 6(b) of the AI Act proposal added most of these approaches to the description of 'logic- and knowledge based approaches'. This description also added 'expert systems', but this has a specific meaning in the medtech sector (see Annex I of the MDCG 2019-11 Guidance), and do not always leverage AI.[377]

The category of 'logic- and knowledge-based approaches' has been criticised for being too broad and including "outdated" approaches.[378] Many of the approaches in this category use established approaches from the software engineering field, and include "traditional" coded programs and implementations of decision-trees.[379] This may encompass software with basic (and medically low risk) functionalities (such as MDSW embedded in

---

[375] German Medical Technology Association (BVMed) (2021) *BVMed positions on the draft of the "Artificial Intelligence Act" (AIA)*. Feedback to Artificial intelligence – ethical and legal requirements. BVMed, Berlin (5 August 2021), 3. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665476_en>.

[376] Sanofi (2021) *Feedback from: Sanofi*. Feedback to Artificial intelligence – ethical and legal requirements. Sanofi, Paris (22 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662846_en>.

[377] Hoffmann La Roche (2021) *Roche feedback to the European Commission's proposed Regulation of Artificial Intelligence (the "AI Act")*. Feedback to Artificial intelligence – ethical and legal requirements. Hoffmann La Roche, Basel (30 July 2021), 3. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665165_en>.

[378] Bayer (2021) *Feedback from Bayer*. Feedback to Artificial intelligence – ethical and legal requirements. Bayer, Leverkusen (29 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663359_en>.

[379] Siemens Healthineers (2021) *Siemens Healthineers' feedback to the European Commission's proposal for a Regulation laying down harmonised rules on artificial intelligence (AI Act)*. Feedback to Artificial intelligence – ethical and legal requirements. Siemens, Erlangen (6 August 2021), 2–3. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665604_en>.

smart thermometers that alerts the user when the temperature corresponds to fever).[380] By contrast, the definition under Article 3(1) of the AI Act proposal is too narrow when it refers to 'generative AI systems'. Generative models are a subclass of machine learning.[381] If the definition is too specific on this point, then it could make it easy for manufacturers/providers to argue that their solution is legally not an 'AI system'.

With regard to the aforementioned deficiencies of Article 3(1) of the AI Act proposal, it would be essential to draw a sharper distinction between traditional analytical approaches and AI-driven approaches. In this regard, there might be more clarity, if the definition focused more on the "black-box" aspect, character and purpose of the AI solution, rather than the specific technical approaches it deploys.[382] For example, the definition could be limited to programming methods, which generate outputs without systematic instructions programmed by the developer.[383] In this case, the definition would primarily cover machine-learning approaches, a term that has a more established understanding among stakeholders.[384]

Another suggestion would be to take into account the nature of AI. According to this reasoning, intelligence by definition is evidently a computational process: the conversion of information about the world into some action.[385] Building the definition around the requirement of "computing appropriate action from context" could be useful, because it would not bog down into technical details, but instead allows the focus to remain on the consequences of AI.[386] In addition, it reminds (or explains to) people that intelligence is not

---

[380] European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry (COCIR) (2021) *COCIR Feedback: Commission proposal for a European Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry, Brussels (2 July 2021), 1–2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2660588_en>.

[381] *See also* HelloFuture (2022) *Generative AI: a new approach to overcome data scarcity*. HelloFuture (21 March 2022). Available from <https://hellofuture.orange.com/en/generative-ai-a-new-approach-to-overcome-data-scarcity>.

[382] Hoffmann La Roche, *supra* note 377, 2.

[383] Alliance for Internet of Things Innovation (AIOTI) (2021) *Feedback from Alliance for Internet of Things Innovation*. Feedback to Artificial intelligence – ethical and legal requirements. Alliance for Internet of Things Innovation, Brussels (2 August 2021), 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665207_en>.

[384] Hoffmann La Roche, *supra* note 377, 3.

[385] Bryson JJ (2022) *Europe Is in Danger of Using the Wrong Definition of AI*. Wired (2 March 2022). Available from <https://www.wired.com/story/artificial-intelligence-regulation-european-union>.

[386] *Ibid*.

"human-likeness" or some kind of supernatural property, rather a physical process that we find in nature to varying degrees.[387]

3.4.2.) Functional roles and AI governance in the value chain of AI-enabled medical devices and digital consumer health products

AI ecosystems and underlying value chains are highly complex in healthcare. By way of illustration, an AI system may combine several models by utilising multiple health datasets obtained from various sources (known as 'multimodal machine learning'[388]). A consortium (consisting of different research and programming teams) may develop these models and a third party may deploy the AI system, possibly with different use cases. This example demonstrates that it is essential to regulate the governance of AI systems with regard to the complexities of ecosystems, and to allocate legal responsibilities within these ecosystems to actors that can best ensure compliance.[389]

In comparison with the Commission's proposal, the Second Presidency Compromise text defines the functional category of 'product manufacturer' in order to clarify their role and obligations within the AI value chain. According to Article 3(5a) of the AI Act proposal, 'product manufacturer' means "a manufacturer within the meaning of any of the Union harmonisation legislation listed in Annex II". By reference to point 11 of Section A of Annex II of the AI Act proposal, this definition of 'product manufacturer' encompasses the definition of 'manufacturer' provided under the Medical Devices Regulation. With regard to Article 23a(3) of the AI Act proposal, high-risk AI systems that are safety components of medical devices, the manufacturer of those products will be considered the provider of the high-risk AI system, and be subject to the obligations of providers of high-risk AI systems under Article 16 of the draft AI Act. In this way, the two functional roles may overlap.

According to Article 3(2) of the AI Act proposal, "'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI

---

[387] *Ibid*.

[388] *See* Rockenbach MABC (2021) *Multimodal AI in Healthcare: Closing the Gaps*. Medium (13 June 2021). Available from <https://medium.com/codex/multimodal-ai-in-healthcare-1f5152e83be2>.

[389] DIGITALEUROPE (2021) *DIGITALEUROPE's initial findings on the proposed AI Act*. Feedback to Artificial intelligence – ethical and legal requirements. DIGITALEUROPE, Brussels (10 August 2021). Available from <https://www.digitaleurope.org/resources/digitaleuropes-initial-findings-on-the-proposed-ai-act>.

system developed and places that system on the market or puts it into service [...]". This allocation of responsibility implicitly assumes that the developer of an AI system will be the one deploying it, or will develop the AI system directly on behalf of a deployer.[390] However, this is often not true, for example, in the context of a general purpose AI system, such as an open software image or speech recognition system. For this reason, Article 3(1b) and Article 4b of the AI Act proposal on 'general purpose AI system' were important additions in the Second Presidency Compromise text (compared to the Commission's proposal). As Recital 12aa of the AI Act proposal explains, due to their peculiar nature and in order to ensure a fair sharing of responsibilities along the AI value chain, such systems should be subject to proportionate and tailored requirements and obligations before their placing on the Union market or putting into service. The implications of Article 4b(1) of the AI Act proposal to telehealth would be that if the general purpose AI system is used as a high-risk AI system or as a component of a AI high-risk system, then the general purpose AI system must comply with the specified requirements for high-risk AI systems.

In addition to the problem of allocating legal responsibilities, inconsistencies between the AI Act proposal and the GDPR may lead to uncertainties regarding the relationship between the provider and the user of an AI system. Article 3(4) of the AI Act proposal defines the 'user' of an AI system as "any natural or legal person, public authority, agency or other body using an AI system under its authority." However, from a data protection point-of-view, the controller will often be the user rather than the provider of an AI system.[391] In these cases, the controller-user (e.g. clinic, laboratory) would be responsible for implementing appropriate technical and organisational measures (under Article 32 of the GDPR), but the provider of the AI system (e.g. medical device software manufacturer) would be responsible for designing appropriate data governance and management practices (under Article 10 of the AI Act proposal).

Furthermore, it will not always be possible for a provider to assess all use purposes of an AI system. Therefore, the initial risk assessment of an AI system (performed by the

[390] Google (2021) *Consultation on the EU AI Act Proposal: Google's submission*. Feedback to Artificial intelligence – ethical and legal requirements. Google, Brussels (15 July 2021), 3. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662492_en>.

[391] European Data Protection Board, European Data Protection Supervisor, EDPB–EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Brussels (18 June 2021), para. 20. Retrieved from <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf>.

provider) might be of a more general nature than the subsequent, more granular data protection impact assessment (carried out by the controller-user under Article 35 of the GDPR), which could also take into account the context of use and the specific use cases. In connection with this, the EDPB and EDPS reminded that the classification of an AI system as "high-risk" due to its impact on fundamental rights triggers a presumption of "high-risk" under the GDPR as far as personal data is processed.[392] On the other hand, Recital 41 of the AI Act proposal notes that even if an AI system is "high risk" under the AI Act proposal, this will not necessarily imply that the use of the system is lawful under the GDPR.

Lastly, the definition of 'user' under Article 3(4) of the AI Act proposal means "any natural or legal person, public authority, agency or other body using an AI system under its authority". By contrast, Article 2(37) of the MDR defines 'user' as "any healthcare professional or lay person who uses a device". In the context of telehealth, the definition of 'user' under the AI Act proposal will refer typically to healthcare providers, and not to individuals, natural persons ('lay persons'), who will often be the data subjects according to the GDPR. For this reason, it is not clear who would be the 'user' of an AI-enabled IoHT device under the AI Act proposal: the patient, who is wearing the device, or the healthcare provider that is remotely monitoring the patient's health condition. In order to ensure a high level of consumer protection, the AI Act proposal should therefore introduce a new category of 'end-user' ('consumer'[393] or 'end-recipient'[394]), and link this with the notion of data subjects. Alternatively, the co-legislators could add an intermediary functional category of 'deployers' to the AI Act proposal, which could be defined as 'an entity that puts into service an AI system developed by another entity without substantial modification.'[395]

---

[392] *Ibid*, para. 21.

[393] BEUC – The European Consumer Organisation (2021) *Regulating AI to Protect the Consumer: Position Paper on the AI Act*. Feedback to Artificial intelligence – ethical and legal requirements. BEUC – The European Consumer Organisation, Brussels (7 October 2021), 5. Available from <https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf>.

[394] Bogucki A, Engler A, Perarnaud C, Renda A (2022) *The AI Act and emerging EU digital acquis: Overlaps, gaps and inconsistencies*. CEPS, Brussels (14 September 2022), 20. Available from <https://www.ceps.eu/download/publication/?id=37468&pdf=CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf>.

[395] Google, *supra* note 390, 4.

3.4.3.) The implications of a risk-based approach in relation to the use of AI systems in integration with Internet of Health Things devices

The AI Act proposal follows a risk-based regulatory approach, similarly to the GDPR. Although the Explanatory Memorandum of the AI Act proposal acknowledged that stakeholders called on the legislature to define the notions/categories of 'risk', 'high-risk', 'low-risk' and 'harm', the legislative proposal did not address these terms, and refers to them with various connotations. For this reason, the risk-based approach of the AI Act proposal lacks clarity and alignment with the GDPR insofar as aspects related to the protection of personal data come into play. For example, 'high risk' under the AI Act proposal is not the same as 'high risk to the rights and freedoms of natural persons' under the GDPR. While the manufacturer of an AI system integrated with an IoHT device can usually measure and define product-related risks to safety and health, risks to fundamental rights (such as to the protection of privacy and personal data) are more subjective and use case-specific. In addition, the provider of that AI system, subject to market access obligations under the AI Act proposal, may not be in a position to assess these aspects.[396]

The risk-based approach of the AI Act proposal suffers from flaws also in relation to risks posed to individuals interacting with an AI system. Apart from Article 52(1) of the AI Act proposal, which imposes a general transparency obligation on providers to inform natural persons that they are interacting with an AI system, there are no references to risks affecting individuals. The obligations imposed on actors *vis-a-vis* the affected persons should emanate more concretely from the legal protection of the individual. The EDPB and the EDPS urged the co-legislators to address the rights and remedies available to individuals subject to AI systems.[397] Although Recital 58a of the AI Act proposal acknowledged this matter, the binding parts of the text did not address these shortcomings.

In a big data context, it is important to point out that harms are often systemic, and 'linear cause and effect' cannot always describe the relation between action and consequences.[398] In these cases, the AI Act proposal does not offer affected individuals or groups adequate legal remedy or access to harm mitigation tools. The establishment of a new

---

[396] DIGITALEUROPE, *supra* note 389.

[397] EDPB–EDPS Joint Opinion 5/2021, *supra* note 391, para. 18.

[398] McMahon A, Buyx A, Prainsack B (2020) Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond. *Medical Law Review* 28(1):155–182 at 156. DOI: <https://doi.org/10.1093/medlaw/fwz016>.

data protection right, a 'right to reasonable inferences' could help to close the accountability gap currently posed by "high-risk inferences" (i.e. inferences drawn by use of big data analytics that are privacy-invasive or reputation-damaging, or have low verifiability in the sense of being predictive or opinion-based while being used for important decisions).[399] In cases where algorithms draw "high-risk inferences" about individuals, this right would require the controller to provide *ex-ante* justification to establish that the inference to be drawn is reasonable. As regards group privacy risks (e.g. privacy risks posed to a specific and often *ad hoc* group of patients), the AI Act proposal does not provide corresponding privacy rights and duties despite the consideration that algorithmically grouped individuals may have a collective interest in how information describing the group are generated and used.[400]

In general, the risk-based approach of the AI Act proposal dictates that the primary (and seemingly only) component for assessment of any AI system are their risks (to citizen safety, health and rights).[401] In order to provide a more balanced, ratio-based assessment of AI systems, the AI Act proposal could also consider their potential benefits, similar to how the certification process of medicinal products takes into account possible advantages for patients.[402] In such cases, what drives the ultimate decision to approve a medicine is a clear assessment that weighs the risks against the possible benefits, with a positive benefit/risk ratio meaning that the advantages are overall worth the potential and known risks.[403]

As regards the integration of AI systems with IoHT devices, the risk classification of set forth by the AI Act proposal must be viewed in light of the MDR. In these cases, Article 6 of the AI Act proposal determines whether an AI system is a 'high-risk AI system' in the following ways:

- With reference to Article 6(1) and point 11 of Section A of Annex II of the AI Act proposal, an AI system that is itself a medical device shall be classified high-risk (under the AI Act proposal), if it is required to undergo a third-party conformity

[399] Wachter S, Mittelstadt B (2019) A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review* 2, 1–130 at 7–8. DOI: <https://doi.org/10.31228/osf.io/mu2kf>.

[400] Mittelstadt B (2017) From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology* 30, 475–494 at 476. DOI: <https://doi.org/10.1007/s13347-017-0253-7>.

[401] Hoffmann La Roche, *supra* note 377, 4.

[402] *Ibid*.

[403] *Ibid*.

assessment with a view to the placing on the market or putting into service of that medical device pursuant to the MDR.

- With reference to Article 6(2) of the AI Act proposal, an AI system intended to be used as a safety component of a medical device covered by the MDR shall be considered as high risk (under the AI Act proposal), if it is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that medical device pursuant to the MDR. This provision shall apply irrespective of whether the AI system is placed on the market or put into service independently from the medical device.

(Pursuant to point 12 of Section A of Annex II of the AI Act proposal, Articles 6(1) and 6(2) of the AI Act proposal also apply to an AI system that is in itself an *in vitro* diagnostic medical device, or is intended to be used as a safety component of an *in vitro* diagnostic medical device.)

Article 3(14) of the AI Act proposal defines the 'safety component of a product or system' as "a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property." However, it is unclear whether that 'safety function' would include a wide range of features that may be tangentially related to safety, but not actually safety-critical for the system (for example, a security feature in a non-safety-critical component of a system).[404] To remove this legal uncertainty and to focus on risks related to health and safety, the legislator could erase from the cited definition the requirement that a component of a product or of a system has to "fulfil a safety function for that product or system". With regard to Article 6(2) of the AI Act proposal and Article 2(2) of the MDR, an AI system intended to be used as a safety component of a medical device will be an accessory to a medical device (because it is an article, and not a medical device itself). In order to make this interpretation clear, the legislator should clarify that the 'safety component of a product or system' should be understood in the meaning of the relevant Union harmonisation legislation listed in Annex II.[405]

Considering that most AI systems that are medical devices or safety components thereof would be classified as 'high-risk' under the AI Act proposal, the classification rule under Article 6 of the AI Act proposal is too broad, and would need to be oriented towards

---

[404] Google, *supra* note 390, 10.

[405] Alliance for Internet of Things Innovation (AIOTI), *supra* note 383, 2.

the specific (e.g. healthcare) context of the application.[406] According to one argument, the AI Act proposal should be more specific in terms of defining health-related AI systems and classify all AI systems as high-risk that process data concerning health and/or interact with patients (data subjects)–not only the ones that pose high-risk of harm to the health and safety of persons or their fundamental rights.[407] For example, an AI system that is interconnected (intended to be used) with a digital consumer health device (wellness application) may pose just as high-risk to the health and safety of persons or their fundamental rights as a medical device. However, that AI system would not be classified as high-risk under the AI Act proposal. Similarly, multiple low-risk AI systems that process raw data collected by wellness applications may, in combination (cumulatively), also lead to high-risks. For this reason, there should be a test to determine whether the combination of low-risk AI systems creates a high-risk system of AI systems.[408] The AI Act proposal could also take into account the risks posed by the environment with which the AI system interacts. An AI system may interact with not only other AI systems, but also with other hardware, software or networks, which might escalate the severity and likelihood of risks. In general, additional EU-level guidance or standards would be useful to lay down specific safety, health and quality requirements for AI-enabled medical devices and wellness applications.[409] There are also calls for more clarification on the range of non-medical device uses of AI in healthcare and their classification for risk under the AI Act proposal.[410]

In certain cases, the AI Act proposal prohibits the use of AI practices due to the intensity and scope of risks that an AI system may generate. The legislator considers these practices particularly intrusive in the rights and freedoms of the concerned persons. For

---

[406] German Medical Technology Association (BVMed), *supra* note 375, 2.

[407] European Association of Hospital Pharmacists (2021) *Feedback from European Association of Hospital Pharmacists*. Feedback to Artificial intelligence – ethical and legal requirements (2 August 2021). European Association of Hospital Pharmacists, Brussels. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665208_en>.

[408] Ryan, Shrishak, *supra* note 374.

[409] European Society of Radiology (2021) *ESR Statement: European Commission proposal for a European Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. European Society of Radiology, Vienna (2 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665222_en>.

[410] Novartis International (2021) *Novartis feedback on Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. Novartis International, Basel (6 August 2021), 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665464_en>.

example, some IoHT devices generate data that may allow the identification or inference of emotions or intentions of data subjects. The use of AI for emotion recognition would entail processing of data concerning health, because it may reveal information relating to the past, current or future mental health status of the data subject. In their Joint Opinion on the draft AI Act, the EDPB and EDPS wrote that: "the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited, except for certain well-specified use-cases, namely for health or research purposes (e.g. patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation."[411] However, the AI Act proposal did not incorporate this recommendation, and classifies emotion recognition systems as high-risk only in the context of law enforcement, but not healthcare.

Article 3(34) of the AI Act proposal defines 'emotion recognition system' as "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data". This narrow definition implies that, for example, an AI-enabled mental health application that identifies or infers emotions or intentions of natural persons based on their data concerning health or other type of personal data (other than biometric data) would not qualify as an 'emotion recognition system'. The provider of such AI-enabled mental health applications (as far as the application does not qualify as a medical device) would only be subject to the general transparency obligation under Article 52(2)(a) of the AI Act proposal. This lack of legal protection is worrying considering that the vast majority of consumer mental health apps on the market process highly sensitive data without appropriate privacy and security safeguards.[412]

3.4.4) The AI Act proposal in light of the Medical Devices Regulation

For a manufacturer/provider of an AI system that is a medical device or is intended to be used as a safety component of a medical device, the obligations established by the AI Act

[411] EDPB–EDPS Joint Opinion 5/2021, *supra* note 391, para. 35.

[412] *See* Mozilla (2022) *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security*. Mozilla (2 May 2022). Available from <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/>.

proposal are thematically similar to the requirements laid down in the MDR.[413] AI-enabled medical devices would be subject to parallel regulatory frameworks covering identical matters: certain provisions of the AI Act proposal would be supplementary; other provisions would be overlapping, with some of them diverging and potentially conflicting. The MDR (coupled with the GDPR) already provides an extensive, often more detailed set of safety, health and quality requirements relating to various aspects of the AI Act proposal (e.g. risk management, quality management system, transparency or data security).[414] For example, the 'General safety and performance requirements' (Annex I) and 'Technical documentation requirements' (Annex II) in the MDR prescribe robust requirements for medical devices. However, the comparison of these provisions with the 'Technical documentation requirements' (Annex IV) set forth under the AI Act proposal shows significant overlaps. If different technical standards are harmonised under the two legislative frameworks, then these might also overlap (with possible contradictions).[415] In general, it would be desirable to avoid a situation whereby manufacturers/providers have to conform to different set of requirements and develop corresponding technical documentations and quality management systems resulting from different safety, health and quality requirements set by the MDR and the AI Act proposal.

One of the shortcomings in the regulation of medical devices is that the number of notified bodies available to carry out conformity assessments according to the MDR is limited.[416] Under the AI Act proposal, Member States will have to designate notified bodies to perform AI-related conformity assessments and market surveillance tasks. With reference to Article 43(3) of the AI Act proposal, for high-risk AI systems covered by the MDR, the provider shall follow the relevant conformity assessment as required under the MDR. However, in the case of other AI systems not covered by the MDR (e.g. AI-enabled digital consumer health products), parallel conformity assessment procedures may increase not only the compliance burden of manufacturers/providers, but also the activities of notified bodies. This could again lead to bottlenecks and further delays for the marketing of medical devices

---

[413] *See also* Palmieri S, Walraet P, Goffin T (2021) Inevitable Influences: AI-Based Medical Devices at the Intersection of Medical Devices Regulation and the Proposal for AI Regulation. *European Journal of Health Law* 28(4):341–358 at 354 *et seq*. DOI: <https://doi.org/10.1163/15718093-bja10053>.

[414] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), *supra* note 380, 2.

[415] *Ibid*.

[416] Hoffmann La Roche, *supra* note 377, 6.

that leverage AI. Another deficiency of this regulatory framework is that incident reporting channels established by the AI Act proposal in parallel with those provided under the MDR may lead to inefficient information flows.[417] Similarly, it would be important to consider that the lack of interaction between the two legal acts may place a heavy burden on manufacturers/providers of continuously learning AI systems to report changes in performance to notified bodies.[418] For these reasons, it would be essential to ensure a pragmatic solution that enables the designation of notified bodies under the AI Act proposal in an expeditious manner and in alignment with the requirements of the MDR.[419]

In addition to these problems, there are concerns deriving from the fact that the AI Act proposal attaches new definitions to notions that already exist in the MDR with different meanings.[420] Examples include the notions of 'importer', 'user'[421], 'putting into service', or 'serious incident'. In a similar way, different risk assessments under the MDR and AI Act proposal might create confusion. For example, an AI system that is a medical device may be categorised as having medium-risk (class IIa or class IIb) under the MDR, whereas the AI Act proposal may classify the same AI system as high-risk. If the risk levels defined in the AI Act proposal would correspond to the risk levels set forth in the MDR, then this would ensure more consistency.

These issues indicate that the "one-size-fits-all" (horizontal) approach of the AI Act proposal lacks the specificity to guarantee the highest level of safety, health and quality requirements for AI-enabled medical devices.[422] Duplications and unnecessary overlaps may cause legal uncertainty and additional burdens for manufacturers/providers. Overregulation may hinder innovation, and therefore prevent European patients from enjoying (first-hand)

---

[417] ResMed (2021) *ResMed consultation response: Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. ResMed, Brussels (30 July 2021), 1. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663398_en>.

[418] Doom L (2020) *Will the MDR improve regulatory oversight of AI solutions?* Aidence, Amsterdam (30 June 2020). Available from: <https://www.aidence.com/articles/mdr-oversight-of-ai-solutions>.

[419] Hoffmann La Roche, *supra* note 377, 7.

[420] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), *supra* note 380, 2.

[421] *See* Chapter 3 Part 3.4.2.

[422] Siemens Healthineers, *supra* note 379 at 2; MedTech Europe (2021) *Proposal for an Artificial Intelligence Act (COM/2021/206): MedTech Europe response to the open public consultation*. Feedback to Artificial intelligence – ethical and legal requirements (6 August 2021). MedTech Europe, Brussels, 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665532_en>.

access to cutting-edge solutions in telehealth. Despite the enormous potential for healthcare innovation in Europe, other jurisdictions have become the preferred location to first place innovative MDSW on the market. There is concern that the highlighted legal problems would further accelerate this process, and result in: (i) stifling the development of innovative solutions in Europe; (ii) increasing the costs for national healthcare systems; and (iii) potentially depriving European patients and citizens of access to state-of-the-art digital health technologies.[423] The Impact Assessment study of the AI Act proposal estimated with respect to the conformity assessment of AI-enabled medical devices that the total compliance cost of an AI "unit" would amount to around EUR 30,000.[424] Obtaining certification for an AI unit may cost on average EUR 16,800-23,000, roughly 10-14% of the development cost.[425] The establishment of a new quality management system may cost EUR 193,000-330,000 upfront plus EUR 71,400 for yearly maintenance.[426] The burdens that the AI Act proposal places on AI developers may have particularly serious impact on small and medium-sized enterprises (SMEs) based in Europe, as well as other entities looking to enter the European market.[427] This problem is amplified by the fact that SMEs make up around 95% of the medical technology industry.[428]

With regard to the abovementioned problems, it would be important to reduce overlaps and simplify compliance in order ensure legal coherence, certainty and clarity.[429] The medical device sector is already one of the most intensively regulated and harmonised product sectors in the EU. Therefore, manufacturers/providers of AI-enabled medical devices should be under extra burden, if they already meet or exceed the corresponding requirements under the framework of the MDR.[430] One suggestion would be to remove the

---

[423] Siemens Healthineers, *supra* note 379, 2.

[424] CEPS, ICF, Wavestone (2021) *Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe. Final Report*. European Commission Directorate-General for Communications Networks, Content and Technology, Brussels, 12. Available from <https://op.europa.eu/s/whEA>.

[425] *Ibid*.

[426] *Ibid*.

[427] Digital Therapeutics Alliance (2021) *Digital Therapeutics Alliance Consultation Response: Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements (6 August 2021). Digital Therapeutics Alliance, Brussels, 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665561_en>.

[428] MedTech Europe, *supra* note 13, 6.

[429] ResMed, *supra* note 417, 1.

[430] German Medical Technology Association (BVMed), *supra* note 375, 8.

MDR from Section A of Annex II of the AI Act proposal, amend the MDR and/or call on the MDCG to develop guidance for AI-enabled medical devices on AI-related requirements.[431] Another option would be to include the publication of an AI-focused implementing act under the MDR and/or the recognition of an AI-focused harmonised standard under the MDR.[432] These approaches could provide not just a less duplicitous and burdensome regulatory framework, but also a cohesive set of requirements for AI-enabled medical devices within the context of their established regulatory framework. In general, it is important to consider that the AI regulatory framework should not only focus on mitigating risks, but it needs to foster the creation of AI ecosystems in the European healthcare sector that are attractive to global innovators and supportive of future advancements.[433] Clear rules and support for innovators of all sizes may ensure that the EU does not inhibit existing and future innovators in digital health.[434]

3.4.5) Data protection requirements for AI systems used in integration with Internet of Health Things devices

As mentioned before, AI holds great promise in telehealth, because it enables the transformation of raw big data generated by the use of IoHT devices into smart, actionable data that supports health-related decision-making and the delivery of improved healthcare services. However, allocating the role of making decisions on data processing operations to machines has significant data protection implications as it poses significant risks to the rights and freedoms of natural persons. One of these issues concerns data governance. In this regard, Article 10(3) of the AI Act proposal requires that '[t]raining, validation and testing data sets shall be relevant, representative, and to the best extent possible, free of errors and

---

[431] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), *supra* note 380, 2–3.

[432] Hoffmann La Roche, *supra* note 377, 6.

[433] European Federation of Pharmaceutical Industries and Associations (EFPIA) (2021) *EFPIA Position Paper on Artificial Intelligence*. Feedback to Artificial intelligence – ethical and legal requirements (30 July 2021). European Federation of Pharmaceutical Industries and Associations, Brussels, 4. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663395_en>.

[434] Pinto R, Baracsi M (2012) Creating an environment for innovative start-ups in healthcare. *Health Policy and Technology* 1(4):187–192 at 191. DOI: <https://doi.org/10.1016/j.hlpt.2012.10.006>; EIT Health (2021) *EIT Health AI consultation response*. Feedback to Artificial intelligence – ethical and legal requirements (29 July 2021). EIT Health, Munich, 1. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663361_en>.

complete." Compared to the Commission's proposal, the AI Act proposal added that datasets should be error-free "to the best extent possible". It is important to point out that the requirement of accuracy is composed of trueness (i.e. proximity of measurement results to the true value) and precision (i.e. repeatability or reproducibility of the measurement).[435] However, both represent a certain margin of error, especially with the use of real-world data, which are particularly relevant in telehealth.[436] Errors may appear in other ways too. For example, experts often tag training data with metadata, which may contain manual errors.[437] Another example is that certain differential privacy techniques intentionally introduce noise into datasets in order to prevent the unintentional disclosure of (special categories of) personal data.[438] Considering that this noise introduces more "error" into the datasets, this might even be in conflict with Article 10(3) of the AI Act proposal. For this reason, the AI Act proposal should include an exception to the requirement of error-free datasets by permitting the use of privacy-enhancing technologies that introduce noise into datasets.

"To the extent that it is strictly necessary" and "subject to appropriate safeguards for the fundamental rights and freedoms of natural person", Article 10(5) of the AI Act proposal allows providers of AI systems to use special categories of personal data "for the purposes of ensuring bias monitoring, detection and correction in relation to high-risk AI systems". This provision would benefit the data subject due to the reduction of AI-related biases, and it would relieve AI manufacturers (at least, partially) of the complexities of processing special categories of personal data.[439] However, it is not clear how this provision interacts with the GDPR. Article 10(5) of the AI Act proposal exemplifies certain technical safeguards, which may be suitable for implementing appropriate safeguards, but there seems to be uncertainty how this provision interplays with the requirements of Article 32 of the GDPR. Moreover, Article 10(5) of the AI Act proposal lacks clarity in light of sentence 3 of Recital 41 of the AI Act proposal, which reads as follows: "[t]his Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant." This guidance for interpretation contradicts the rule provided under Article 10(5) of the AI Act proposal. It is also confusing

---

[435] Hoffmann La Roche, *supra* note 377, 9.

[436] *Ibid*.

[437] Sanofi, *supra* note 376.

[438] Google, *supra* note 390, 8.

[439] German Medical Technology Association (BVMed), *supra* note 375, 4.

why Article 10(5) of the AI Act proposal refers to the definition of special categories of personal data in Article 9(1) of the GDPR, but not to the legal exemptions listed under Article 9(2) of the GDPR. In order to bring clarity in this regard, sentence 3 of Recital 41 of the AI Act could be re-phrased in the following way: "[t]his Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, unless *otherwise provided* [emphasis added]."[440]

Although it is important to exclude bias as much as possible during the development of an AI system, the AI Act proposal should not prescribe unreasonable requirements that may hamper innovation. For example, it is worth considering whether a medically irrelevant and low-impact bias of an AI-enabled medical device should rule out its use even when otherwise the device reliably detects a particular disease and would bring significant health-related benefits for patients.[441] It is also important to consider that the elimination of bias from the training datasets of AI-enabled medical devices requires the processing of large datasets containing data concerning health.[442] Datasets to train AI systems must meet data quality criteria, including in relation to relevance, representativeness, accuracy, completeness, as well as application-area specific properties.[443] For this reason, machine learning based on anonymised or synthetic data is often inadequate in healthcare.

For computing and security reasons, certain IoT-enabled telehealth systems make use of AI on decentralised datasets stored on IoHT devices instead of uploading data to a cloud-based big data service. For example, federated learning is a technique used by AI developers to train machine learning models without centralised data collection, which enables AI systems to learn and adapt over time from real-world data without having to collect user data in centralised datasets.[444] By design, these AI systems do not log raw user data to a central server. However, this implies that it may not always be possible for these systems to demonstrate compliance with dataset requirements set forth under Article 10 of the AI Act proposal. Moreover, these systems may not generate centralised logs required by Article 12 of the AI Act proposal, and they may not be able to provide direct access to

---

[440] *Ibid*.

[441] *Ibid*, 3.

[442] *Ibid*, 3–4.

[443] Veale M, Borgesius FZ (2021) Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International* 22(4):97–112 at 103. DOI: <https://doi.org/10.9785/cri-2021-220402>.

[444] Google, *supra* note 390, 10.

datasets in line with Article 64 of the AI Act proposal.[445] Without an explicit exception for AI systems that use federated learning or other on-device learning techniques, the AI Act proposal would render the use of federate learning and other decentralised learning techniques in high-risk systems illegal, thereby undermining opportunities to improve AI systems while protecting the privacy and personal data of data subjects.[446]

Article 12(1) of the AI Act proposal requires providers of high-risk AI systems to ensure that these systems allow the generation of automatic recording of events ("logs") over the duration of the life cycle of the system. Article 16(d) of the AI Act proposal requires providers to retain copies of these logs when the system is "under their control". However, to the extent that these logs include personal data, providers presumably will need to establish an independent legal basis for such processing operations under Article 6 of the GDPR.[447] Accordingly, providers will also need to establish that such activities comply with principles relating to processing of personal data, in particular the principle of data minimisation established under Article 5 of the GDPR. As the AI Act proposal does not provide further clarity on how providers can fulfil these requirements in light of the GDPR, they may not be able to achieve the necessary level of compliance.[448]

In contrast to the GDPR, the AI Act proposal lacks provisions on organisational measures relating to the implementation and risk mitigation of AI systems. However, it would be important to ensure through the mandatory establishment of appropriate organisational mechanisms that conformity assessment procedures and post-market operations of AI systems take into consideration the inputs of health professionals and ethicists on practical and ethical considerations relating to the use of AI-enabled medical devices.[449] For example, an expert ethical review of AI applications could help to ensure respect of AI-specific, foundational ethical principles in healthcare.[450] In addition to this, it

---

[445] *Ibid*.

[446] *Ibid*.

[447] MedTech Europe, *supra* note 422, 3.

[448] *Ibid*.

[449] European Cancer Organisation (2021) *Feedback from European Cancer Organisation*. Feedback to Artificial intelligence – ethical and legal requirements. European Cancer Organisation, Brussels (6 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665530_en>.

[450] European Patients' Forum (EPF) (2021) *EPF's Response & Accompanying Statement: Public consultation on the White Paper on Artificial Intelligence*. Feedback to Artificial intelligence – ethical and legal requirements. European Patients' Forum, Brussels (6 August 2021), 8. Available from

would be important to prescribe appropriate training/qualification for the workforce that develops and/or applies an AI-enabled medical device.[451] Furthermore, there should be an established procedure for users (typically health professionals) to send feedback of their experiences of using a certain AI-enabled medical device to the provider and manufacturer.[452]

Human oversight of AI applications in healthcare can be continuous, intermittent or retrospective.[453] Article 14(1) of the AI Act proposal requires that natural persons shall oversee high-risk AI systems "during the period in which the AI system is in use". However, any AI-enabled medical device that relies solely or primarily on human attention and oversight cannot possibly keep up with the volume and velocity of algorithmic decision-making.[454] In some cases, the only effective oversight possible can take place before or after the use of an AI system as part of retrospective (periodic) performance reviews with respect to individual patients or patient cohorts. Therefore, Article 14 (1) of the AI Act proposal should set forth a more reasonable requirement that providers must guarantee human oversight in accordance with generally acknowledged technological/scientific progress.[455]

In general, it is still best to view AI more as a supporting tool that can improve the delivery of healthcare (from diagnosis to treatment), and not as a replacement to it.[456] However, in certain applications, which are limited today but are expected to grow in the

<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665528_en>.

[451] Pharmaceutical Group of the European Union (PGEU) (2021) *PGEU feedback on the European Commission Proposal for an EU Regulation on Artificial Intelligence*. Feedback to Artificial intelligence – ethical and legal requirements. Pharmaceutical Group of the European Union, Brussels (20 July 2021), 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662654_en>.

[452] Kiseleva A (2020) AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability? *European Pharmaceutical Law Review* 4:5–16 at 13. DOI: <https://doi.org/10.21552/eplr/2020/1/4>.

[453] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), *supra* note 380, 3.

[454] *Ibid*.

[455] *Ibid*, 3–4.

[456] European Patients' Forum (EPF) (2021) *Public consultation on European Health Data Space – EPF accompanying paper*. Feedback to Artificial intelligence – ethical and legal requirements. European Patients' Forum, Brussels (26 July 2021), 11. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665528_en>; *see also* Thelisson E (2022) AI Technologies and Accountability in Digital Health *In*: Compagnucci MC, Wilson M, Fenwick M, Forgó N, Bärnighausen T (eds) *AI in eHealth: Human Autonomy, Data Governance and Privacy in Healthcare*. Cambridge University Press, Cambridge, 166–206 at 182–183. DOI: <https://doi.org/10.1017/9781108921923.011>.

future, the clinical safety and performance levels of an autonomous ('no human in the loop') AI system (e.g. AI-enabled ophthalmic telesurgery[457]) may outperform those which are subject to human intervention ('human in the loop'). For those applications, the requirement of continuous human oversight may conflict with the MDR's requirement to reduce risks as far as possible. For this reason, Article 14(4)(e) of the AI Act proposal could be modified to ensure that users are able to intervene on the operation of the high-risk AI system or interrupt the system by use of a 'stop' button (or a similar procedure), unless human interference may increase risks and/or reduce performance.[458]

In order to guarantee that AI systems are understandable to developers, users and regulators, they must be transparent and explainable. Transparency requires that providers (and users) document and publish sufficient information before the deployment of an AI system. According to the EDPB-EDPS Joint Opinion on the AI Act proposal: "[d]ata subjects should always be informed when their data is used for AI training and / or prediction, of the legal basis for such processing, general explanation of the logic (procedure) and scope of the AI-system. [...] Furthermore, the controller should have explicit obligation to inform data subject of the applicable periods for objection, restriction, deletion of data etc."[459] In healthcare, good practice would entail that healthcare providers regularly publish information on how they make decisions about the use of AI and how they evaluate technology periodically, its uses, its known limitations and the role of decision-making, in order to facilitate external auditing and oversight.[460] However, the general transparency requirement under Article 52(1) of the AI Act proposal does not specify such obligations; the referred provision only requires providers to inform natural persons that they are interacting with an AI system. The EDPB-EDPS Joint Opinion on the AI Act proposal added that: "[a] right to explanation should provide for additional transparency."[461] Indeed, a prior understandable explanation of the AI system should be a prerequisite for the data subject to give informed consent to data processing by use of an AI system, and also, for the patient to make an informed decision before their submission to an AI-enabled telehealth service. An

---

[457] Urias MG, Patel N, He C *et al.* (2019) Artificial intelligence, robotics and eye surgery: are we overfitted? *International Journal of Retina and Vitreous* 5:52 at 1–2. DOI: <https://doi.org/10.1186/s40942-019-0202-y>.

[458] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), *supra* note 380, 9.

[459] EDPB–EDPS Joint Opinion 5/2021, *supra* note 391, para. 60.

[460] World Health Organization, *supra* note 163 at 27.

[461] EDPB–EDPS Joint Opinion 5/2021, *supra* note 391, para. 60.

AI system should be explainable to the best extent possible and according to the capacity of those to whom the explanation is directed (e.g. a health professional acting in the capacity of a 'user' under the AI Act proposal, or a patient acting in the capacity of a 'data subject' under the GDPR).

Finally, providers must provide a reasonable level of transparency to allow regulatory review of AI-enabled medical devices. This does not necessarily imply that every single computational step must be traceable, but market surveillance authorities should have access to assumptions and limitations, operational protocols, data properties and output decisions.[462] In order to support these activities, providers could add an algorithm change protocol to the technical documentation, which would contain elements on "how" the algorithm learns while remaining safe and effective.[463]

Article 63(9) of the AI Act proposal narrowed the possibility of notified bodies to access the source code of a high-risk AI system. According to the Commission's proposal, notified bodies would have had access to training, validation and testing datasets. However, granting full access to training datasets would be problematic where:[464]

- providers/manufacturers do not have direct access to the training data, i.e., where the training data remains behind security and privacy shields (e.g. federated learning);
- data protection or intellectual property rules do not permit providers/manufacturers to store training datasets themselves; or
- the quantity of training data is so vast that storing it would cause a disproportionate cost and environmental impact (e.g. the GPT-3 language model was trained on the entire internet).

Access to testing datasets is typically sufficient, because those datasets cover more sources of bias than training data.[465] However, the requirement to retain and grant access to datasets may actually increase data protection risks for datasets that contain personal (or

---

[462] Meszaros J, Compagnucci MC, Minssen T (2022) The Interaction of the Medical Device Regulation and the GDPR. Do European Rules on Privacy and Scientific Research Impair the Safety and Performance of AI Medical Devices? *In*: Cohen IG, Minssen T, Price II WN, Robertson C, Shachar C (eds) *The Future of Medical Device Regulation Innovation and Protection*. Cambridge University Press, Cambridge, 77–90 at 88. DOI: <https://doi.org/10.1017/9781108975452.007>.

[463] *See* Paassen R (2020) *A regulatory perspective of Artificial Intelligence in Medical Devices* (23 November 2020). QServe Group, Arnhem. Available from <https://www.qservegroup.com/eu/en/i824/a-regulatory-perspective-of-artificial-intelligence-in-medical-devices>.

[464] European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR), *supra* note 380, 4.

[465] *Ibid*.

pseudonymised) data, especially in contrast to a scenario in which they would be deleted in line with the GDPR's data minimisation and storage limitation principles.[466] Moreover, it is not clear how data should be stored and protected to meet post-market obligations under the AI Act proposal.[467]

[466] Google, *supra* note 390, 11.

[467] ResMed, *supra* note 417, 1.

CHAPTER 3:
PRIVACY AND DATA PROTECTION ASPECTS OF INTERNET OF HEALTH THINGS

1.) Protection of privacy and personal data in relation to the use of Internet of Health Things from human rights perspectives

This chapter analyses privacy and data protection issues in IoT-enabled telehealth. For this, it is first necessary to understand the nature and interaction of the right to respect for private life (privacy) and the right to personal data protection in this context. With regard to the various legal regimes of international human rights law and EU fundamental rights protection, the link between the two rights can be broadly conceptualised in three ways:[468]

(a) data protection is a subset (one of the facets) of the right to privacy based on the argument that all elements of data protection are justified by privacy concerns;

(b) the right to privacy and the right to personal data protection are separate but complementary rights, both deriving from the individual's right to informational self-determination, which is an aspect of the right to personality, and which stems from the framework right ("mother-right") of human dignity; or

(c) the right to personal data protection is an independent right, because although it overlaps with the right to privacy (since they both ensure informational and data privacy), data protection serves a number of purposes that privacy does not, and is true *vice versa*.

While none of these three models seems to provide a definite explanation of how the two rights interact, each model presents elements that may be useful for interpreting and drawing the contours of privacy and data protection in telehealth. The first model implies that the lawfulness of processing data concerning health by use of IoHT devices must be interpreted with regard to the rules (and relevant case law) on permissible/justified interferences with the right to privacy. This is the prevailing model of the UN legal instruments described below. The second model serves to highlight that the primary purpose of privacy and data protection rules is to protect human dignity. The violation of an

[468] *See* Lynskey O (2015) *The Foundations of EU Data Protection Law*. Oxford University Press, Oxford, 91–106; *see also* Fuster GG, Hijmans H (2019) The EU rights to privacy and personal data protection: 20 years in 10 questions (Discussion paper). *Exploring the Privacy and Data Protection connection: International Workshop on the Legal Notions of Privacy and Data Protection in EU Law in a Rapidly Changing World* (14 May 2019). Available from: <https://cris.vub.be/files/45839230/20190513.Working_Paper_Gonza_lez_Fuster_Hijmans_3_.pdf>.

individual's privacy or personal data may have negative consequences on the individual, irrespective of whether the violation actually leads to material harm. Non-material "harm" can result, for example, from a lack of trust in the data management and governance practices of certain IoT-enabled telehealth solutions. In turn, this lack of trust may cause loss of health benefits (which hinders the individual's right to healthcare), or a chilling effect on the exercise of information and communication rights (which impedes the free development and manifestation of the individual's personality). This model is closest to the legal framework of the Council of Europe. Finally, the third model suggests that data protection law pursues a multitude of "non-intimacy-oriented" purposes that privacy law does not capture (e.g. data quality, data security, accountability). This model best reflects the nature of EU law.

1.1.) Privacy and data protection implications of UN legal instruments in relation to the use of Internet of Health Things

International legal instruments adopted within the UN do not proclaim the right to personal data protection to be a separate, independent human right, however, the right to privacy is a long-established right in international human rights law. Article 12 of the Universal Declaration on Human Rights[469] (UDHR) marked the first time that an international legal instrument (which became customary international law) declared an individual's right "not to be subjected to arbitrary interference with his privacy, family, home or correspondence" by any State, group or person.[470] International treaty law affirmed this provision when the right to privacy was enshrined in the International Covenant on Civil and Political Rights[471] (ICCPR). Article 17 of the ICCPR repeats the wording of Article 12 of the UDHR by guaranteeing that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence" by any State, group or person, and that "[e]veryone has the right to the protection of the law against such interference".[472]

---

[469] Universal Declaration of Human Rights (adopted 10 December 1948), 217 A (III), Paris (henceforth: 'UDHR'). Available from: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

[470] *See also ibid*., Article 30.

[471] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976), A/RES/21/2200, United Nations Treaty Series 999:171 (henceforth: 'ICCPR'). Available from: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

[472] *Cf. ibid*., Articles 5(1) and 17(1)–(2).

Data protection must meet privacy requirements

In its General Comment No. 16, the UN Human Rights Committee (which monitors the implementation of the ICCPR by its State parties) reinforced that the right to privacy must be guaranteed with both vertical and horizontal effects against all interferences and attacks, whether they emanate from State authorities or from natural or legal persons.[473] Despite the pace of technological change since the adoption of General Comment No. 16 (in 1988) and the concomitant development of privacy and data protection laws, it may seem odd to rely on such an old document to draw implications from Article 17 about privacy considerations in IoT-enabled telehealth. Nevertheless, General Comment No. 16 remains an appropriate starting point for interpreting Article 17, as it sets the standards to which the UN Human Rights Committee periodically holds States in its assessment of their implementation of Article 17.[474] With regard to the subject matter, General Comment No. 16 lays down the following legal requirements:

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes."[475]

What follows from this passage is that the aim of protecting personal information processed by various devices is to protect the broader aspects of an individual's private life. In other words, to prohibit or restrict the processing of data, which could reveal information about an individual's private life, and possibly, lead to discrimination or irreversible harms.

The obligation of States to take effective measures to ensure that personal data are processed in conformity with privacy requirements is important for the legal protection of

---

[473] United Nations Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (Thirty-second session, 8 April 1988) (henceforth: 'General Comment No. 16'), paras. 1 and 9. Available from: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en>.

[474] Krishnamurthy V (2020) A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. *AJIL Unbound*, 114:26–30 at 28. DOI: <https://doi.org/doi:10.1017/aju.2019.79>; *see also* ICCPR, *supra* note 471, Article 40.

[475] General Comment No. 16, *supra* note 473, para. 10.

individuals (patients) using IoHT devices. Considering that processing of personal data in IoT-enabled telehealth systems typically relies on pervasive data collection (by sensors), linkage of datasets and the use of data science methods for big data analytics, the system creates privacy risks by allowing the possibility to draw potentially invasive inferences about the individual.[476] This phenomenon (known as 'sensor fusion'), whereby data from different sensors (embedded in smart devices) are combined to generate a resulting set of information which has greater value than if information were used separately, implies that eventually "every thing may reveal everything".[477] The example of self-tracking (quantified self) IoHT devices shed light on the extent to which information can be inferred from sensors through aggregation and advanced analyses.[478] These devices often use an elementary sensor (e.g. gyroscope) to capture raw data (e.g. measure orientation and velocity), but rely on sophisticated algorithms to extract sensible information (e.g. number of steps taken by the user), which may deduce potentially sensitive information (e.g. health condition of the user). In these cases, while the individual using the IoHT device may give consent to share the original information for one specific purpose, the individual may not intend to share the secondary (derived and inferred) information for other purposes. Given that individuals are granted little control or oversight over how their personal data are used to draw such inferences about their lives, a 'right to reasonable inferences' could be introduced to help close the accountability gap, and to broaden the remit of the protection of personal data necessary to establish effective safeguards for the protection of privacy.[479] This proposed obligation that a controller provides *ex-ante* justification on why an inference is reasonable would not only expand the individual's control over their derived and inferred data, but it could also help to achieve "the most effective protection" of an individual's private life, as required by General Comment No. 16.

---

[476] *Cf.* Raij A, Ghosh A, Kumar S, Srivastava M (2011) Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. *CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Vancouver, May 2011)*, 11–20 at 11. DOI: <https://doi.org/10.1145/1978942.1978945>; Wachter S (2018) The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology* 10(2):266–294 at 267. DOI: <https://doi.org/10.1080/17579961.2018.1527479>.

[477] Peppet SR (2014) Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent. *Texas Law Review* 93:85–176 at 93. DOI: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>.

[478] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP 223) (16 September 2014), 7–8. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

[479] Wachter, Mittelstadt, *supra* note 399 at 580 *et seq*.

Legitimate limitations to the right to privacy during the COVID-19 pandemic

In the face of the COVID-19 pandemic, States have had to take effective measures to protect the right to life and health of all individuals within their territory and all those subject to their jurisdiction. The UN Human Rights Committee recognised that such measures might in certain circumstances result in restrictions on the enjoyment of individual rights guaranteed by the ICCPR.[480] For example, the technological toolbox that supported the epidemiological fight included the imposition of the use of mobile applications (IoHT devices) for contact tracing and warning, and monitoring of self-isolation (home quarantine). Any mandatory requirement to process personal (health-related and/or location) data by use of these applications amounted to an interference with the individual's right to privacy. Article 4(1) of the ICCPR acknowledges that in time of public emergency, if it threatens the life of the nation and the existence of it is officially proclaimed, the States parties to the ICCPR may take measures derogating from their obligations under the ICCPR to the extent strictly required by the exigencies of the situation. However, the UN Human Rights Committee reminded that States parties should not derogate from ICCPR rights or rely on a derogation made when they are able to attain their public health objectives by invoking the possibility of introducing reasonable limitations on certain rights, such as Article 17 (right to privacy), in accordance with their provisions.[481] In connection with vaccinations, it shall be borne in mind that even in times of public emergency, it is forbidden to make anybody subject to medical or scientific experimentation without the individual's free consent, since this is a non-derogable right under Article 4(2) of the ICCPR.

'The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (as a subsidiary means for the determination of the rules of international law) sets the general interpretative principles relating to the justification of limitations, including any limitations to the right to privacy. According to this instrument: "public health may be invoked as a ground for limiting certain rights in order to allow a state to take measures dealing with a serious threat to the health of the population or individual members of the population. These measures must be specifically

---

[480] United Nations Human Rights Committee, Statement on derogations from the Covenant in connection with the COVID-19 pandemic (30 April 2020), CCPR/C/128/2, para. 2. Available from: <https://www.ohchr.org/Documents/HRBodies/CCPR/COVIDstatementEN.pdf>.

[481] *Ibid*., para. 2(c); *see also* United Nations Human Rights Committee, General Comment No. 29: States of Emergency (Article 4) (31 August 2001), CCPR/C/21/Rev.1/Add.11, paras. 4–6. Available from: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.11&Lang=en>.

aimed at preventing disease or injury or providing care for the sick and injured. [...] Due regard shall be had to the international health regulations of the World Health Organization."[482] The Siracusa Principles adds to this that "the scope of a limitation [...] shall not be interpreted so as to jeopardize the essence of the right concerned."[483] "All limitation clauses shall be interpreted strictly and in favor of the rights at issue", and "in the light and context of the particular right concerned."[484] Any limitation must meet the requirements of legality, necessity, proportionality and non-discrimination.[485] As for proportionality, the United Nations Human Rights Office of the High Commissioner has explained that the limitation (interference) must be appropriate to achieve its protective function; and it must be the least intrusive option among those that might achieve the desired result.[486]

International baseline for the protection and use of health-related data

As part of the special procedures of the UN Human Rights Council, the Special Rapporteur on the right to privacy presents an annual report to the UN Human Rights Council and the General Assembly. The investigation of the relationship between privacy and health data has become one of the focal points of these annual reports.[487] In addition to this, the Special Rapporteur established the Task Force on Privacy and the Protection of Health-Related Data with a mandate to prepare its 'Recommendation on the Protection and Use of Health-Related Data'. The purpose of this Recommendation, which the Special Rapporteur presented to the UN General Assembly,[488] is to serve as a minimum set of international data protection standards for the implementation of health-related data at domestic level, and to become a

---

[482] United Nations Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (28 September 1984), E/CN.4/1985/4, paras. 25–26. Available from: <https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf>.

[483] *Ibid*., paras. 2.

[484] *Ibid*., paras. 3–4.

[485] *Ibid*., paras. 9–11.

[486] United Nations Human Rights Office of the High Commissioner, Emergency Measures and COVID-19: Guidance (27 April 2020). Available from: <https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf>.

[487] *See* United Nations Special Raporteur on the right to privacy (n.d.) *Annual thematic reports*. United Nations Human Rights Office of the High Commissioner, Geneva. Available from: <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx> (accessed 1 October 2022).

[488] United Nations General Assembly, Report of the Special Rapporteur on the right to privacy (5 August 2019), A/74/277. Available from: <https://undocs.org/A/74/277>.

reference point on how health-related data must be protected in light of the right to privacy (and other human rights).[489]

Due to the digitisation of the contact between individuals and the health system, as well as the generation of large quantities of data in the course of these interactions, the Recommendation is with regard to health-related data collected through contact with smart devices.[490] Regarding digital technologies, Chapter X of the Recommendation provides guidance on 'Mobile applications, devices and systems', while Chapter XVI addresses 'AI, Big Data and Health-related Algorithmic transparency and fairness'. The significance of these provisions is that they recommend a more holistic perspective of the protection of health-related data, which is particularly important in the context of IoT-enabled telehealth systems. For example, the Recommendation proposes a "broad interpretation" to technology to which the Recommendation and legal regulations apply.[491] In line with this principle, the Recommendation provides guidance not only in relation to the use of "mobile applications, devices and wearables" in healthcare, but also for "systems" and "external hosting" of health-related data.

As for guidance for States on regulating AI in healthcare, the Recommendation puts forward more stringent requirements than the EU's AI Act proposal. For example, "patient and health worker representatives should be consulted before adopting health-related algorithms".[492] Compared to the AI Act proposal, the Recommendation also places more emphasis on the protection of data subjects with regard to the specificities of processing health-related data by use of AI systems. For example, "health workers using health-related algorithms should inform data-subjects that a health-related algorithm is being used and of the risks associated and their rights."[493] Moreover, the Recommendation contains an explicit

---

[489] Statement by Mr. Joseph Cannataci, Special Rapporteur on the right to privacy (1 March 2019) (United Nations Human Rights Council, Fortieth session, 25 February – 22 March 2019), Geneva, 6. Available from: <https://www.ohchr.org/Documents/Issues/Privacy/StatementHRC_40_Privacy.pdf>.

[490] United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, Explanatory Memorandum to the Recommendation on the Protection and Use of Health-related Data (4 October 2019), Geneva, para. 1.1. Available from: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf>.

[491] United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, Recommendation on the Protection and Use of Health-related Data (5 December 2019), para. 22.1. Available from: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf>.

[492] *Ibid*., para. 34.1(e).

[493] *Ibid*., para. 34.1(g).

provision that "[d]ata subjects harmed by health-related algorithms should be able to seek compensation".[494]

1.2.) Privacy and data protection implications of the European Convention on Human Rights in relation to the use of Internet of Health Things

Article 8 of the European Convention on Human Rights[495] (ECHR) declares the 'right to respect for private and family life'. In order to invoke this right before the European Court of Human Rights (ECtHR), an applicant must show that their complaint falls within at least one of the four interests listed in Article 8(1) of the ECHR, namely: private life, family life, home and/or correspondence. If the ECtHR determines that the applicant's claim falls within the scope of Article 8(1), then it examines whether there has been an interference with that right or whether it concerns the State's positive obligations to protect the right.[496] Article 8(2) of the ECHR permits interference with privacy as far as it is "in accordance with the law" (or prescribed by law) and is "necessary in a democratic society" to protect one of the legitimate aims stipulated in Article 8(2), such as health, or the rights and freedoms of others.

Confidentiality of health-related data serves to protect privacy and public interest

Although Article 8 of the ECHR does not explicitly refer to the protection of personal data, the ECtHR has recognised that the protection of personal data (including medical information) is of fundamental importance to the enjoyment of the right to respect for private and family life. The ECtHR held that "[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8", and "[t]he subsequent use of the stored information has no bearing on that finding.[497] "[I]n determining

---

[494] *Ibid*., para. 34.1(d).

[495] Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953), ECT No. 5, Council of Europe, Rome. Available from: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

[496] European Court of Human Rights (2020) Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence. Council of Europe, Strasbourg (31 August 2020), 7 [para. 1]. Available from: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

[497] *S. and Marper v. the United Kingdom* (nos. 30562/04 and 30566/04), European Court of Human Rights, Judgment (4 December 2008), ECLI:CE:ECHR:2008:1204JUD003056204, para. 67. Available from: <http://hudoc.echr.coe.int/eng?i=001-90051>.

whether the personal information [...] involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained".[498] Regarding the protection of health-related data, the ECtHR elaborated in *Z v. Finland* that the principle of respecting the confidentiality of personal health/medical data not only serves to respect the privacy of patients, but it also helps to preserve confidence in the health system, and therefore to protect public interest (e.g. in the case of transmissible diseases):

> "the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community [...]. The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention".[499]

Prevention of privacy violations to health-related data is a positive State obligation

In *I. v. Finland*, the ECtHR addressed a case in which the applicant argued that (the staff of) a public hospital did not adequately secure her medical data against unauthorised access. In its judgment, the ECtHR emphasised the importance of security measures in the protection of health-related data. The ECtHR confirmed that States are obliged to implement the principles of Article 8 in relation to data protection measures in order to make sure that there is no violation of the protected rights in the relationships between private parties (in case at hand, the applicant and the hospital personnel):

> "Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations

---

[498] *Ibid*.

[499] *Z v. Finland* (no. 22009/93), European Court of Human Rights, Judgment (25 February 1997), ECLI:CE:ECHR:1997:0225JUD002200993, para. 95. Available from: <https://hudoc.echr.coe.int/eng?i=001-58033>.

> inherent in an effective respect for private or family life [...]. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[500]

The ECtHR went further in its reasoning by ruling that the mere existence of general data protection rules is not enough to meet positive State obligations under Article 8 of the ECHR. The State is also obliged to create an effective system of data security to ensure that other (including private) actors do not violate the right to privacy protected by Article 8 of the ECHR:

> "the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place."[501]

Justification of interference with privacy concerning the processing of health-related data

The 'right to respect for private and family life' is not an absolute right but a so-called qualified right under the ECHR, which means that it may be interfered, if it is in accordance with the law and is necessary to protect the rights of another individual or the wider public interest. One of the requirements for the establishment of a legal basis is that the interference must be foreseeable, that is to say, the rules must be "sufficiently clear and detailed to guarantee adequate protection against interference".[502] In particular, they must contain appropriate indication as to the scope and conditions of exercise of the power conferred on the data controller to gather, record and store information, and specify the conditions in which data records may be created, the procedures that have to be followed and the information which may be stored.[503] As for implementing appropriate safeguards, the ECtHR held (in a different case with implications for the design of IoT-enabled telehealth systems) that:

---

[500] *I v. Finland* (no. 20511/03), European Court of Human Rights, Judgment (17 July 2008), ECLI:CE:ECHR:2008:0717JUD002051103, para. 36. Available from: <https://hudoc.echr.coe.int/eng?i=001-87510>.

[501] *Ibid*., para. 47.

[502] *Amann v. Switzerland* (no. 27798/95), European Court of Human Rights, Judgment (16 February 2020), ECLI:CE:ECHR:2000:0216JUD002779895, para. 76. Available from: <https://hudoc.echr.coe.int/eng?i=001-58497>.

[503] *See ibid*.

> *"the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data."*[504]

The ECtHR has pointed out that the right to privacy concerning the protection of health-related data may be limited, but always in a carefully delimited way. In *M.S. v. Sweden*, the ECtHR found that medical data communicated by one public institution to another in the context of an assessment of whether an individual satisfies the legal conditions for obtaining a benefit which the individual had requested may be deemed proportionate to the legitimate aim pursued, if it is "subject to important limitations and [is] accompanied by effective and adequate safeguards against abuse".[505] The ECHtR warned that the "disclosure of [health-related] data may dramatically affect [the individual's] private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism".[506] For example, in *Surikov v. Ukraine*, the ECtHR held that the collection and storage of information relating to an individual's health for an excessively long time period, together with the disclosure and use of such data for purposes unrelated to the original reasons for their collection, constituted a disproportionate interference with the right to respect for private life:

> "systematic storage and other use of information relating to an individual's private life by public authorities entails important implications for the interests protected by Article 8 of the Convention and thus amounts to interference with the relevant rights [...]. This is all the more true [...] when the processing affects highly intimate and sensitive categories of information, notably the information relating to physical or mental health of an identifiable individual".[507]

Similarly, in *L.H. v. Latvia*, the ECtHR concluded that the state party violated Article 8 of the ECHR, because the applicable law did not limit in any way the purpose for which an institution responsible for monitoring the quality of medical care provided in medical institutions could collect medical data:

---

[504] *M.M. v the United Kingdom* (no. 24029/07), European Court of Human Rights, Judgment (13 November 2012), ECLI:CE:ECHR:2012:1113JUD002402907, para. 200. Available from: <https://hudoc.echr.coe.int/eng?i=001-114517>.

[505] *M.S. v. Sweden* (no. 74/1996/693/885), European Court of Human Rights, Judgment (27 August 1997), paras. 42–44. Available from: <https://hudoc.echr.coe.int/eng?i=001-58177>.

[506] *Z v. Finland*, *supra* note 499, para. 96.

[507] *Surikov v. Ukraine* (no. 42788/06), European Court of Human Rights, Judgment (26 January 2017), ECLI:CE:ECHR:2017:0126JUD004278806, para. 70. Available from: <https://hudoc.echr.coe.int/eng?i=001-170462>.

> "The Court notes that the [institution] appears to have collected the applicant's medical data indiscriminately, without any prior assessment of whether the data collected would be "potentially decisive", "relevant" or "of importance" [...] for achieving whatever aim might have been pursued".[508]

Convention 108

As mentioned, the ECHR does not refer explicitly to the protection of personal data. In order to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[509] ("Convention 108"). This is the only legally binding commitment of countries in data protection with a global dimension and fully horizontal scope of application (i.e. applicable to both public and private sector data processing activities). The purpose of Convention 108 is to secure in the territory of each State for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.[510] In terms of the relevance of Convention 108 to the present topic, Article 6 prescribes that "personal data concerning health [...], may not be processed automatically unless domestic law provides appropriate safeguards."[511] Following the adoption of the Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows,[512] Convention 108 underwent a modernisation by adopting another protocol (Convention 108+)[513] to respond to new challenges in the digital era, allow safer exchanges of personal data at international level and strengthen the effective implementation of the Convention. In connection with this,

---

[508] *L.H. v. Latvia* (no. 52019/07), European Court of Human Rights, Judgment (29 April 2014), ECLI:CE:ECHR:2014:0429JUD005201907, para. 58. Available from: <https://hudoc.echr.coe.int/fre?i=001-142673>.

[509] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985), CETS No. 108, Council of Europe, Strasbourg. Available from: <https://rm.coe.int/1680078b37>.

[510] *Ibid*., Article 1.

[511] *Ibid*., Article 6.

[512] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (adopted 8 November 2001, entered into force 1 July 2004), ETS No. 181, Council of Europe, Strasbourg. Available from: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626>.

[513] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text (128th Session of the Committee of Ministers, 17–18 May 2018), ETS No. 223, Council of Europe, Elsinore. Available from: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>.

it is important to point out that Convention 108(+) is not subject to the judicial supervision of the ECtHR, but the Court has considered the Convention in its case law relating to the application of Article 8 of the ECHR.

Recommendation on the protection of health-related data

In order to develop the principles and rules laid down in Convention 108, the Committee of Ministers of the Council of Europe has adopted several (legally non-binding) recommendations. With regard to the development of new technological tools in the health sector and the exponential growth of the volume of health-related data processed, the Committee of Ministers adopted 'Recommendation CM/Rec(2019)2 on the protection of health-related data'.[514] The Recommendation provides guidelines for member States on regulating the processing of health-related data in order to guarantee respect for the right to privacy and protection of personal data and to facilitate the development of secure, interoperable health information systems. Principle 3 of the Recommendation essentially defines IoHT devices under the term 'mobile devices', which means "a set of tools accessible in a mobile environment making it possible to communicate and manage health-related data remotely. They may take different forms, such as connected medical objects and devices which can be used for diagnostic, treatment or well-being purposes, among other things". The Explanatory memorandum to the Recommendation describes 'mobile devices' as "the concept of connected devices for health-related data management purposes [...] [f]rom medical systems to "m-health" or "quantified self" applications".[515] Principle 16.1 of the Recommendation points out that: "[w]here the data collected by mobile devices, implanted in the individual or not, may reveal information on the physical or mental state of an individual in connection with their health and well-being or concern any information regarding health-care and social welfare provision, they constitute health-related data." "However, where health-related data are not collected or processed in the context of a care provision activity by health professionals, and are used only by the person who collects them, the legal and functional framework for the processing of health-related data as defined in

[514] Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (adopted by the Committee of Ministers at the 1342nd meeting of the Ministers' Deputies, 27 March 2019), Council of Europe. Available from: <https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e>.

[515] Council of Europe, 5.1 Steering Committee on Media and Information Society (CDMSI), Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (1342nd meeting, 27 March 2019), Council of Europe, para. 38. Available from: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093339f8>.

this Recommendation would not be applicable to them (household exemption)."[516] It is also worth highlighting that Principle 16.2 of the Recommendation goes beyond data protection roles by recommending that: "clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer and the software distributor, whose respective roles must be determined in advance."

Although there is a convergence in recently adopted international and supranational legal instruments on the definition of 'health-related data', the use of different terms and accompanying definitions makes it difficult to grasp the exact scope of data that fall under legal protection.[517] For example, the aforementioned Explanatory memorandum to the Recommendation provides a broader interpretation to the term 'health-related data' than the corresponding authoritative interpretations of Article 4(15) and Recital 35 of the GDPR:[518]

> "25. The term "health-related data" will henceforth be preferred to "medical data" so that the protective system can be applied to all processing of personal data relating to a person's health and go beyond the scope of the medical professions, given that the sensitive data in question are increasingly used outside this environment.
>
> 26. It conveys a broad concept of health data, which includes the processing of information on the past, present and future (regarding notably genetic data and the predictive dimension of their analysis), physical or mental health of a person, who may be sick or healthy. [...]
>
> 28. [Health-related data] also concerns so-called medical welfare or welfare data, which refers to all data generated by professionals practising in the general welfare and medical welfare sector if they help to characterise the data subject's state of health. For the sake of simplicity, the term health-related data also covers the term medical welfare data.
>
> 29. Health-related data should be defined so that the information characterising a person's health situation as a whole is also afforded appropriate protection, including with regard to its medical and social welfare dimension. It can also include all information concerning the person's lifestyle and well-being where it is connected to her or his health."

---

[516] *Ibid*., para. 153.

[517] *See also* Mulder T (2019) The Protection of Data Concerning Health in Europe. *European Data Protection Law Review* 5(2):209–220. DOI: <https://doi.org/10.21552/edpl/2019/2/10>.

[518] *Cf*. under this chapter: '2. The scope of data concerning health under the GDPR with regard to the use of Internet of Health Things devices'; *see also* Malafosse JB (2015) *Introductory Report for updating Recommendation R(97)5 of the Council of Europe on the protection of medical data*. T-PD(2015)07, Council of Europe, Strasbourg (15 June 2015), 1–2. Available from: <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a601a>.

1.3.) Privacy and data protection implications of the EU Charter of Fundamental Rights with regard to the use of Internet of Health Things devices

Article 8 of the Charter of Fundamental Rights of the European Union[519] ('Charter') establishes the 'right to the protection of personal data', which sits alongside the 'right to respect for private and family life' under Article 7 of the Charter. The 'Explanations relating to the Charter of Fundamental Rights' provides the following explanation on Article 7 of the Charter:

> "The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR. To take account of developments in technology the word 'correspondence' has been replaced by 'communications'.
>
> In accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR".[520]

Regarding Article 8 of the Charter, the 'Explanations relating to the Charter of Fundamental Rights' adds the following reasoning:

> "This Article has been based on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC 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 [...] as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States. Article 286 of the EC Treaty is now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union." [521]

Article 8 of the CFREU establishes "three pillars" for the right to the protection of personal data: it imposes obligations on those who decide to process personal data; grants

---

[519] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, 391–407. ELI: <http://data.europa.eu/eli/treaty/char_2012/oj>; on scope of application *see also* Court of Justice of the European Union Research and Documentation Directorate (2021) *Field of Application of the Charter of Fundamental Rights of the European Union*. Court of Justice of the European Union, Luxembourg (March 2021). Available from: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf>.

[520] Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, 17–35 at 20. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2007.303.01.0017.01.ENG>.

[521] *Ibid*.

subjective rights to the individuals whose data are processed; and establishes independent monitoring of compliance with the obligations and respect of rights.

Despite the explicit existence of the two rights in the Charter, there is a lack of consensus among scholars about the nature and interaction of these two rights under EU law, while the CJEU has not expressed itself clearly on this matter.[522] If there is indeed a 'right to the protection of personal data' that is different from the 'right to privacy' under EU law, then it is important to analyse the scope of the two rights, their interplay, essence and grounds for legitimate interference/limitation with regard to the context of IoT-enabled telehealth. In terms of their substantive scope, the 'right to the protection of personal data' covers all information relating to an identified or identifiable natural person. This interpretation results from the 'Explanations relating to the Charter of Fundamental Rights', which refers to Directive 95/46/EC (repealed by the GDPR) and Convention 108.[523] However, data protection does not cover all aspects of privacy. For example, protection against the "detection" of the (home/work/other) environment of IoHT device users, the confidentiality of electronic communications (and related metadata) in IoT-enabled telehealth systems, or protection against unsolicited communications via IoHT devices would not be guaranteed by the 'right to privacy', but not necessarily data protection. Similarly, the processing of intrinsically privacy-sensitive data by technologies relying on body-centric computing might, if anonymised, escape the reach of data protection, but the right to privacy may still safeguard them.[524]

In assessing permissible interferences/limitations of the two rights from a human rights perspective, the crux of the problem is that the requirements relating to lawful interference with the 'right to respect for private life' described in Article 8(2) of the ECHR are not exactly identical with the requirements generally applicable to limitations of the rights enshrined in the Charter.[525] Until now, the CJEU has determined the legality of

---

[522] *See* Fuster, Hijmans, *supra* note 468.

[523] Kokott J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law* (3)4: 222–228 at 225. DOI: <https://doi.org/10.1093/idpl/ipt017>.

[524] Gellert R, Gutwirth S (2013) The legal construction of privacy and data protection. *Computer Law & Security Review* 29(5):522–530 at 526–527. DOI: <https://doi.org/10.1016/j.clsr.2013.07.005>.

[525] *See* Fuster GG, Gutwirth S (2014) A legal tool for the prospective assessment of EU fundamental rights compliance. *In*: Fuster GG, Gutwirth S, Somody B, Székely I (eds) *Consolidated legal report on the relationship between security, privacy and personal data protection in EU law* (Deliverable 5.2). The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making (PRISMS), 9–27 at 14–15. Available from: <https://www.researchgate.net/publication/289539808_Consolidated_legal_report_on_

interferences/limitations with the two rights on a case-by-case basis. In general, the CJEU has followed a "broad approach to scope and a strict approach" to exceptions, ensuring that there is always a controller accountable for the processing of personal data.[526] However, commentators have criticised the CJEU's efforts to distinguish the two fundamental rights. According to one criticism, "the CJEU seems to struggle with the scope of the fundamental right to data protection, including instances of when its essence would be adversely affected. As a result of that struggle, the CJEU often perplexingly portrays data protection as a minimalistic right limited to security measure."[527]

2.) The scope of data concerning health under the GDPR with regard to the use of Internet of Health Things devices

Following the abovementioned analysis of international human rights law and EU fundamental rights protection, the subsequent parts of this chapter examine the privacy and data protection implications of EU secondary legislation for the use of IoHT devices. The first issue concerns the determination of the scope of 'data concerning health' in relation to the use of IoHT devices. As it constitutes a special category of personal data, Article 9(1) of the GDPR prohibits the processing of 'data concerning health', unless there is a lawful exemption to it under Article 9(2) of the GDPR. Recital 53 of the GDPR emphasises that the processing of personal data for health-related purposes "merits higher protection". The rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe (irreversible and long-term)

---

the_relationship_between_security_privacy_and_personal_data_protection_in_EU_law_PRISMS_Deliverable_52>.

[526] *See* Docksey C, Hijmans H (2019) The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law. *European Data Protection Law Review* 5(3):300–316. DOI: <https://doi.org/10.21552/edpl/2019/3/6>.

[527] Brkan M (2019) The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal 20*(6):864–883 at 878. DOI: <https://doi.org/doi:10.1017/glj.2019.66>; *see also* Fuster GG (2014) Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection. *Birkbeck Law Review* 2(2):263–278 at 273–274. Available from: <http://www.bbklawreview.org/uploads/1/4/5/4/14547218/263_fighting-for-your-right-to-what-exactly_2-2.pdf>.

consequences on the individual's fundamental rights than misuse of other, "normal" personal data.[528] If data protection law would treat data concerning health as "ordinary" personal data, then there would be a risk that the higher level of protection could be undermined. With regard to these considerations, it is important to determine what constitutes processing of 'data concerning health' in IoT-enabled telehealth systems.

In this regard, the main challenge posed by IoT-enabled telehealth systems is that the combination of data and/or the use of data science methods may allow even seemingly innocuous raw data to come within the definition of 'data concerning health'.[529] The uptake of new 'technologies for healthy lifestyle' has questioned the boundaries of established normative data categories.[530] For example, digital consumer health (e.g. quantified self) devices may register data relating to the well-being of the individual, which does not necessarily constitute 'data concerning health' as such. However, data concerning well-being (e.g. life habits) may make it possible to draw inferences about an individual's health based on the variability of data concerning well-being over a given time period.[531] Similarly, natural language processing methods may make it possible to draw inferences about an individual's emotional health status.[532] With regard to these risks, controllers should anticipate this possible shift in the qualification of certain data categories, and take adequate measures accordingly.[533]

With reference to Article 4(15) of the GDPR, "'data concerning health' means personal data related to the physical or mental health of a natural person, including the

---

[528] Article 29 Data Protection Working Party, Letter from the Article 29 Working Party addressed to Ms Le Bail to deliver input to the Commission on the current practices at national level, the problems encountered in implementing the Directive as well as some suggestions for improvements or changes in relation to special categories of data ("sensitive data"), notification and the practical implementation of the Article 28(6) of the Directive 95/46/EC, Advice Paper on special categories of data ("sensitive data") (20 April 2011), 4. Available from: <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf>.

[529] Article 29 Data Protection Working Party, Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth, Annex – health data in apps and devices (5 February 2015), 3. Available from: <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf>.

[530] *See* Lucivero, Prainsack, *supra* note 185 at 45.

[531] *See* Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP 223), *supra* note 478, 17 [para. 4.4].

[532] *See* Zhang T, Schoene AM, Ji S, Ananiadou S (2022) Natural language processing applied to mental illness detection: a narrative review. *Npj Digital Medicine* 5(46):1–13. DOI: <https://doi.org/10.1038/s41746-022-00589-7>.

[533] Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP 223), *supra* note 478, 17 [para. 4.4].

provision of health care services, which reveal information about his or her health status". In connection with this definition, Recital 35 of the GDPR states that "[p]ersonal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject." Recital 35 elaborates that this includes "any information [...] of the data subject independent of its source". Considering that data science methods can be used to "predict" patient's health outcomes, it is important to point out that legal protection is afforded not only in relation to the past and present, but also the anticipated future health status (i.e. health risks) of the data subject.

By means of textual interpretation of Article 4(15) and Recital 35 of the GDPR, there are two controversial points of legal interpretation.[534] The first question is whether:

(a) only data that are already related to the health status of a natural person *and* are revealing of information about their health status [if the emphasis of the interpretation is on Article 4(15)]; or
(b) any data revealing information about the health status of a natural person [if the emphasis of the interpretation is on the elaboration in Recital 35]

are protected as special categories of personal data. In this regard, Article 29 Data Protection Working Party wrote that "the term 'data revealing...' is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded."[535] Moreover, the CJEU pointed out in *Lindqvist* that the expression 'data concerning health' "must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual."[536] If, indeed, the second legal interpretation prevails, then the next legal question relates to the threshold between:

(a) what constitutes 'direct revelation' of information; and
(b) what qualifies as only 'indirect revelation' of information

---

[534] Malgieri G, Comandé G (2017) Sensitive-by-distance: quasi-health data in the algorithmic era. *Information & Communications Technology Law* 26(3):229–249 at 232–234. DOI: <https://doi.org/10.1080/13600834.2017.1335468>.

[535] Article 29 Data Protection Working Party, Letter from the Article 29 Working Party addressed to Ms Le Bail [...], *supra* note 528 at 6.

[536] *See Criminal proceedings against Bodil Lindqvist* (C-101/01), Court of Justice of the European Communities, Judgment, (6 November 2003), *European Court Reports 2003 I-12971*, ECLI:EU:C:2003:596, para. 50. CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62001CJ0101>.

relating to the health status of the data subject. Considering that the nature of data (e.g. raw data, complex data) and its certainty (e.g. received data, observed data, derived data, inferred data, predicted data) have no relevance in their degree of relationship with the individual's health status, the only (unsatisfactory) solution for establishing a threshold between 'direct/indirect revelation' of information appears to be a case-by-case approach.[537]

Although the legal landscape has changed, the interpretation of Article 29 Data Protection Working Party is still indicative on when personal data constitutes 'health data (in apps and devices)':[538]

(a) Data are inherently medical data. This is the category of data about the physical or mental health status of a data subject generated in a professional medical context. This includes all data related to contacts with patients and their diagnosis and/or treatment by (professional) providers of healthcare services, and any related information on diseases, disabilities, medical history and clinical treatment. This also includes any data generated by devices or apps used in this context, irrespective of whether they qualify as 'medical devices'.

(b) There is a demonstrable relationship between the raw dataset and the capacity to determine a health aspect (health status or health risk) of a person based on the raw data itself or on the data in combination with data from other sources.

(c) Inferences are drawn about an individual's health status or health risk (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate).

In essence, this test encompasses the following key indicators: (a) intrinsic sensitivity of a certain information; (b) ease of inferring sensitive data from other information; and (c) health use purpose. These indicators can help to answer whether "quasi-health data" in IoT-enabled telehealth reaches the 'degree of revelation' required to fall under the scope of 'data concerning health'. The test can be rephrased through the so-called 'data sensitiveness by computational distance' (or 'sensitive-by-distance') interpretation tool, which takes into account two variables:[539]

---

[537] Malgieri, Comandé, *supra* note 534 at 234–235; *see also* Schneble CO, Elger BS, Shaw DM (2020) All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent. *Journal of Medical Internet Research* 22(5):e16879 at 2. DOI: <https://doi.org/10.2196/16879>.

[538] Article 29 Data Protection Working Party, Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth, Annex – health data in apps and devices, *supra* note 529, 2–5.

[539] Malgieri, Comandé, *supra* note 534 at 238–239.

(a) the intrinsic sensitiveness (a static variable) of personal data; and
(b) the computational distance/capacity required (a dynamic variable) between some kind of data and purely data concerning health.

From an objective perspective, computational capacity depends on the level of development of data retrieval technologies at a certain moment, the availability of 'accessory data', and the applicable legal restraints on processing personal data. From a subjective perspective, computational capacity depends on the specific data mining efforts (or the ability to invest in them) taken by a given controller, in particular its economic resources, human resources, and use of accessory data.

As a supplementary remark, if a natural person processes personal data by use of an IoHT device in the course of a purely personal or household activity (i.e. without transmitting data to the "public space"), it is plausible to argue that this falls under the 'household exemption' granted by Article 2(2)(c) of the GDPR. This exemption may also extend to social media groups in which members share fitness data with each other. The anonymisation of personal data in IoT-enabled telehealth systems is another case when the processing may fall outside the GDPR's scope of application. However, it is not always straightforward to ascertain whether data are fully anonymous. If the data subject can be re-identified by "means likely reasonably to be used either by the controller or by any other person", then the data concerned would remain personal data.[540] The problem with data generated by the use of an IoHT device is that it is challenging to ensure that they become anonymous data, because they are usually associated with a specific device, which *de facto* renders the individual identifiable.[541] Recital 30 of the GDPR supports this interpretation:

> "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

---

[540] GDPR, *supra* note 313, Recital 26; *see also Patrick Breyer v Bundesrepublik Deutschland* (C-582/14), Judgment of the Court (Second Chamber) (19 October 2016), Court Reports – Court of Justice, ECLI:EU:C:2016:779, paras. 42–48. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-582/14>.

[541] *See* Dove ES, Chen J (2020) To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices? *European Journal of Risk Regulation The Journal of Law, Medicine & Ethics* 48(S1):187–195 at 188. DOI: <https://doi.org/10.1177/1073110520917046>.

3.) Legal bases for processing data concerning health generated by the use of Internet of Health Things devices under the GDPR

3.1.) Substantive law

Literature and practice distinguishes between primary and secondary use of health data. The legal relevance of this distinction is that different legislation may apply to different uses of data concerning health. 'Primary use of health data' refers to the processing of data concerning health that are collected directly from a patient for the purpose of providing healthcare (or social care) service directly to that patient. 'Secondary use of health data' refers to the processing of data concerning health initially collected in the context of providing healthcare (or social care), but later (re-)used for other purposes (i.e. not directly for the benefit of the patient), such as public health, scientific research or statistical purposes. The GDPR does not explicitly mention the term 'secondary use', but it is understood to be broadly in line with the term 'further processing' of data, which is described in Recital 50 and incorporated in the principle of 'purpose limitation' under Article 5(1)(b).

The peculiarity of the legal bases for processing data concerning health generated by the use of IoHT under the GDPR relate to its primary use purpose. In this regard, it is important to point out that data concerning health collected by an IoHT device (sensor-generated data) are typically linked with other types of personal data (e.g. patient's name, date of birth or email address) that do not necessarily fall under the scope of 'special categories of personal data'. Considering that the datasets and processing operations (including their means and purpose) are intrinsically linked, they must be considered as part of the same processing activity, and therefore subject to the (stricter) legal regime applicable for the processing of data concerning health.

Under the GDPR, processing of data concerning health generated by the use of IoHT for primary use is lawful only if and to the extent that:

(a) at least one of the legal bases set forth under Article 6(1) applies; and

(b) at least one of the legal bases set forth under Article 9(2) applies, which provides exemption to the general prohibition on processing special categories of personal data declared under Article 9(1).

Although the GDPR harmonises the rules permitting legitimate exemptions to the general prohibition of processing data concerning health, Article 9(4) allows Member States to "maintain or introduce further conditions, including limitations, with regard to the processing of [...] data concerning health." This means that data protection rules in relation to the processing of data concerning health may vary country-by-country. In some Member States, where the organisation of the health system is decentralised, the legislation of subnational entities may add an extra layer of complexity to this. The organisation of the health system may also imply that the legal bases for processing data concerning health varies between different categories of healthcare providers, with publicly funded healthcare providers applying different legal bases from private healthcare providers.

A study commissioned by the European Commission on the 'Assessment of the EU Member States' rules on health data in the light of GDPR' examined the legal bases used to legitimate processing of data concerning health in Member States based on legal surveys completed by national level expert correspondents.[542] Regarding data processing for the purpose of providing healthcare to the data subject in a "traditional" in-person healthcare setting (such as a doctor's surgery or a clinic), the most frequently cited legal bases (by correspondents from Member States) were Article 6(1)(c) ("compliance with a legal obligation") in conjunction with Article 9(2)(h) ("provision of health or care").[543] In contrast, the most common legitimation for processing app or device-derived data in healthcare were Article 6(1)(a) ("consent") in conjunction with Article 9(2)(a) ("consent") (cited by correspondents from 18 Member States, of whom 13 mentioned this as the sole legal base combination).[544] (It is important to highlight that this legitimation to process data concerning health is in addition to the patient's consent for the use of such an app or device based on national medical law.).

With regard to the variety of legal bases invoked, there is no clear answer to what the appropriate legal base combination is for processing data concerning health generated by

---

[542] European Commission Consumers, Health, Agriculture and Food Executive Agency, Hansen J, Wilson P, Verhoeven E *et al*. (2021) *Assessment of the EU Member States' rules on health data in the light of GDPR*. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2818/546193>.

[543] *Ibid*., 28.

[544] *Ibid*., 35.

the use of IoHT under the GDPR. Overall, the results of the aforementioned survey indicate that as we move from in-person healthcare settings to telehealth and digital healthcare solutions, there is a greater reliance on patient consent and less frequent reference to sector-specific legislation. However, the results also show that there is significant legal fragmentation in the domain, and that the legal bases may differ case-by-case depending on the national regulatory framework and the circumstances of the case. For example, the legal bases may differ depending on whether the patient uses an IoHT device upon the recommendation or the prescription of a health professional. In the latter case, the health system-specific data protection rules (described above) may lead one Member State (or subnational entity) to require consent as the legal basis, while another to incline towards a legal obligation to record all aspects of the patient's interaction with the healthcare system.

When a controller intends to rely on the patient's consent for processing data concerning health generated by the use of IoHT, it must take into account the 'Guidelines 05/2020 on consent under Regulation 2016/679' in which the EDPB interpreted the implementation of the GDPR's consent mechanism in an online environment.[545] The EDPB reminded that consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered.[546] As long as a processing activity lasts, the controller must be able to prove that the data subject has consented.[547] For example, in an online context, it is sufficient to merely refer to a correct configuration of the respective website. Instead, the controller should retain information on the session in which the data subject expressed consent, together with documentation of the consent workflow at the time of the session, and a copy of the information that the controller presented to the data subject at that time.[548]

Considering that certain IoHT devices may offer multiple use purposes, the controller of personal data generated by the use of such IoHT device may need to seek consent from data subjects from time to time. However, there are different data protection and data governance rules between Member States concerning consent requirements for the processing of data concerning health (and their specificities in telehealth). A possible

---

[545] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (v. 1.1) (4 May 2020). Available from: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

[546] *Ibid*., 5 [para. 3].

[547] *Ibid*., 22–23 [paras. 107–108].

[548] *Ibid*., 23 [para. 108].

solution could be the implementation of 'dynamic consent', which is an interactive, personalised communications interface that allows data subjects to give or revoke consent in light of changing circumstances (e.g. processing purposes, device functionalities).[549] However, the downside of this approach is that regular requests may entail a reduction in the attention data subjects give to such requests (a phenomenon known as "consent fatigue"), which may result in data subjects approving consent requests without really analysing them in detail.[550]

Article 7(3) of the GDPR prescribes that the data subject shall have the right to withdraw his or her consent at any time, and that it shall be as easy to withdraw as to give consent. The EDPB noted that when the controller obtains the data subject's consent through a service-specific user interface (e.g. an app or the interface of an IoT device), the data subject must be able to withdraw consent via the same electronic interface, because switching to another interface for the sole reason of withdrawing consent would require undue effort.[551] In case the data subject withdraws his or her consent and the controller intends to continue to process the personal data on another legal basis, they cannot silently migrate from consent (which is withdrawn) to this other legal basis. The controller must notify the data subject about any change in the legal basis for processing in accordance with the transparency and information requirements under Articles 12 and 13 of the GDPR. In case the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation, for reasons of public interest in the area of public health, or for the establishment, exercise or defence of legal claims, in accordance with Articles 17(1)(b) and 17(3) of the GDPR. If there is no other legal basis justifying the processing (e.g. further storage) of the personal data, they must be deleted by the controller.

Finally, another challenge relating to the determination of the legal bases for processing data concerning health generated by the use of IoHT is due to the ubiquitous nature of data flows in IoT-enabled telehealth systems. The healthcare provider (as controller or processor) and the patient (as data subject) are located in different places, and the data ecosystem often consists of other players, such as the IoHT device maker's platform (as

---

[549] Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K (2015) Dynamic consent: a patient interface for twenty-first century research networks *European Journal of Human Genetics* 23:141–146 at 142. DOI: <https://doi.org/10.1038/ejhg.2014.71>.

[550] Quinn P, Habbig AK, Mantovani E, De Hert P (2013) The Data Protection and Medical Device Frameworks — Obstacles to the Deployment of mHealth across Europe? *European Journal of Health Law* 20:185–204 at 203. DOI: <https://doi.org/10.1163/15718093-12341267>.

[551] *Ibid*., 23–24 [para. 114].

controller or processor). In this ecosystem, processing activities may take place in an inter-jurisdictional context: either within the EU/EEA (e.g. between Member States), or between the EU/EEA and third countries or international organisations.[552] The GDPR is applicable to a given processing activity, if it meets either the "establishment" criterion under Article 3(1) or the "targeting" criterion under Article 3(2), or by virtue of public international law according to Article 3(3).[553] The first criteria requires that either the controller or the processor is established in the EU, while the second criteria means that the data subject is physically present in the EU.

In terms of the jurisdictional rule for cross-border healthcare provided or prescribed in a Member State other than the Member State of affiliation, Article 4(1)(a) of 'Directive 2011/24/EU on the application of patients' rights in cross-border healthcare'[554] sets forth that cross-border healthcare shall be provided in accordance with the legislation of the Member State of treatment. According to Article 3(d) of Directive 2011/24/EU, in the case of telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established. Consequently, the legal bases for processing data concerning health generated by the use of IoHT under the GDPR is impacted by the data protection and/or sectoral legislation of the Member State where the healthcare provider is established.

With reference to Article 77(1) of the GDPR and without prejudice to any other administrative or judicial remedy, the data subject has the right to lodge a complaint with a supervisory authority in the Member State of his or her habitual residence, place of work or place of the alleged infringement. It is worth noting that in the case of IoT-enabled telehealth systems, the option to bring a complaint in the "place of the alleged infringement" could give rise to "forum shopping". As regards judicial remedies, according to Article 79(2) of the GDPR, proceedings against a controller or a processor must be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively,

---

[552] *See also* Rak R (2022) International Transfers of Data Concerning Health After Schrems II: A Need for Sector-Specific Legal Avenues and Supplementary Measures. *In*: Casolari F, Gatti M (eds) *The Application of EU Law Beyond Its Borders*. CLEER Papers 2022/3. T.M.C. Asser Institute, The Hague, 187–206 at 187. Available from: <https://www.asser.nl/media/795814/cleer_022-03_web_final.pdf>.

[553] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (v. 2.1) (12 November 2019), 4. Available from: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf>.

[554] 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, OJ L 88, 4.4.2011, 45–65. ELI: <https://data.europa.eu/eli/dir/2011/24/oj>.

such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

3.2.) Case law

As IoT in healthcare is still in its relative infancy, case law relating to the legal bases for processing data concerning health generated by the use of IoHT are few and far between. Notable cases have revolved around the question of whether it is lawful to deploy thermal cameras to monitor body temperature (by non-invasive means) in the fight against COVID-19. In one case, the Spanish Data Protection Authority (DPA) launched an investigation into the underground service of Bilbao, where the operating company employed health professionals to monitor the body temperature of passengers.[555] The health professionals randomly selected passengers entering the underground station to pass through an automated thermal camera system. The camera only displayed a temperature map, and there was no identity check mechanism. The only consequence deriving from the temperature map was that the health professionals would carry out a second test, with a manual thermometer, to verify whether the temperature was above the threshold. Then, if it was still above the threshold, the passenger in question would receive a recommendation to avoid accessing the service and contact a doctor. The Spanish DPA concluded that the GDPR was not applicable to this case, as it did not fall under its material scope, because the passengers were not asked to identified themselves, so no personal data were processed relating to an identified or identifiable natural person. However, the Spanish DPA noted that although passengers remained anonymous, the procedure was carried out in public space, so anybody who was recommended not to access the undergroud would be known to have a high temperature, which would qualify as data concerning health. Therefore, it could be debatable (on a case-by-case basis) whether the circumstances make a person identifiable.

In an almost identical case concerning the use of thermal cameras at Brussels South Charleroi Airport in the framework of the fight against COVID-19, the Belgian DPA arrived

[555] *METRO BILBAO, S.A.*, Agencia Española de Protección de Datos [Data Protection Authority of Spain], case no. E/03884/2020, resolution of 24 May 2020. Available from: <https://www.aepd.es/es/documento/e-03884-2020.pdf>.

to the "opposite" conclusion.[556] In terms of the facts, the difference in this case was that all passengers had to pass through an automated thermal camera system, and in case of high temperature, the firefighter-paramedical staff of the airport carried out two follow-up manual tests and asked questions about any symptoms without taking notes. If this led to a suspicion of COVID-19, the passenger was prohibited from flying. The airport relied on Articles 6(1)(c) ("legal obligation") and 9(2)(i) ("public interest in the area of public health") of the GDPR to process personal data. However, the Belgian DPA found that there was no such legal obligation since the protocol invoked by the controller to justify the processing was not legally binding. Moreover, the protocol was not precise enough regarding the purposes pursued and the circumstances of the monitoring. The controller did not publish in its privacy policy or any other document that it is using thermal cameras for data processing, and therefore it violated the principle of transparency by not making the information accessible to passengers. The DPA concluded that the controller did not assess correctly the necessity of the processing, because the respective EU agencies did not consider that temperature control was an efficient measure.

Two further cases were related to the use of thermal cameras in specific contexts. In the first, the Spanish DPA launched another investigation on body temperature checks carried out by a department store chain.[557] The company was using thermographic cameras to verify whether employees and customers had high body temperature, as a potential symptom of COVID-19. In contrast to the abovementioned case of Metro Bilbao, in this case, private security guards supervised the measurements, and the body temperature of all persons passing through the automated thermal camera system were measured. Again, the Spanish DPA did not reach a solid conclusion regarding whether temperature measurement falls under the material scope of the GDPR, and added that the circumstances of each case should be taken into account (e.g. type of device used and whether personal data are stored). Nevertheless, in this particular case (similarly to the Metro Bilbao case), the Spanish DPA

---

[556] *Gebruik van warmtebeeldcamera's op de luchthaven Brussels South Charleroi Airport in de strijd tegen COVID-19* [Use of thermal cameras at Brussels South Charleroi Airport in the framework of the fight against COVID-19], Gegevensbeschermingsautoriteit [Data Protection Authority (Belgium)], case no. 47/2022, decision of 4 April 2022. Available from: <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-47-2022.pdf>.

[557] *EL CORTE INGLÉS, S.A.*, Agencia Española de Protección de Datos [Data Protection Authority of Spain], case no. E/03882/2020, resolution of 25 May 2020. Available from: <https://www.aepd.es/es/documento/e-03882-2020.pdf>.

found that the GDPR was not applicable, because there were no processing of data related to identifiable persons.

Lastly, the French Council of State was requested to rule on whether a fixed thermal camera installed at the entrance of the municipality building in Lisses and portable thermal cameras used in schools constituted legitimate processing of personal data under the GDPR.[558] As access to the municipality building was possible by avoiding the use of the fixed thermal camera, this did not give rise to processing. However, when portable thermal cameras were used in schools, teachers and pupils with high temperature were asked to leave. Regarding this practice, the Council of State held that the collection of health data carried out by thermal cameras constituted processing within the meaning of Article 4(2) of the GDPR. It was an automated processing to collect temperature data in order to display the existence or absence of a deviation from normal. The Council of State explained that although the identification of people whose temperature was recorded did not make it possible to regard this data as personal, it was possible that the image processed by the system, even if not stored, was sufficiently precise to be identifiable. In any case, the identity of the persons before the collection of the data was known, and therefore the data processed was personal within the meaning of the GDPR. Furthermore, the Council of State held that the processing did not have a lawful basis. Although the municipality claimed to have sent each family a form of consent to the rules of the health protocol for the return of children to class established by the public authorities, the fact that the children's access to school was subject to the acceptance of the use of the temperature measurement by thermal camera excluded in any case that the consent would be regarded as free. The processing also did not meet the conditions set forth under Articles 9(2)(g) or 9(2)(h) of the GDPR, because there were no laws and regulations providing for necessity of the use of thermal cameras. In connection with Article 9(2)(h), the additional condition prescribed in Article 9(3) was also not satisfied, i.e. the requirement that these data be handled by health professionals bound by medical secrecy.

---

[558] *L'association InterHop et les autres*, Conseil d'État [Council of State (France)], case no. 441065, decision of 26 June 2020. Available from: <https://www.conseil-etat.fr/decisions-de-justice/dernieres-decisions/conseil-d-etat-26-juin-2020-cameras-thermiques-a-lisses>.

4.) The *sui generis* database right and the rights of users to access, use and share data generated by the use of Internet of Health Things

4.1.) The *sui generis* database right relating to data obtained or created by the use of Internet of Health Things under the Database Directive and its interplay with the Data Act Proposal

The Database Directive was adopted in 1996 to protect the intellectual creativity embodied in the selection or arrangement of the contents of a database through copyright (Article 3), and the substantial investment made in the collection, verification and presentation of the contents of a database through the *sui generis* database right (Article 7).[559] The underlying consideration for creating a *sui generis* database right was that copyright was not the appropriate instrument to protect non-original databases, which are nevertheless valuable and have required substantial investment.[560] As a "quasi-property right", it comes on top of any existing rights: according to Article 7(4), the *sui generis* database right applies irrespective of the eligibility of a database (or its contents) for protection by copyright or by other rights. The *sui generis* database right protects data in an "indirect way". This means that the *sui generis* database right does not directly protect from unauthorised access to data as such, but protects against extracting or re-utilising data stemming from the systematically or methodologically arranged database.

Since its adoption, the transformation of the technological and economic landscape has tested the applicability of the Database Directive. The growth of data recorded, collected or generated by sensors or machines in an IoT environment (independent of direct and economically significant human intervention) raises the issue of whether databases containing these kind of (typically big) data would fall under the *sui generis* database right. According to the 2018 Evaluation of the Database Directive, the predominant view at the time was that the *sui generis* database right does not protect raw machine-generated

[559] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, 20–28. ELI: <https://data.europa.eu/eli/dir/1996/9/2019-06-06>.

[560] Pila J, Torremans P (2019) *European Intellectual Property Law* (Second Edition). Oxford University Press, Oxford, 490.

databases, because such databases do not meet the condition of 'substantial investment'.[561] This argument is based on the ECJ's judgments in *British Horseracing* and the *Fixtures Marketing* cases in which the ECJ held that only investments into 'obtaining' the contents of a database (i.e. seeking out existing independent material to commercialise a database) are relevant for the 'substantiality' threshold, whereas investments into the 'creation' of material are irrelevant.[562] Big datasets would generally be so-called 'spin-off databases', i.e. by-products of the company's central activity for which data would not be 'obtained', but 'created'.[563] Based on this "narrow interpretation" of the *sui generis* database right, the investments of 'producers' of sensor- or machine-generated data would therefore be excluded from the scope of the right, because such investments would have to be regarded as investments in the 'creation' of data.

However, due to digital transformation, business models are changing and the economic importance of what may appear to be a "by-product" of a business activity today may become the core of a business model tomorrow. According to an industrial survey, the collection and verification of data for database content require substantially more investment than the actual production of databases.[564] These changes may lead to the revision of the exclusion of sensor- and machine-generated data from the *sui generis* database right. For example, investments into the establishment of a measuring, obtainment or documentation infrastructure, or the methodical or systematic structuring of raw data may become relevant

---

[561] Commission Staff Working Document "Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 147 final", SWD(2018) 146 final, 25 April 2018, 35. Available from: <https://ec.europa.eu/newsroom/dae/redirection/document/51764>.

[562] *The British Horseracing Board Ltd and Others v William Hill Organization Ltd.* (C-203/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10415, EU:C:2004:695. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-203/02>, paras. 31–42; *Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP)* (C-444/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10549, EU:C:2004:697, paras. 40–53. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-444/02>; *Fixtures Marketing v Oy Veikkaus AB* (C-46/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10365, EU:C:2004:694, paras. 34–49. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-46/02>; *Fixtures Marketing v Svenska Spel AB* (C-338/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10497, EU:C:2004:696, paras. 24–37. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-338/02>.

[563] European Commission Directorate-General for Communications Networks, Content and Technology, Karanikolova K, Chicot J, Gkogka A *et al*. (2018) *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases. Annex 1: In-depth analysis of the Database Directive, article by article*. Publications Office of the European Union, Luxembourg, 60. DOI: <https://data.europa.eu/doi/10.2759/04895>.

[564] Commission Staff Working Document "Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 147 final", *supra* note 561, 36.

for assessing 'substantiality' under Article 7 of the Database Directive.[565] However, a proposed distinction between sensor-data and machine-generated data in order to delineate between 'obtaining' (collecting) data from the environment and 'creating' (generating) data by the machine itself or the internal (real-time) operation of a product or service would be questionable when taking a closer look.[566]

In the context of IoHT, sensors may both collect and generate data, depending on the nature and use of the device, which would make the abovementioned distinction insufficient (without further legal clarification). In case an AI system is used in combination with an IoHT device, investments in the development and the implementation of the AI system could meet the 'substantial' threshold, and data science methods by AI could be interpreted as 'creation' of data.[567] However, the abovementioned distinction would raise problems when an AI system is integrated with an IoHT device, so that the data-collecting device also performs systematic analysis of data. Another problem relating to the abovementioned distinction concerns whether the source of the sensors is under the exclusive control of the patient, or whether third parties (e.g. healthcare provider) can also control the sensors. Moreover, in distributed data networks, it is becoming increasingly difficult to allocate relevant investment to certain parties, which not only has repercussions on the verification of 'substantial investment' to establish legal protection, but also on the question of whom is the database maker.[568]

Article 35 (Chapter X) of the Data Act proposal[569] lays down that in order not to hinder the exercise of the rights of users to access and use IoT data (as established under Article 4 of the Data Act Proposal), or to share such data with third parties (Article 5 of the Data Act Proposal), the *sui generis* database right does not apply to databases containing data obtained from or generated by the use of an IoT product or a related service. Recital 84

---

[565] Leistner M (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. *In*: Lohsse S, Schulze R, Staudenmayer D (eds) *Trading Data in the Digital Economy: Legal Concepts and Tools.* Münster Colloquia on EU Law and the Digital Economy III. Nomos, Baden-Baden, 25–58 at 29. Available from: <https://doi.org/10.5771/9783845288185-25>.

[566] European Commission Directorate-General for Communications Networks, Content and Technology *et al*., *supra* note 114, 41–42.

[567] European Commission Directorate-General for Communications Networks, Content and Technology, Hartmann C, Allan J, Hugenholtz P *et al*. (2020) *Trends and developments in artificial intelligence : challenges to the intellectual property rights framework.* Final report. Publications Office of the European Union, Luxembourg, 93. DOI: <https://data.europa.eu/doi/10.2759/683128>.

[568] European Commission Directorate-General for Communications Networks, Content and Technology *et al*, *supra* note 114, 42.

[569] Data Act proposal, *supra* note 68.

of the Data Act Proposal explains that it is necessary to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service claim the *sui generis* database right under Article 7 of the Database Directive. According to the Commission's Impact Assessment Report, the exclusion of machine-generated data from the *sui generis* database right aims to reduce costs relating to restricted access to and the use of such data, potential transaction costs, costs of opportunistic litigation, the risk of conflicting interpretation of the Database Directive's scope, and diverging national implementations.[570] Article 35 is an expression of the understanding that the *sui generis* database right hinders innovation, which is even more true where the *sui generis* database right has the potential of creating obstacles to data sharing, and hence, a risk of hindering follow-on innovation that depends on the use of data shared by others.[571]

Article 35 of the Data Act Proposal should be considered *lex specialis* with regard to the Database Directive, because it gives precedence to the exercise of the rights of users to access, use and share data generated by the use of an IoT device or related service over the application of the *sui generis* database right under the Database Directive.[572] However, some uncertainties endure. First, it is unclear whether the first part of Article 35 should be understood as a limitation of the scope of exclusion (i.e. it only applies when the rights under Articles 4 and 5 are hindered). Alternatively, it can be interpreted as an introductory statement (i.e. a property right in data will always hinder the exercise of those rights, so the *sui generis* database right is always excluded in relation to IoT data).[573] Second, Article 35 puts "obtained" and "generated" data on the same level, which may create ambiguities for the abovementioned reasons. If the goal is to clarify that IoT data do not enjoy *sui generis* database right protection, it may be preferable to state that for the purpose of the Database

---

[570] Commission Staff Working Document Accompanying the Document "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", SWD(2022) 34 final (23 February 2022), 45. CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN>.

[571] Drexl J, Banda C, Otero BG *et al*. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)*. Max Planck Institute for Innovation and Competition, Munich, 93 [para. 257]. Available from: <https://pure.mpg.de/rest/items/item_3388757/component/file_3395639/content>.

[572] *Ibid*., 91 [para. 256].

[573] Margoni T, Gils T, Kun E (2022) *Chapter X of the Data Act and the Sui Generis Database Right*. KU Leuven CiTiP Blog (14 June 2022). Available from: <https://www.law.kuleuven.be/citip/blog/chapter-10-of-the-data-act-and-the-sui-generis-database-right/>.

Directive, IoT data as defined in the Data Act are created data and therefore excluded from protection *ab origine* (and *ex tunc*).[574] Finally, it is unclear whether Article 35 addresses only users and data holders, or whether third parties who invest substantially to obtain data from either the data holder or the data user, or to verify or present the data, may qualify for the *sui generis* database right regardless of this provision.[575]

4.2.) The rights of users to access, use and share data generated by the use of Internet of Health Things and related services under the Data Act Proposal and their interplay with the GDPR

According to Article 1(1) of the Data Act Proposal, the Regulation aims to lay down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, as well as making data available by data holders to data recipients. It grants users the rights to access, use and share (both personal and non-personal) data generated by the use of an IoT product or related service. These rights are complementary and without prejudice to the existing access and portability rights for data subjects under the GDPR. The Data Act Proposal also aims to contribute to data governance frameworks within the common European data spaces, and to enhancing data sharing outside these data spaces. However, it seems that the objective of the Data Act Proposal to provide horizontally applicable rules for all sectors of the digital economy suffers from deficiencies when applied to the specific context of Internet of Health Things.

In terms of its material scope, Recital 14 of the Data Act Proposal states that the Regulation targets, among other IoT products, "medical and health devices" "that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things)". The distinction between medical and (consumer) health devices would imply that the scope of application extends to all IoHT devices. However, the ambiguous definition of 'product' under Article 2(2) of the Data Act Proposal (and its relation with Recital 15) may lead to uncertainties. The exclusion of items "whose primary function is not the storing and processing of data"

[574] *Ibid*.

[575] *Ibid*.

from the definition of 'product' may have unintended effects, because all IoT devices actually 'process' data within the meaning of Article 4(2) of the GDPR. If the intention is to exclude "products that are primarily designed to display or play content, or to record and transmit content", such as smartphones or cameras, then this may lead to uncertainties about whether certain IoHT devices are covered by the Data Act Proposal, or not. For example, a smart watch may function both as a smart phone and as a wearable device. Another borderline case would be a smart health mirror, which integrates different types of sensors and cameras (which are arguably sensors themselves) as indivisibly linked modules of the device.[576] To exclude these devices would actually result in a weakening of the intended protection.

In delineating the scope of the rights of access, sharing and use of data, the Data Act Proposal does not distinguish between personal data, as defined under Article 4(1) of the GDPR, and non-personal data. However, the Data Act Proposal uses the term 'data' indistinctively to refer to personal and non-personal data, which may lead to confusion. IoHT devices may generate personal and non-personal data simultaneously, but it could often be unfeasible to separate the two types of data. This may require the extension of data protection law to entire raw datasets/databases generated by the use of the device, when otherwise it would not be necessary. In light of this, the Data Act Proposal needs to be analysed more specifically where it provides for rules that exclusively apply to non-personal data, and thereby, may deviate from data protection rules. In the worst case, the interpretation may lead to conflicting obligations that an addressee cannot fulfil at the same time.[577]

It would also be important for the co-legislators to clarify the meaning of "data generated by the use of a product or related service". According to Recital 31 of the Data Act Proposal, the Regulation grants users the rights to access, share and use such data "irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing." By explicitly including 'observed data', the Data Act Proposal (albeit in its Recitals) is clearer than the GDPR. The 'right to data portability' under Article 20(1) of the GDPR is based on "data provided by the data subject", without further elaboration on what this actually implies. The Article 29 Data Protection Working Party interpreted this provision to include personal data

---

[576] *See* Andreu Y, Chiarugi F, Colantonio S *et al*. (2016) Wize Mirror – a smart, multisensory cardio-metabolic risk monitoring system. *Computer Vision and Image Understanding* 148:3–22 at 4. DOI: <https://doi.org/10.1016/j.cviu.2016.03.018>.

[577] Drexl J, Banda C, Otero BG *et al*., *supra* note 571, 105 [para. 291].

that are "observed from the activities of the user", but exclude 'derived data' and 'inferred data', which include personal data that are created by a service provider (for example, algorithmic results).[578] For example, the controller may 'observe' data provided by the data subject by virtue of using an IoHT device, but when it 'derives' or 'infers' data, these data will typically not constitute "data provided by the data subject". Recital 15 of the Data Act Proposal corresponds to this by stating that: "information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation". However, the exclusion of 'derived' and 'inferred' data may jeopardise the effectiveness of the right to access, share and use data in an IoT context.

The Data Act Proposal takes the data subject's act of generating the data as the point of departure for defining the data that shall be the object of the right, but it pays no credit to guaranteeing the effectiveness of the right as regards the attainment of its purpose.[579] One of the shortcomings of this approach is that it does not take into account that data collected by an IoHT is often processed in the device itself by an embedded software that enables the sensor to function in accordance with pre-defined safety, health and quality criteria. This may happen through mere calculation whereby additional information is used ('derived data'), or through data analysis relying on statistical assumptions ('inferred data'). For this reason, instead of a "conduct-based" approach, the Data Act Proposal should adopt a functional "purpose-bound" and "interest-based" approach" to cover also derived and inferred data where this is necessary to enable added-value uses and services.[580] This implies that the rights to access, share and use IoT data under the Data Act Proposal would cover a larger body of personal data than the data portability right under the GDPR, and would rather be in line with the scope of personal data that the data subject has the right to access. As the EDPB clarified, the data subject shall have the right to access all types of personal data concerning him or her under Article 15 of the GDPR, regardless of whether it is 'observed' (or 'raw'), 'inferred' or 'derived' data.[581]

---

[578] Article 29 Data Protection Working Party, Guidelines on the right to data portability (rev. 01) (5 April 2017), 9–10. Available from: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44099>.

[579] Drexl J, Banda C, Otero BG *et al*., *supra* note 571, 10 [para. 23].

[580] *Ibid*., 11 [para. 25], 106 [para. 296].

[581] European Data Protection Board, Guidelines 01/2022 on data subject rights - Right of access (18 January 2022), 31 [para. 96]. Available from: <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf>.

Access to data generated by the use of products or related services may also involve access to information stored on the terminal equipment of a subscriber or user. The EDPB and EDPS recommended that the Data Act Proposal should clarify that the data holder may make these data available to a third party only where there is a valid legal basis under Article 6 of the GDPR (and where relevant, Article 9 of the GDPR and Article 5(3) of the ePrivacy Directive).[582] This protection would be relevant, for example, when the user of an IoHT device prescribed by a healthcare provider (acting as data holder) intends to give access to or requests the data holder to transmit the data that the user has generated by use of the device to a data recipient (e.g. another healthcare provider).

It would also be useful to clarify the notions of 'user' and 'data holder'. The definition of 'user' under Article 2(5) of the Data Act Proposal means "a natural or legal person that owns, rents or leases a product or receives a services". This provision does not require that the person is personally using the product. Conversely, a person who uses the product without having such legal title (e.g. a person who uses an IoHT device purchased by his or her family member) may not enjoy the rights provided by the Data Act Proposal. For this reason, as mentioned, the Regulation should follow an interest-based approach, which means that only a person who has a legitimate interest in data access should be identified as the 'user' of a product. As regards the definition of 'data holder', Article 2(6) of the Data Act Proposal prescribes that the data holder has the 'ability' to make non-personal data available based on the "control of the technical design of the product and related service". However, this may lead to confusion in the case of an Internet of Health Things device, where the device manufacturer typically controls the technical design of the device, but the healthcare provider has the ability and control over what data it makes available.

In connection with this, there is also a need to clarify the concept of 'making available data', because it is not clear whether: (a) this only involves an obligation to grant access to data in the form of "*in situ* accessibility"; (b) the user should also be allowed to copy the data and to port the data; or (c) there is even an obligation for the data holder to transfer the data.[583] As regards the obligation to allow for 'direct accessibility' of the data under Article 3(1) of the Data Act Proposal, Recital 21 seems to limit this obligation to granting *in situ*

---

[582] European Data Protection Board, European Data Protection Supervisor, 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) (4 May 2022), 14 [para. 45]. Available from: <https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf>.

[583] *Ibid*., 26 [para. 65].

accessibility. However, in order to guarantee that users may exercise the rights to access, share and use data effectively, mere *in situ* accessibility may often not be enough. This problem is amplified by the fact that Article 5(1) of the Data Act Proposal does not provide any details on the technical and organisational measures required to make the data available, where applicable, "continuously and in real-time". What is missing is an obligation for the data holder to guarantee interoperability; or alternatively (less ambitiously), an obligation to make available the data in a "structured, commonly used and machine-readable format", which would be in line with the wording of Article 20(1) of the GDPR.[584]

5.) Functional roles and allocation of responsibilities in IoT-enabled telehealth ecosystems

IoT-enabled telehealth systems are often composed of a complex ecosystem of actors that are responsible or subjects of the system and its processing operations. In terms of data-related aspects, there are three possible ways to describe the functional role of the actors in the ecosystem (and the relationship between them): an IoT service-based, a data protection-based or a data governance-based perspective. The first perspective focuses on international technical standards for IoT services, the second on the functional categories in the GDPR, while the third highlights the functional categories set forth by the Data Governance Act[585]. The three perspectives demonstrate that the allocation of responsibilities between actors is challenging in IoT-enabled telehealth systems due to the different conceptualisation of functional roles by various normative instruments. For the success of legal protection against any 'information-induced harms' in this context, it would be essential that the normative

[584] *Ibid*., 108 [para. 301].

[585] *See* Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, 1–44 (henceforth: 'Data Governance Act'). ELI: <https://data.europa.eu/eli/reg/2022/868/oj>.

framework becomes grounded in a better understanding of data and its relationship to people, new technologies and various business models.[586]

5.1.) IoT service-based functional roles

The IoT service-based perspective of IoT-enabled telehealth ecosystems focuses on the functional role of actors in the design, development, connection, operation and use of IoT-enabled telehealth systems. According to this perspective, each actor plays at least one functional role, but there may be overlaps, if one or more actor(s) play multiple roles (e.g. in case the IoHT device manufacturer and the IoT-enabled telehealth application service developer is the same entity). The exact relationship between functional actors depends on the business/service model implemented in the particular case. In general, an IoT-enabled telehealth ecosystem is composed of the following IoT service-based functional roles:[587]

(a) IoHT device manufacturer: responsible for manufacturing and providing an IoHT device that is capable of transmitting raw data and/or content to the application service provider and network provider according to the service logic;

(b) network provider: performs activities relating to the access and integration of resources provided by other providers, the support and control of the IoT capabilities of infrastructure, and the offering of IoT capabilities, including network capabilities and resource exposure to other providers;

(c) platform provider: provides integration capabilities and open interfaces for application service providers, including data storage, data processing and/or device management capabilities, and specific support for different types of applications;

(d) IoT-enabled telehealth service developer: utilises capabilities and resources provided by the IoHT device manufacturer, network provider and platform provider in order to design and develop an IoT-enabled telehealth service for application users, which includes the implementation, testing and integration of services with the platform;

---

[586] *See also* Purtova N (2018) The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* 10(1):40–81 at 80. DOI: <https://doi.org/10.1080/17579961.2018.1452176>.

[587] *See cf.* International Telecommunication Union, *supra* note 79, Appendix I; International Organization for Standardization, International Electrotechnical Commission, *supra* note 121, para. 10.5.

(e) IoT-enabled telehealth application service provider: manages and operates the IoT-enabled telehealth service; and

(f) IoHT device and IoT-enabled telehealth application user: the end-user of an IoT-enabled telehealth service (IoHT device) provided by the IoT-enabled telehealth application service provider.

In addition to these, there may be other (atypical) functional roles and relationships in IoT-enabled telehealth ecosystems. For example, the role of an IoT broker would encompass processing requests from the IoT service requesters in order to determine the set of service providers that will provide or process data, and to distribute the workload tasks among them.[588]

5.2.) Data protection-based functional roles

The increasing number and variety of actors in IoT-enabled telehealth ecosystems suggests that the intensive compliance regime of the GDPR is challenging to ensure in this context. The complex mesh of functional roles requires the proper allocation of legal responsibilities among entities engaged in the processing of personal data in IoT-enabled telehealth ecosystems. According to Article 4(7) of the GDPR, the controller "alone or jointly with others, determines the purposes and means of the processing of personal data".[589] It follows from the definition that the role of a 'controller' relates either to a single processing operation or to a set of operations.[590] However, the definition does not require that the controller actually has access to the processed personal data.[591] Instead, what matters is that the controller should have influence over the processing of personal data by virtue of an exercise

[588] Viswanathan H, Lee EK, Pompili D (2012) Mobile grid computing for data- and patient-centric ubiquitous healthcare. *2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT) (Seoul, 18 June 2012)*, 36–41 at 37. DOI: <https://doi.org/10.1109/ETSIoT.2012.6311263>.

[589] GDPR, *supra* note 313, Article 4(7).

[590] *See Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* (C-40/17), Judgment of the Court (Second Chamber) (29 July 2019), Court Reports – General Court, ECLI:EU:C:2019:629, para. 72. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-40/17>.

[591] *See Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Judgment of the Court (Grand Chamber) (C-210/16) (5 June 2018), Court Reports – Court of Justice, ECLI:EU:C:2018:388, para. 38. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-210/16>.

of decision-making power (based on factual, rather than formal analysis).[592] Determining the purposes and the means amounts to deciding respectively the "why" and the "how" of the processing. In a specific processing operation, the controller is the actor who determines why the processing takes place (i.e. "to what end" or "what for"), and how this objective shall be achieved (i.e. which means shall be employed to attain the objective).[593] The controller is always the responsible actor for making decisions on the purpose of the processing, but as regards the determination of means, a distinction ought to be made between 'essential' and 'non-essential' means.[594] 'Essential means' are closely linked to the purpose and the scope of the processing, and are usually reserved to the controller. These means include, for example, the type of personal data processed; the duration of the processing; the categories of recipients; and the categories of data subjects. By contrast, 'non-essential means' concern the practical aspects of implementation, such as the choice of a particular hardware or software, or the exact security measures, which may be left to a processor to decide on.[595]

The definition of 'controller' and its interpretation may lead to the following allocation of responsibilities between functional actors in IoT-enabled telehealth ecosystems in the following cases:[596]

- When a device manufacturer develops or modifies the operating system of an IoHT device or installs software determining its overall functionality (such as the frequency of data collection, or when and to whom data are transmitted, and for which purpose), then the device manufacturer would qualify as controller.
- When users of quantified self IoHT devices share their data with others via a social network platform (e.g. to foster a form of fitness competition within a group), the social network platform may become a controller in its own right, if it processes these data for distinct purposes that it has determined itself (e.g. it uses the data to infer information about a user's active lifestyle, and displays sports-related ads to the user).

---

[592] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (2 September 2020), paras. 19–20. Available from: <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>.

[593] *Ibid*., para. 33.

[594] *Ibid*., para. 38.

[595] *Ibid*.

[596] *See* Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP 223), *supra* note 478, 11–13 [paras. 3.3.1–3.3.4]; *see also* European Commission Consumers, Health, Agriculture and Food Executive Agency *et al*., *supra* note 542, 36–37.

- Similarly, an IoT data platform that hosts data generated by the use of IoHT devices (e.g. in order to centralise and simplify certain aspects of data management) may also qualify as a controller, if the development of platform services involves the processing of personal data for its own defined purposes.
- When the use of an IoHT device (or one of its advanced features) requires the installation of a third-party application (following the obtainment of the consent of the user), the application developer may become (independent or joint) controller, if it is able to access the personal data of the user of the IoHT device.

In case of joint controllership, joint participation in the determination of purposes and means implies a common decision taken by two or more entities, or a result from converging decisions by two or more entities.[597] However, the use of a common data processing system or infrastructure does not necessarily lead to a joint controllership between entities. This is the case when the processing operations are separable and one party performs certain operations without intervention from the other, or the provider is a processor in the absence of any purpose of its own.[598] For example, the various institutions involved in a health research project consortium may use IoHT devices to collect data from data subjects in their respective environment and "feed" this data into a common AI-enabled data platform hosted by one of the institutions. In this case, the institutions involved in a would qualify as joint controllers for the data processing that is performed on the common platform (because they decided together the purpose and the means of the processing), but each institution would qualify as an independent controller for any other processing performed outside the common platform for their own purposes.[599]

With regard to the development of national eHealth infrastructures in Member States, joint controllership may arise when the public authority of a Member State establishes a health data sharing platform to govern the sharing of electronic health data between healthcare providers within the Member State (and between regions). (The public authority is responsible for the design of the processing and the way the platform is used.) In this case, the plurality of controllers results in an unclear situation that would endanger the protection of the rights of data subjects. Consequently, the public authority establishing the switch point

---

[597] *See* European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, *supra* note 592, 18 [para. 51].

[598] *Ibid*., 20 [para. 66].

[599] *Ibid*., 21 [para. 66].

should act as a joint (or independent) controller.[600] In such scenarios, where there are multiple controllers within the same ecosystem, it is good practice to offer data subjects a single point of contact in order to facilitate the exercise of their rights.[601]

As for the functional role of processors, with reference to Articles 4(8) and 28(1) of the GDPR, there are two basic conditions for an entity to qualify as a 'processor': a) be a separate entity in relation to the controller; and b) process personal data on the controller's behalf.[602] According to Recital 81 of the GDPR: "when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of [the GDPR], including for the security of processing." As it is relevant to IoT-enabled telehealth services, it is noteworthy to mention that although the GDPR does not preclude that the processor offers a preliminary-defined service, in those cases, the controller must make the final decision to actively approve the way the processing is carried out and/or be able to request changes, if necessary.[603] For example, if an IoT-enabled telehealth application provider decides to use a cloud service provider for centralised storage of data generated by IoHT devices, it must also make sure that the cloud service provider, regardless of what it offers in its standardised terms and conditions, respects its specific instructions (on storage periods, retention and deletion of data etc.).

---

[600] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) (16 February 2010), 24. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>; for corresponding issues relating to the EU cross-border electronic health data exchange platform (known as 'MyHealth@EU') *see also* Article 29 Data Protection Working Party, Letter of the Chair of the ART 29 WP to eHEALTH: Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services (11 April 2018), 1–2. Available from: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52057>; European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI) (12 July 2019), 7–9 [paras. 14–18 and footnote 21]. Available from: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_en.pdf>.

[601] Article 29 Data Protection Working Party, Letter of the Chair of the ART 29 WP to mHEALTH: your letter of 7th December 2017 and a new draft code of conduct with the request of a positive opinion from the WP29 under the Data Protection Directive, (11 April 2018), 2. Available from: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52056>.

[602] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, *supra* note 592, para. 74.

[603] *Ibid*., para. 82.

5.3.) Data governance-based functional roles

Due to the absence of institutionalised data governance structures and processes, the health systems of Member States are not leveraging the health-related potentials of sharing data (generated by the use of IoHT devices).[604] In order to increase trust in data sharing, the Data Governance Act regulates and underpins the establishment of mechanisms strengthening the control of data subjects and data holders over data that relates to them.[605] According to an analogical interpretation of Recital 3 of the Data Governance Act, the Data Governance Act would function as *lex generalis* to regulations adopted in the context of the EDHS. However, there might be uncertainties, for example, if the conditions for data re-use under the Data Governance Act would differ from the conditions for secondary use of electronic health data set forth by sectoral legislation.

Despite acknowledging the objectives that it pursues, the EDPB and the EDPS made it clear during the legislative procedure of the Data Governance Act "that the Proposal [...] does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law."[606] In this regard, "the Proposal raises significant inconsistencies with the GDPR" and "in general, the EDPB and the EDPS underline that the Proposal should define the roles in respect of personal data protection law (data controller, processor or joint controller) of each type of 'actor' (data sharing service provider, data altruism organisation, data user)".[607] The Data Governance Act addressed these recommendations only partially, and established entirely new functional categories (which are largely in line with the OECD's use of terminology in relation to the sphere of data governance[608]). From this perspective, the following functional roles exist in the data governance (data sharing mechanisms) of IoT-enabled telehealth ecosystems:

---

[604] *See* Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final – SEC(2020) 405 final – SWD(2020) 296 final, SWD(2020) 295 final (25 November 2020), 19–20. Available from: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71225>.

[605] Data Governance Act, *supra* note 585, Recital 5.

[606] European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (11 March 2021), 7 [para. 19]. Available from: <https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf>.

[607] *Ibid*., 8 [para. 25], 11 [para. 39].

[608] *See also* OECD (2019) *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing, Paris, 34–38. DOI: <https://doi.org/10.1787/276aaca8-en>.

(a) According to Article 2(7) of the Data Governance Act, 'data subject' has the same meaning as the notion of 'data subject' under the GDPR. With regard to the subject matter, the data subject is typically the citizen/patient using an IoHT device.

(b) According to Article 2(8) of the Data Governance Act, "'data holder' means a [...] person who is not a data subject with respect to the specific data in question, which, [...] has the right to grant access to or to share certain personal data or non-personal data". In the public sector, different types of organisations might act as data holders of data concerning health, such as ministries and authorities (responsible for healthcare and social insurance), statistical agencies, or public universities or research institutes.[609] In the present context, they may become data holders, for example, if data generated by the use of IoHT devices are integrated into a patient's EHR. However, as the EDPB and the EDPS pointed out, the problem with the definition of 'data holder' is that: "rather than stating that a legal person has the right to grant access to or share personal data, it would be more appropriate referring to whether and under which conditions a certain processing of personal data can be performed or not."[610] In connection with this, another problem is that the definition of 'data sharing' under Article 2(10) of the Data Governance Act lacks clarity and interplay with the GDPR, because it is unclear what "joint or individual use of [personal] data [...] directly or through an intermediary" may encompass.[611]

(c) According to Article 2(9) of the Data Governance Act, "'data user' means [...] a person who has lawful access to certain personal or non-personal data and has the right, including under [the GDPR] in the case of personal data, to use that data". Data users represent the demand side of the health data ecosystem, and may encompass a diverse range of entities. In the present context, a data user may use raw data collected by IoHT devices in order to generate smart and actionable data. However, the EDPB and the EDPS noted that it is unclear how the notion 'data user' interacts with the notions of 'controller' and 'processor' under the GDPR.[612]

---

[609] European Commission Directorate-General for Communications Networks, Content and Technology, Peijl S, Denny E, Koring E *et al*. (2020) Study to support an impact assessment on enhancing the use of data in Europe. Report on Task 1 – Data governance. Publications Office of the European Union, Luxembourg, 14. DOI: <https://data.europa.eu/doi/10.2759/759296>.

[610] European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Data Governance Act, *supra* note 606, 11 [para. 31 *et seq.*].

[611] *Ibid*., 13 [para. 40].

[612] *Ibid*., 12 [para. 38].

(d) According to Article 2(11) of the Data Governance Act, "'data intermediation service' means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other [...]". Recital 27 of the Data Governance Act adds that "[d]ata intermediation services could include bilateral or multilateral sharing of data or the creation of platforms or databases enabling the sharing or joint use of data, as well as the establishment of specific infrastructure for the interconnection of data subjects and data holders with data users." Theoretically, data intermediation services may consist of a variety of actors in healthcare, such as data repositories, (federated networks of) data trusts, data cooperatives, personal information management systems or personal data stores (PIMS/PDS), or trusted third parties.[613] In the present case, data intermediaries may foster connections between the demand side and the supply side of health data markets in relation to secondary use of data generated by IoHT devices.[614] However, as the concept of 'data intermediation service' in the Data Governance Act is restricted to commercialised data sharing relationships, it has limited relevance to the subject matter (e.g. if a data subject monetises their data concerning health, or a data holder sells their synthetic health datasets via a data intermediation service).

(e) Finally, under the Data Governance Act, data subjects may provide consent to voluntarily share their data concerning health with recognised data altruism organisations.[615] For example, data subjects may voluntarily share data generated by their use of IoHT devices with a data altruism organisation in order to enable researchers to monitor and make early detections of possible epidemic hotspots.[616]

---

[613] *See also* OECD, *supra* note 608, 36–38; Centre for Data Ethics and Innovation (2021): *Unlocking the value of data: Exploring the role of data intermediaries. An exploration of the role intermediaries could play in supporting responsible data sharing*. Centre for Data Ethics and Innovation, London (22 July 2021), 9. Available from <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf>.

[614] *See also* DigitalHealthEurope, Kolitsi Z, Kalra D, Wilson P *et al*. (2021) *DigitalHealthEurope recommendations on the European Health Data Space. Supporting responsible health data sharing and use through governance, policy and practice*. DigitalHealthEurope, 5, 7. Available from <https://digitalhealtheurope.eu/wp-content/uploads/DHE_recommendations_on_EHDS_July_2021.pdf>.

[615] Data Governance Act, *supra* note 585, Article 2(16) and Article 18; *see also* Shabani M (2021) The Data Governance Act and the EU's move towards facilitating data sharing. *Molecular Systems Biology* 17(3):e10229 at 2. DOI: <https://doi.org/10.15252/msb.202110229>.

[616] *See* Robert Koch-Institut (n.d.) *Corona Datenspende*. Robert Koch-Institut. Available from <https://corona-datenspende.de>.

CHAPTER 4:
DATA PROTECTION ROLES IN TELECONSULTATION

1.) Case study: problem description

Teleconsultations (online doctor visits) enable the provision of healthcare (telemedicine) via a telecommunications channel (video conferencing application) established between a patient and a healthcare provider (health professional).[617] The particular benefits of teleconsultation among telehealth services is that it can facilitate access to healthcare through direct audiovisual connection between patients and health professionals. Teleconsultations can provide continuous, flexible and more comfortable care for patients, reduce waiting times, save costs and strengthen patient–doctor relationships. Of course, it is important to point out that teleconsultations cannot replace human-physical contact that is essential in many medical cases, and may not provide the same quality of care. Nevertheless, it can serve as a force multiplier for healthcare systems.

Considering that the provision of teleconsultation services requires resource-intensive IT infrastructure and complex software architecture, many healthcare providers opt to use teleconsultation services offered by healthcare platforms. As part of their cloud computing services, these platforms offer a teleconsultation functionality to their users (patients and healthcare providers). However, this functionality relies on the integration of a video communications API service provided by a separate entity. This makes the identification of data protection functional roles and allocation of responsibilities between parties involved in the teleconsultation challenging. Against this background, this chapter examines the privacy and data protection aspects of a teleconsultation service offered by healthcare platforms to their users via an integrated video communications API service.

The analysis builds on empirical evidence collected from the following cases:[618]

(a) when users (patients and healthcare providers) conduct teleconsultation by using the online doctor marketplace and related healthcare SaaS functionalities of Healthcare Platform "**A**", which has integrated the video communications API service of Video API Provider "**X**"; and

[617] Sometimes the term 'teleconsultation' also refers to the use of ICT tools for remote consultations between health professionals. However, in this chapter, the meaning of 'teleconsultation' is restricted to the use of video conferencing applications between patients and health professionals.

[618] The analysis has altered company names and modified/simplified real-world facts encountered in the course of an industrial PhD collaboration.

(b) when users (patients and healthcare providers) conduct teleconsultation by using the healthcare SaaS functionalities of Healthcare Platform "**B**", which has integrated the video communications API service of Video API Provider "**Y**".

2.) Technical background information

2.1.) Teleconsultation on Healthcare Platform "A" by using the video API service of Video API Provider "X"

Video communications API functions of Video API Provider "X"

Video API Provider "**X**" offers a variety of communication-enabling services, which include its APIs (application programming interfaces), SDKs (software development kits), software, code snippets, documentation, technical support, the website, as well as the features, functionalities and connectivity provided through its proprietary platform. The video API platform of Video API Provider "**X**" enables the developer (in the present case: Healthcare Platform "**A**") to embed real-time face-to-face video calls, messaging, screen-sharing and other services into its website or mobile app. The video API platform includes client libraries for web, iOS, Android, Windows and Linux, as well as server-side SDKs and a REST (representational state transfer) API. The video API platform uses WebRTC (Web Real-Time Communication protocols) for audio-video communications. All applications built in integration with the video API platform require two primary components:

- The client — client-side code that runs in a browser or mobile app, and that is set up by the developer using the video API platform's client-side libraries (which are available for Web, iOS, Android, Windows and Linux). The client-side handles most functionalities of the video API platform.
- The server — server-side code executed on a web server that is set up by the developer using the video API platform's server SDKs (which are available for Node, PHP, Java, .NET, Python and Ruby).

Video chat sessions of Video API Provider "X"

Every video chat via the video API platform of Video API Provider "**X**" takes place within a session. A session is a "virtual room" where clients (i.e. any browser or mobile app utilising client-side code from the video API platform's client SDKs) can interact with each other in real-time. Each session is associated with a unique session ID. Multiple clients can chat with each other by connecting to the same session (using the same session ID). Sessions are hosted in the cloud of Video API Provider "**X**", which manages:

- client connections (via a persistent event or signalling connection using WebSockets to constantly listen for new events dispatched by the session);
- audio-video streams (i.e. audio-video signals, which include a client's published camera and microphone feed);
- user events (e.g. a new client connecting or disconnecting); and
- other issues that are not handled by the client SDKs or server SDKs.

The app server, which is set up by the app developer (Healthcare Platform "**A**") using the server SDKs of the Video API Provider "**X**", executes the server-side code and is responsible for creating new sessions and generating unique authentication tokens ("keys") in order to allow each client to join a session. (Tokens have expiration dates specified by the server, whereas sessions never expire.) Tokens can be assigned roles—publisher, subscriber, or moderator—, which determine the permissions of the client, such as to publish an audio-video stream to the session using the device's webcam and microphone, or to subscribe to any audio-video streams published by other clients in the session.

In outline, when a health professional (User A) initiates a teleconsultation (video chat session) with a patient (User B) using the browser or mobile app of Healthcare Platform "**A**", which integrates the video communications API of Video API Provider "**X**", the following steps take place:

1. The app server of Healthcare Platform "**A**", using code from the video API server SDK of Video API Provider "**X**", requests the video API cloud of Video API Provider "**X**", through its video REST API, to create a session (virtual room). The video API cloud of Video API Provider "**X**" creates the session and returns the session ID to the app server of Healthcare Platform "**A**". At this point, the session is unoccupied.
2. When User #1 loads the client-side application of Healthcare Platform "**A**", which was built with the video API client SDK provided by Video API Provider "**X**", Client

#1 (i.e. the web page or mobile app of Healthcare Platform "A" that User #1 is using) receives session info from the app server. This includes a unique authentication token (the client's "key") created by the app server of Healthcare Platform "**A**".

3. Client #1 uses the session ID and token to establish a connection with the session. Client #1 can then publish an audio-video stream to the session and listen for important events (such as whether the other user joins the session). At this point, Client #1 is the only participant in the session.
4. When User #2 loads the client-side application in a separate web page or mobile device (Client #2), Client #2 receives the session ID and a unique token from the app server of Healthcare Platform "**A**". Client #2 uses that info to establish a connection to the session.
5. Once Client #2 is connected to the session, Client #2 can subscribe to Client #2's stream. Client #2 then publishes its own video stream to the session, and Client #1 subscribes to it. From this point, both clients are subscribed to each other's stream in a one-to-one video chat, and are both "listening" for new events.

2.2.) Teleconsultation on Healthcare Platform "B" by using the video API service of Video API Provider "Y"

Video communications API functions of Video API Provider "X"

Video API Provider "**Y**" offers a customer engagement platform to power personalised interactions and connection with users through a variety of communication-enabling services. Video API Provider "**Y**" provides a programmable real-time communications platform that allows the developer (in the present case: Healthcare Platform "**B**") to add a video chat functionality to its web, iOS and Android applications. Video API Provider "**Y**" provides APIs, SDKs and helper tools to capture, distribute, record and render audio and video applications. The video API is built on top of WebRTC, and uses the REST APIs and client-side SDKs of Video API Provider "**Y**". The video API also provides global STUN/TURN relays, media services for large-scale group conferences and recording, and signalling infrastructure, so that developers can build scalable applications.

The programmable aspect of the video API allows the developer to have full control over how video appears in its application. The video API provides signalling, user access management, media processing and media delivery to enable real-time communications. Media exchange (i.e. the sharing of audio, video and other data with video participants) takes place either directly, peer-to-peer or through the servers of Video API Provider "**Y**", depending on the type of video room the developer chooses to use. Signalling is managed in the global infrastructure of Video API Provider "**Y**", and is the process of discovery and negotiation to set up, control and end a WebRTC session.

All applications built with the video API of Video API Provider "**Y**" require both a frontend and a backend component:

- The frontend is the mobile client or web browser client application that users will interact with and that connects to the cloud of Video API Provider "**Y**". Video API Provider "**Y**" provides SDKs for JavaScript, iOS and Android.
- The backend is the application server that is required to generate access tokens for participants. The developer can also use an application server to interact with the APIs of Video API Provider "**Y**" in order to create and manage video room settings or recordings.

Video chat sessions of Video API Provider "X"

A room represents a virtual space where end-users can communicate by use of the video API of Video API Provider "**Y**". Technically, a room is a computing resource that provides the following services to client applications through a set of APIs:

- Session service: end-users can connect and disconnect from rooms (when an end-user connects, it becomes a room participant); and
- RTC (Real-Time Communication) service: participants can communicate audio, video and other data using WebRTC. RTC services are typically architected in two layers:
    - Signalling layer, which deals with the control information. The communicating entities typically exchange signalling messages to agree on what is communicated (e.g. audio, video), and how to communicate (e.g. codecs, formats). In the case of Video API Provider "**Y**", signalling always takes place between clients and its cloud, which orchestrates the communication.

- Media layer, which deals with the audiovisual information itself. Media packets typically transport encoded and encrypted audio and video bits. In the case of Video API Provider "**Y**", media are mediated by the video API platform, but can also be exchanged directly among clients, depending on the type of video room.

The video rooms provided courtesy of Video API Provider "**Y**" are based on a publish/subscribe model. This means that a participant can publish media tracks to the room. The other participant(s) can then subscribe to these tracks to start receiving the media information. Depending on the type of room chosen, there are two different ways media can be exchanged in a video room:

- Peer-to-peer (P2P): participants in P2P rooms exchange media directly. In this case, the infrastructure of Video API Provider "**Y**" acts as the signalling server, which makes it possible for participants to discover each other and negotiate the communications (i.e. transmission of audio and video data), in agreement with the application and SDK requirements. (The only exception is when media exchange requires TURN [Traversal Using Relays around Network address translation]. In that case, a TURN server blindly relays the encrypted media bits to guarantee connectivity. As a matter of note, the TURN server cannot decrypt or manipulate the media.) As Video API Provider "**Y**" does not intercept the media in P2P rooms, it is not possible to record or transcode the media or make it interoperate with other RTC services.
- Group: in group rooms, a participant exchanges media with the cloud of Video API Provider "**Y**", which acts as a Selective Forwarding Unit (SFU). Group rooms can have up to 50 concurrent participants and allow additional functionalities.

In terms of the security of P2P rooms, the private key is exchanged directly with the remote peer (end-to-end encryption). As regards the security of group rooms, each participant has their own private key exchanged with the media server using the DTLS 1.2/SRTP communication protocols in the transport layer. All media published to or subscribed from the room is transported through this secure connection. The encryption key exchange uses a technique known as Perfect Forward Secrecy (PFS).

In outline, when a health professional (User A) initiates a teleconsultation (video room session) with a patient (User B) using the browser or mobile app of Healthcare

Platform "**B**", which integrates the video communications API of Video API Provider "**Y**", the following steps take place:

1. Creation of a video room:
    1.1. The app server of Healthcare Platform "**B**" requests Video API Provider "**Y**" to create a room using the REST API.
    1.2. Video API Provider "**Y**" validates the provided API credentials and creates the room. Video API Provider "**Y**" keeps track of the room state until it is completed.
    1.3. Video API Provider "**Y**" returns the room information to the application of Healthcare Platform "**B**". This includes a unique room identifier, which can be used in subsequent API requests to refer to this room. At this point, the room is still empty.
2. Client #1 (i.e. the web page or mobile app of Healthcare Platform "**B**" that the health professional is using) receives an access token to connect to the room (in order to ensure that the application of Healthcare Platform "**B**" has full control of who is authorised to join the room):
    2.1. Client #1 requests an access token from the application server of Healthcare Platform "**B**". This is typically accomplished by sending an HTTP request from the client application.
    2.2. The application server of Healthcare Platform "**B**" uses the customer account credentials of Healthcare Platform "**B**" at Video API Provider "**Y**" to generate a cryptographically secure access token using the helper libraries of Video API Provider "**Y**". Access tokens (as JSON Web Tokens) are short-term credentials that are signed with a Twilio API Key Secret and contain grants which govern the actions that the client holding the token is permitted to perform. All access tokens of Video API Provider "**Y**" include the following information:
        - a Video API Provider "**Y**" account SID (public identifier of the Video API Provider "**Y**" account associated with the access token);
        - an API Key SID (public identifier of the key used to sign the token);
        - an identity grant (which sets the Video API Provider "**Y**" user identifier for the client holding the token); and
        - the API Key Secret (associated with the API Key SID used to sign the access token and verify that it is associated with the Twilio account).

2.3. The access token is returned to Client #1.

3. Client #1 connects to the room:

   3.1. Client #1 connects to the room using the SDK connect interface of Video API Provider "**Y**", and authenticates with the access token that was fetched.

   3.2. Video API Provider "**Y**" checks the access token. If it is valid, a signalling connection is established between the client and the room. At this point, the client becomes a participant in the room and can publish and/or subscribe to media tracks from other participants.

4. Client #2 (i.e. the web page or mobile app of Healthcare Platform "**B**" that the patient is using) may connect to the room to become a participant by obtaining an access token from the application server of Healthcare Platform "**B**".

5. Publication of and subscription to media tracks:

   5.1. A room participant can publish audio, video and data tracks to the room.

   5.2. The rest of the room participants are notified of this track publication and can subscribe to it.

6. A third-party (e.g. a family member, an interpreter) can be added (optionally) by:

   6.1. creating a new access token through WebRTC in order to make them a regular participant; or

   6.2. dialing them (making a traditional phone call) with the programmable voice API of Video API Provider "**Y**".

3.) Data protection impact assessment (DPIA) for teleconsultation

The Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (endorsed by the EDPB) clarified the relevant provisions of the GDPR in order to provide legal certainty on when and how to carry out a

DPIA.[619] According to the Guidelines, a DPIA is a process designed to describe the processing of personal data, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing by assessing them, and by determining the measures to address them. DPIAs are important tools for accountability as they support controllers not only to comply with requirements of the GDPR, but also to demonstrate that they have taken appropriate measures to ensure compliance. The following sections discuss the rationale as to why a DPIA is required for processing in the context of teleconsultation.

3.1.) Is teleconsultation subject to a DPIA?

According to Article 35(1) of the GDPR, carrying out a DPIA is only mandatory "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons". As the GDPR does not provide an exhaustive list of "high risk" processing operations, the Article 29 Data Protection Working Party, in its above-mentioned Guidelines, spelled out nine criteria which should be considered when assessing whether a concrete set of processing operations require a DPIA. The Article 29 Data Protection Working Party considered that the more of these criteria are relevant to the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. In any case, a processing that satisfies at least two of these criteria would require the controller to carry out a DPIA. This requirement is regardless of safeguards and measures that the controller envisages to implement. In teleconsultation, processing of personal data concerns four of these nine established criteria, namely: (i) sensitive data or data of a highly personal nature; (ii) data concerning vulnerable data subjects; (iii) innovative use or application of new technological or organisational solutions; and (iv) systematic monitoring. Consequently, processing of personal data in teleconsultation is subject to a DPIA.

[619] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (4 April 2017 as last revised and adopted 4 October 2017). Available from: <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711>.

3.2.) Should a DPIA address teleconsultation as a single processing operation or a set of similar processing operations?

Teleconsultation involves multiple processing operations (enumerated under Article 4(2) of the GDPR), which are performed on personal data or on sets of personal data. Article 35(1) of the GDPR sets forth that a "single assessment may address a set of similar processing operations that present similar high risks." In other words, a single DPIA can be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose and risks. The Article 29 Data Protection Working Party has added that a DPIA can also be useful for assessing the data protection impact of a technology product, where this is likely to be used by different controllers to carry out similar or different processing operations. In such cases, the controllers should share or make publicly accessible a reference DPIA, implement the measures described in the DPIA, and provide a justification for conducting a single DPIA. Consequently, (joint or independently collaborating) controllers processing personal data in teleconsultation may carry out one DPIA for all related processing operations.

3.3.) When and who must carry out a DPIA relating to teleconsultation?

The controller should carry out a DPIA prior to the processing, which is consistent with the principle of data protection by design and by default. However, the DPIA is an on-going process, which the controller must update throughout the lifecycle of the processing. Although the controller might have other DPIAs in place, a DPIA is required for processing operations which, in particular, involve using new technologies, or are of a new kind and where no DPIA has been carried out before by the controller, or where they become necessary in light of the time that has elapsed since the initial processing. Therefore, if teleconsultation is a new service offered by the controller, it must carry out a DPIA for related processing operations ex-ante.

With regard to Article 35(1) of the GDPR, the controller is responsible for carrying out the DPIA. According to Article 35(2), the controller shall seek the advice of the data protection officer, where designated. The controller must document this advice and the decisions taken within the DPIA. The DPO must monitor the performance of the DPIA. If

the processing is wholly or partly performed by a processor (as is the case with certain processing operations in teleconsultation), the processor must assist the controller in carrying out the DPIA and provide any necessary information (in line with Article 28(3)(f) of the GDPR). Furthermore, it is good practice to define and document other specific roles and responsibilities according to internal policies. Where appropriate, the controller should seek advice from independent experts of different professions (e.g. lawyers, IT experts, security experts, etc.). The Chief Information Security Officer (CISO), if appointed, and/or the IT department, should assist the controller. According to Article 35(9) of the GDPR, the controller must also seek the views of data subjects or their representatives, where appropriate. The Article 29 Data Protection Working Party stated that those views could be sought through a variety of means (e.g. survey sent to end users of the teleconsultation service), depending on the context, and ensuring that the controller has a separate lawful basis for processing any personal data involved in seeking such views.

3.4.) What is the methodology for carrying out a DPIA in relation to teleconsultation?

Article 35(7), together with Recitals 84 and 90 of the GDPR set out the minimum features and elements of a DPIA. The requirements outlined in the GDPR provide a broad, generic and customisable framework for designing and carrying out a DPIA. Consequently, it is up to the controller to choose an appropriate methodology. However, this methodology must be compliant with the criteria established in Annex 2 of the Article 29 Data Protection Working Party's above-mentioned Guidelines. In risk management terms, a DPIA aims at “managing risks” to the rights and freedoms of natural persons by establishing the context, assessing the risks, and treating those risks. The DPIA should be regarded as a tool for managing risks to the rights of the data subjects (and not to the organisation), and therefore the DPIA should assess the possible impacts from their perspectives.

3.5.) Is there an obligation to publish a DPIA relating to teleconsultation?

The GDPR does not require the publication of a DPIA; it is the controller's decision to do so. However, the Article 29 Data Protection Working Party recommended that controllers should consider publishing at least parts, such as a summary of the DPIA's main findings. When the DPIA would present specific information relating to security risks for the controller or give away commercially sensitive information, it is sufficient to publish a statement that the controller carried out a DPIA. Ultimately, the purpose of carrying out a DPIA relating to teleconsultation should be to foster trust in the controller's service and processing operations, and demonstrate accountability and transparency.

3.6.) Does the controller have to consult the supervisory authority about a DPIA relating to teleconsultation?

With regard to Article 36(1) of the GDPR, the controller must consult the supervisory authority prior to processing, if the DPIA indicates that the processing would result in high risk in the absence of measures taken by the controller to mitigate the risk. In other words, whenever the controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high). From the perspective of healthcare platforms, when they are acting as controllers, they must assess the risks on a case-by-case basis taking into account the technical, organisational and security practices implemented by the video communications API service providers and their sub-processors.

4.) Description of processing operations in teleconsultation

4.1.) Legal basis and purposes of processing

In the teleconsultation use cases described above, processing consists of two sets of operations (and related purposes):

- processing of personal data relating to the technical arrangement (and intrinsically linked service aspects) of a teleconsultation, in particular:
    - processing of personal data that relates to the relationship of the healthcare platform (Healthcare Platform "**A**" or Healthcare Platform "**B**"), as a customer, with the video communications API service provider (Video API Provider "**X**" or Video API Provider "**Y**") ("customer account data"); and
    - processing of personal data used to identify the source and destination of a video call between the customer's end users (in the present case: patients and health professionals) ("customer usage data"); and
- processing of personal data during the teleconsultation (face-to-face communication), when the healthcare provider delivers healthcare service to the patient ("customer content").

This distinction between the arrangement of a teleconsultation and the actual content of the online doctor visit actually mirrors the "in-person" scenario of when a patient books an appointment on a healthcare platform to arrange an in-person visit to a healthcare provider. In the latter case, the processing of personal data relating to the arrangement of a doctor's visit to the healthcare provider is under the influence of the healthcare platform. Therefore, it is a controller in that processing operation. Afterwards, when the healthcare provider provides in-person medical service to the patient at its clinic, the processing of the patient's personal data becomes subject to a different processing activity, determined by a different entity, the healthcare provider, rather than the healthcare platform. In this processing phase, the healthcare platform is a processor acting on behalf of the healthcare provider. In summary, the only difference between teleconsultation and the "in-person" scenario is that, in the former case, the processing of personal data relating to the provision of medical service takes place online, not in person. The processing of personal data relating to the arrangement of a doctor's visit, whether in person or online, is managed in both cases by the healthcare platform as part of its services.

4.2.) Types of personal data

In the two teleconsultation use cases described above, the types of personal data processed are similar with slight differences. When end users (patients and healthcare providers) use

the teleconsultation service provided by Healthcare Platform "**A**" (customer), which has integrated the video communications API service of Video API Provider "**X**", the following types of personal data are processed:

- Customer account data, which encompasses:
    - personal data relating to the relationship of Healthcare Platform "**A**" with Video API Provider "**X**", including the names, phone numbers and/or contact information of individuals authorised by Healthcare Platform "**A**" to access their account at Video API Provider "**X**" and/or use the services and billing information; and
    - personal data processed by Video API Provider "**X**" for the purposes of storing, transmitting or exchanging customer content, sending goods, and to provide the services, that may include shipping address, data used to trace and identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the services, and the date, time, duration and type of communication, and/or data provided by the channels used by the customer to communicate with its users.
- Customer content, which encompasses:
    - personal data exchanged by use of the services provided by Video API Provider "**X**", such as text, call recording, message bodies, conversation transcriptions, voicemail recordings, voicemail transcription, video recording, video files, images and sound.

On the other hand, when end users (patients and healthcare providers) use the teleconsultation service provided by Healthcare Platform "**B**" (customer), which has integrated the video communications API service of Video API Provider "**Y**", the following types of personal data are processed:

- Customer account data, which encompasses:
    - personal data relating to the relationship of Healthcare Platform "**B**" with Video API Provider "**Y**", including the names or contact information of individuals authorised by Healthcare Platform "**B**" to access its account at Video API Provider "**Y**", and billing information of individuals that Healthcare Platform "**B**" has associated with its account, as well as any data Video API Provider "**Y**" may need to collect for the purpose of identity

verification (including providing MFA (Multi-Factor Authentication) services), or as part of its legal obligation to retain subscriber records.

- Customer usage data, which encompasses:
    - data processed by Video API Provider "**Y**" for the purposes of transmitting or exchanging customer content utilising phone numbers either through the Public Switched Telephone Network (PSTN) or by way of other communication networks, including data used to identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the services of Video API Provider "**Y**", and the date, time, duration and the type of communication, as well as activity logs used to identify the source of service requests, optimise and maintain performance of the services, and investigate and prevent system abuse.
- Customer content, which encompasses:
    - personal data exchanged as a result of using the services of Video API Provider "**Y**", such as text message bodies, voice and video media, images, email bodies, email recipients, sound, and, where applicable, details that Healthcare Platform "**B**" submits to the services from its designated software applications and services, as well as data stored on behalf of Healthcare Platform "**B**", such as communication logs within the services or marketing campaign data that Healthcare Platform "**B**" has uploaded to the services of Video API Provider "**Y**".

4.3.) Types of data subjects

When end users (patients and healthcare providers) use the teleconsultation service provided by Healthcare Platform "**A**" (customer), which has integrated the video communications API service of Video API Provider "**X**", the processing affects the following data subjects:

- Customer content may concern the following categories of data subjects:
    - customer's authorised users, who are those individuals that are authorised by the customer to use the services of Video API Provider "**X**" on behalf of the customer; and

    - customer's customers and end users (i.e. healthcare providers and patients)
- Customer account data may concern the following categories of data subjects:
    - customer's employees and agents;
    - customer's authorised users; and
    - customer's customers and end users (i.e. healthcare providers and patients)

On the other hand, when end users (patients and healthcare providers) use the teleconsultation service provided by Healthcare Platform "**B**" (customer), which has integrated the video communications API service of Video API Provider "**Y**", the processing affects the following data subjects:

- Customer content may concern the following categories of data subjects:
    - customer's end users (i.e. healthcare providers and patients).
- Customer account data may concern the following categories of data subjects:
    - customer's employees and individuals authorised by customer to access customer's account at Video API Provider "**Y**" or make use of the MFA services or telephone number assignments received from Video API Provider "**Y**".
- Customer usage data may concern the following categories of data subjects:
    - customer's end users (i.e. healthcare providers and patients).

4.4.) Sources of personal data: end users

4.4.1.) Patients

In the context of teleconsultation, the patient is a natural person who seeks to receive or receives healthcare using information and communication technologies, in a situation where the health professional and the patient are not in the same location. Before, during and after the teleconsultation, information relating to an identified or identifiable patient (as the data subject) are processed. As mentioned, this may involve processing of personal data in the course of the provision of teleconsultation (e.g. collection of patient's data concerning health for the purpose of medical diagnosis and creation/updating of patient's electronic health

record), but also in relation to thereof (e.g. management of patient's personal information for the purpose of booking a teleconsultation appointment).

Special scenarios may emerge when multiple parties participate in a teleconsultation on the patient's side. This may be the case when, for example, a family member, a guardian, a translator, or other person whom the patient trusts, joins the teleconsultation. They may connect to the virtual room by using the same client as the patient, or by using a different (third) client. However, the latter arrangement is only possible in group rooms (not in P2P rooms). Similarly, a group therapy with multiple patients can also only be performed in group rooms. There is also the possibility that a person unintentionally appears in a teleconsultation (e.g. an identifiable person positioned behind the patient in a video call). Although these people may not fit into any of the functional notions provided by the GDPR (e.g. 'data subject', 'third party', 'recipient'), the controller must nevertheless assess the risks to the rights and freedoms of these persons, and implement appropriate measures to protect their privacy and personal data (e.g. by providing a functionality that enables the blurring of the background).

4.4.2.) Healthcare providers

According to Article 3(g) of the 'Directive 2011/24/EU on the application of patients' rights in cross-border healthcare'[620], "'healthcare provider' means any natural or legal person or any other entity legally providing healthcare". Although the healthcare provider is the entity that determines the purposes and means of the processing (during the online doctor's visit), in practice, the teleconsultation (as a video call) is launched and conducted by a health professional. Under Article 3(f) of Directive 2011/24/EU, a 'health professional' encompasses a variety of professions of distinct nature. The health professional may work either as a sole practitioner, or on behalf (with or for) a clinic. In the first case, the health professional is the healthcare provider, and thus, the controller. However, in the second case, it is the organisation (the clinic) as such, and not the individual (the health professional) within the organisation, that acts as the controller within the meaning of the GDPR. As a jurisdictional rule, Article 3(d) of Directive 2011/24/EU clarifies that in the case of

[620] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, *see supra* note 554.

telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established.

It is important to point out that the rights and freedoms of the health professional as an individual need to be respected. It is not only patients, who have a reasonable expectation of privacy in teleconsultation, but health professionals have as well. For this reason, it is debatable whether the recordings of teleconsultation should be prohibited, or permitted, and if so, under what conditions. The argument in favour is that if it were made consensually, teleconsultation recordings could benefit both patients and health professionals. For example, a teleconsultation recording could enable the health professional (or another health professional) to re-evaluate an online medical examination ex-post. On the other hand, it could help the patient to remember important advice or complex information; allow more time to process information; or share the doctor's guidance with family members. This would amount to processing for "purely personal reasons", which falls under the exemption of Article 2(2)(c) of the GDPR.

The privacy policies of leading online doctor marketplaces in Europe suggest that the general industrial practice is to prohibit the recording of teleconsultations. For instance, the Teleconsultation Notice of Healthcare Platform "**A**" prohibits patients from recording teleconsultations or distributing any material related to them. (However, there is no mention of whether health professionals may record teleconsultations, or not.) By comparison, one competitor's General Terms and Conditions for Users (Patients) sets forth that neither patient, nor the practitioner is allowed to record, copy or broadcast any content or extracts of content in connection with the teleconsultation, regardless of the means, medium, process or purpose. Any infringement of the right to image, respect for privacy or professional and medical confidentiality may be subject to sanctions, including criminal sanctions. They also clarify that at no moment can a third party, the staff of the healthcare platform or their service providers see or record any of the teleconsultation's contents. Another competitor's Conditions of the Use of Services also prohibits the recording of the teleconsultation, but permits the user to take a screenshot of the teleconsultation, if necessary and for the sole purpose of establishing a diagnosis or completing the patient's medical record.

5.) The data protection role of healthcare platforms in teleconsultation

In order to allocate data protection responsibilities among parties involved in teleconsultation, it is first necessary to clarify their functional roles. The functional role of a party does not stem simply from a formal designation of it being either a "controller" or "processor", or the nature of the entity that is processing personal data, but from its actual activities and the relationship between the parties in a specific context. For example, the same entity may act as controller for certain processing operations and as processor for others, and thus, the qualification as a controller or a processor has to be assessed with regard to each specific data processing activity. The focus of this analysis is on the data protection role of the healthcare platforms in relation to healthcare providers and video communications API services providers. The healthcare platforms play a central role in this context, because they not only connect patients with doctors, but they also integrate video communications API services into the services provided by the platforms.

In the present scenarios described above, the qualification of the healthcare platforms (Healthcare Platform "**A**" and Healthcare Platform "**B**") as a controller / processor must be established on the basis of an assessment of the factual circumstances surrounding the processing of personal data in teleconsultation. Accordingly, the following this assessment seeks to analyse in which processing operations do healthcare platforms act as (individual or joint) controllers? With reference to Article 4(7) of the GDPR, 'controller' means any entity "which, alone or jointly with others, determines the purposes and means of the processing of personal data". This definition contains five elements, which must be assessed separately, taking into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR,[621] in order to determine whether the respective healthcare platform is a controller.

[621] *See* European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, *supra* note 592.

5.1.) Assessment of controllership (I.): "the natural or legal person, public authority, agency or other body"

The entities in question are the healthcare platforms (Healthcare Platform "**A**" and Healthcare Platform "**B**") as legal persons. Concerning that both platforms belong to a larger company group, it is important to clarify whether there is any instance of processing on behalf of other group entities, or whether the parent company exercises influence over the decision-making. In the case of Healthcare Platform "**A**", the Privacy Policy states that Healthcare Platform "**A**" always takes the strategic decisions regarding the purposes and means of the processing of the personal data of patients, but another group entity also plays an important role in the decision-making process relating to the processing of the personal data of health professionals. These group entities are joint controllers of the personal data of patients and health professionals (users) registered on the platform. In the case of Healthcare Platform "**B**", the Privacy Policy states that another group entity jointly decides the purposes and methods of processing relating to the service package of Healthcare Platform "**B**" that includes the teleconsultation functionality.

5.2.) Assessment of controllership (II.): "determines"

The second element of the definition refers to the assessment of whether the respective healthcare platform (Healthcare Platform "**A**" or Healthcare Platform "**B**") influences control over the processing by virtue of exercising decision-making power about the key elements of the processing. In the present cases, in the absence of control arising from any legal provision, all relevant factual circumstances must be taken into account in order to reach a conclusion as to whether the respective healthcare platform exercises a determinative influence over processing of personal data in certain phases (processing operations) of the teleconsultation. An assessment of the exact contractual terms and relationships between the different parties involved can facilitate the determination of which party (or parties) is acting as the controller. Normally, a controller–processor agreement establishes who the determining party (controller) and the instructed party (processor) are. However, as the EDPB Guidelines 07/2020 explains, the terms of a contract are not decisive in all circumstances. In line with the factual approach, the word "determines" means that the

entity, which actually exerts influence on the purposes and means of the processing, is the controller. This means that even if the processor offers a service that is preliminarily defined in a specific way, the processor must present the controller with a detailed description of the service in order to make the final decision to actively approve the way the processing is carried out and to be able to request changes, if necessary. The processor cannot at a later stage change the essential elements of the processing without the approval of the controller.

In terms of the data protection relationships between the healthcare platforms and the video communications API service providers, the following assessments can be made. The Data Processing Addendum of Video API Provider "**X**" is one of the additional terms and policies incorporated into the Master Services Agreement concluded between Video API Provider "**X**" and Healthcare Platform "**A**" and other group entities (as the "customer"). According to the Data Processing Addendum of Video API Provider "**X**", the parties agree that with regard to the processing of customer content, the Healthcare Platform "**A**" may act either as a controller or processor and Video API Provider "**X**" acts as a processor (where Healthcare Platform "**A**" is a controller) or sub-processor (where Healthcare Platform "**A**" is a processor). For the purpose of improving and enhancing the services, Video API Provider "**X**" acts as an independent controller (and the Healthcare Platform "**A**" is a controller). The Data Processing Addendum of Video API Provider "**X**" makes it clear that Video API Provider "**X**" processes customer content as a processor for the performance of the services in accordance with the instructions of Healthcare Platform "**A**" set forth in the Master Services Agreement and the Data Processing Addendum. In addition to this, the parties acknowledge that, with regard to the processing of customer account data, Healthcare Platform "**A**" is a controller and Video API Provider "**X**" is an independent controller, not a joint controller with Healthcare Platform "**A**". In summary, the Data Processing Addendum of Video API Provider "**X**" differentiates between processing of personal data relating to the arrangement of a teleconsultation and the content of the teleconsultation.

The contractual terms between Healthcare Platform "**B**" and Video API Provider "**Y**" are phrased similarly in the Data Protection Addendum of Video API Provider "**Y**", which is part of the Master Sales Agreement concluded between Video API Provider "**Y**" and Healthcare Platform "**B**" and other group entities (as the "customer"). The parties agree that with regard to the processing of customer content, Healthcare Platform "**B**" may act either as a controller or processor, and Video API Provider "**Y**" is a processor. The Data Protection Addendum of Video API Provider "**Y**" sets forth that Video API Provider "**Y**" processes

customer content in accordance with the customer's instructions. Moreover, the parties acknowledge that, with regard to the processing of customer account data, Healthcare Platform "**B**" is a controller and Video API Provider "**Y**" is an independent controller, not a joint controller with the customer. The parties also acknowledge that with regard to the processing of customer usage data, Healthcare Platform "**B**" may act either as a controller or processor, and Video API Provider "**Y**" is an independent controller, not a joint controller with Healthcare Platform "**B**". In summary, similarly to the previous case, the Data Processing Addendum of Video API Provider "**Y**" differentiates between processing of personal data relating to the arrangement of a teleconsultation and the content of the teleconsultation.

In terms of the data protection relationships between the healthcare platforms and the healthcare providers, there is a similar distinction between two sets of processing operations. According to their respective Privacy Policies, Healthcare Platform "**A**" and Healthcare Platform "**B**" act as controllers of the personal data of users, who register to the platform (as patients or health professionals). Indeed, as the EDPB Guidelines 07/2020 points out, when an entity engages in processing of personal data as part of its interactions with its users, it will generally be the one who can factually determine the purpose and means of the processing and is, therefore, acting as a controller within the meaning of the GDPR. However, it is important to differentiate between these processing operations and processing relating to the provision of a medical service (in-person doctor's visit). As mentioned above, in the latter phase, the healthcare platforms have no control over the determination of the purpose and (essential) means of processing the patient's personal data.

The Privacy Policy of Healthcare Platform "**A**" explicitly mentions this distinction (addressing the patient users of the website who are looking for information about health professionals): "[w]e will store these data on our platform and we will transfer these data to the specialist, and/or to the clinic which employs the specialist. Once your personal data is transferred to the specialist or clinic, the specialist or clinic becomes an independent data controller of your personal data and will process your personal data for its own purposes (for example, for the purposes of the provision of medical or similar services). Such processing will be governed by the specific specialist's, or clinic's privacy policy." What follows from the above-cited provisions is that the healthcare platforms and the healthcare providers (registered on the platforms) make a distinction between processing of personal data relating to the arrangement of a medical service on the platform and processing of personal data

relating to the actual provision of a medical service. This allocation of responsibilities is similar to the above-mentioned relationship between the healthcare platforms and the video communications API service providers, albeit the difference is that, in this case, the provision of the medical service takes place in person, not online.

5.3.) Assessment of controllership (III.): "the purposes and means"

As the EDPB Guidelines 07/2020 explains, determining the purposes and the means amounts to deciding respectively why the processing takes place (i.e. "to what end" or "what for"), and how this objective shall be reached (i.e. which means shall be employed to attain the objective). The controller must decide on both the purpose and the means of the processing. Article 5(1)(b) of the GDPR establishes that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. As regards the determination of means, a distinction has to be made between essential and non-essential means. According to the EDPB Guidelines 07/2020, the notion of "essential means" is closely linked with the purpose and the scope of the processing, and is inherently reserved to the controller. Examples of essential means are the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?"), and the categories of data subjects ("whose personal data are being processed?"). "Non-essential means" concern more practical aspects of implementation, such as the choice of a particular type of hardware or software, or the detailed security measures which may be left to the processor to decide on. Although the controller may leave decisions on non-essential means to the processor, the EDPB Guidelines 07/2020 recommends the documentation of the minimum necessary technical and organisational measures between the controller and the processor in a contract or other legally binding instrument.

In the context of teleconsultation, as mentioned above, the processing of personal data may take place for purposes relating to either the arrangement of a teleconsultation or the online provision of a medical service. In the first case, the purpose and means are determined by the healthcare platform that processes the personal data of users (patients and health professionals) in order to enable them to conduct teleconsultation via the platform's

"auxiliary service". In the second case (during the online provision of a medical service), the healthcare professional (on behalf of the healthcare provider) determines the purpose and means of processing the personal data of the patient. Although the processing of the patient's personal data for the purpose of providing healthcare takes place by means of a video communications API service that is integrated into the healthcare platform, the technical aspects of this processing are "non-essential means". They are simply supplementary to the core processing activity determined by the healthcare provider in the communications content of the healthcare service.

5.4.) Assessment of controllership (IV.): "alone or jointly with others"

The controller is the actor who "alone or jointly with others" determines the purposes and means of the processing. This means that several different entities may act as controllers for the same processing, with each of them being subject to the applicable data protection provisions. According to the EDPB Guidelines 07/2020, the overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. More specifically, joint participation needs to include the determination of purposes, on the one hand, and the determination of means, on the other hand. If both of these elements are determined by all entities concerned, they should be considered joint controllers of the processing at issue. In practice, joint participation can take different forms, such as a common decision by two or more entities or converging (complementing and inextricably linked) decisions by two or more entities. However, as the CJEU clarified in *Fashion ID*, that a "natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means."[622]

In light of the foregoing, it is necessary to determine whether joint controllership exists between the respective healthcare platform and the video communications API service providers with regard to the processing of customer account data and customer usage data (the latter only in the case of Healthcare Platform "**B**" and Video API Provider "**Y**"). In

[622] *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, *supra* note 590, para. 74.

essence, this question is about which entity processes personal data for the purpose of transmitting or exchanging customer content, or to put simply, which entity determines the technical arrangements of a video call. In the present cases, there are converging economic interests between the healthcare platforms and the video communication API service providers (in providing service to end users) arising from the same processing operation. However, the EDPB Guidelines 07/2020 pointed out that the mere existence of a mutual (e.g. commercial) benefit arising from a processing activity does not give rise to joint controllership by itself. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely paid for services rendered, it is acting as an independent controller or processor, rather than as a joint controller.

In the present cases, the healthcare platforms and the video communications API service providers successively process the same personal data in a chain of operations (in order to arrange the technical aspects of a teleconsultation, as explained above), with each of these actors having an independent purpose in their part of the chain. As the Data Protection Addendum of Video API Provider "**X**" and the Data Protection Addendum of Video API Provider "**Y**" set forth, both video communications API service providers pursue their own purposes relating to the processing of customer account data and customer usage data. This means that, for example, Video API Provider "**X**" may, as an independent controller, process data used to trace and identify the source and destination of a communication (as part of "customer account data") for the purposes defined in the Privacy Policy of Video API Provider "**X**". However, these purposes differ from the purposes of processing personal data established by Healthcare Platform "**A**" in its Privacy Policy, despite the fact that Healthcare Platform "**A**" may, as independent controller, also process information about the user's device, IP address, time zone, language or browser for the purpose of providing a teleconsultation service to its users.

5.5.) Assessment of controllership (V.): "processing of personal data"

The purposes and means determined by the controller must relate to the "processing of personal data". As patients must provide personal information when registering to the services of an online doctor marketplace, and booking a teleconsultation thereof, those

entities process personal data relating to data subjects. According to the Privacy Policies of Healthcare Platform "**A**" and Healthcare Platform "**B**", this may include the processing of the following personal data: patient's name, telephone number, email address, reason for visit, type of medical examination and usage data. For the purpose of the technical arrangement of a teleconsultation, the healthcare platforms and the video communications API service providers process customer usage data in order to identify the source and destination of a video call. This implies the processing of data subjects' telephone numbers, data on the location of the device generated in the context of providing the service, the date, time, duration and the type of communication, as well as activity logs (used to identify the source of service requests, optimise and maintain performance of the services, and investigate and prevent system abuse). However, during the provision of healthcare by means of teleconsultation, neither the healthcare platform, nor the video communications API service provider processes personal data in the customer content. If the patient shares personal data with the health professional during the video call, healthcare platform would process this personal data (as processor) only, if the health professional records it in the patient's electronic health record on the healthcare platform.

5.6.) Assessment of processorship

In follow-up to the previous assessment of controllership, it is also important to clarify why healthcare platforms act as processors in relation to the processing of personal data during the patient–doctor interaction ("customer content")? According to Article 4(8) of the GDPR, the processor "processes personal data on behalf of the controller." This implies that the processor must be a separate entity in relation to the controller and processing personal data on the controller's behalf. With regard to the first condition, the healthcare platforms and the healthcare providers are clearly separate entities. As for the second condition, acting "on behalf of" means serving someone else's interest. This means that the processor may not carry out processing for its own purpose(s). As the EDPB Guidelines 07/2020 explains, in the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means. The controller's instructions may though leave a certain degree of discretion to the processor on how to best serve the controller's interests in allowing the choice of the

most suitable technical and organisational means. Furthermore, nothing prevents the processor from offering a preliminary defined service, but the controller must make the final decision to approve the way that the processor carries out the processing and/or to be able to request changes, if necessary.

The Teleconsultation Notice of Healthcare Platform "**A**" allocates responsibility between Healthcare Platform "**A**" and the healthcare providers in line with the aforementioned considerations. (As a matter of note, there are no corresponding terms and conditions for teleconsultation available by Healthcare Platform "**B**".) The Teleconsultation Notice of Healthcare Platform "**A**" sets forth that the health professional is solely responsible for the online consultation services. On the other hand, Healthcare Platform "**A**" is solely responsible for providing auxiliary technical services to facilitate online consultation and for granting users the right to access the platform. The services provided by Healthcare Platform "**A**" depends on the health professional's decision and may include: (i) reservation services for online consultations; (ii) audiovisual communication services; and (iii) redirection services to the health professional's payment provider. In all cases, Healthcare Platform "**A**" is considered a mere "intermediary service provider" in the context of teleconsultation services, therefore, the relevant exemptions and exclusions of responsibility established with respect to intermediate service providers according to the law will apply, unless otherwise indicated in the Teleconsultation Notice of Healthcare Platform "**A**". The Teleconsultation Notice of Healthcare Platform "**A**" also makes it clear that the patient acknowledges that Healthcare Platform "**A**" is only a provider of auxiliary technical services and is not involved in the provision of healthcare services.

Regarding data processing, the Teleconsultation Notice of Healthcare Platform "**A**" states that patients must provide the health professional with the personal data necessary to create and maintain the patient's health records (if applicable), as well as contact data, including their email address and telephone number. The provision of some teleconsultation services may be dependent on the patient providing additional data; in this regard, the health professional will inform the patient about the data that is required. In addition to this, the health professional may register the teleconsultation (on the platform or elsewhere), and may create and maintain the necessary patient's health record (if applicable), and will maintain it for the period of time required by law. However, Healthcare Platform "**A**" is not responsible for the creation, maintenance or updating of the patient's clinical or medical history. The health professional is solely responsible for the secure storage of the patient's health record

created as a result of a teleconsultation and the personal data included therein, in accordance with laws and regulations. Although the Teleconsultation Notice of Healthcare Platform "**A**" does not explicitly mention this, but if the health professional stores the patient's health record on the platform, then the general privacy policy conditions of Healthcare Platform "**A**" will apply. With regard to the foregoing terms and conditions, it is clear that Healthcare Platform "**A**" may not carry out processing for its own purpose(s). The Healthcare Platform "**A**" may process personal data collected as a result of a teleconsultation only acting "on behalf of" the healthcare provider.

5.7.) Summary: allocation of responsibilities

Based on the foregoing assessment, the following table summarises the data protection functional roles (according to the various types of processed personal data), when users (patients and healthcare providers) conduct teleconsultation by using the healthcare platform of Healthcare Platform "**A**", which has integrated the video communications API service of Video API Provider "**X**":

	Patient	**Healthcare provider**	**Healthcare platform (customer)** (Healthcare Platform "**A**")	**Video communications API service provider platform** (Video API Provider "**X**")
Customer account data I. (personal data that relates to the customer relationship of Healthcare Platform "**A**" with Video API Provider "**X**")	third party	third party	data subject (personal data relating to the customer's employees and agents)	controller
Customer account data II. (personal data used to identify the source and destination of a video call)	data subject	data subject (personal data relating to the health professional)	independent controller	independent controller
Customer content (personal data exchanged during the patient-doctor teleconsultation)	data subject	controller	Processor	sub-processor

The following table summarises the data protection functional roles, when users (patients and healthcare providers) conduct teleconsultation by using the healthcare platform of Healthcare Platform "**B**", which has integrated the video communications API service of Video API Provider "**Y**":

	Patient	**Healthcare provider**	**Healthcare platform (customer)** (Healthcare Platform "**B**")	**Video communications API service provider platform** (Video API Provider "**Y**")
Customer account data (personal data that relates to the customer relationship of Healthcare Platform "**B**" with Video API Provider "**Y**")	third party	third party	data subject (personal data relating to the customer's employees and agents)	controller
Customer usage data (personal data used to identify the source and destination of a video call)	data subject	data subject (personal data relating to the health professional)	independent controller	independent controller
Customer content (personal data exchanged during the patient-doctor teleconsultation)	data subject	controller	Processor	sub-processor

CHAPTER 5:

ONLINE DOCTOR MARKETPLACES IN THE EUROPEAN HEALTH DATA SPACE

1.) Case study: problem description

The Proposal for a Regulation on the European Health Data Space[623] ('EHDS proposal') is the EU's first proposal of a domain-specific common European data space. According to Recital 1 of the EHDS Proposal, the Regulation has three aims:

- to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data);
- to enhance the (re-)use of health data for other purposes that would benefit society, such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities (secondary use of electronic health data); and
- to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of electronic health record systems ('EHR systems').

The objective of this chapter is to analyse the data protection-related implications of the EHDS Proposal for an online doctor marketplace that also provides healthcare SaaS functionalities (such as a cloud-based EHR system or teleconsultation services). The analysis builds on empirical evidence collected from a real-world scenario, and focuses on the practical challenges that an online doctor marketplace may face when implementing the provisions of the EHDS Proposal.[624] These compliance challenges include applying the EHDS Proposal in concrete circumstances, establishing new data governance structures and the (re)configuration of certain platform functionalities. The focus of the analysis is on:

(a) the general provisions of the EHDS Proposal (applicability and definitions); and
(b) the rights of natural persons relating to the primary use of their electronic health data provided by the EHDS Proposal, and their interaction with corresponding data subject rights under the GDPR.

---

[623] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, Strasbourg (3 May 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197>.

[624] The analysis has altered company names and modified/simplified real-world facts encountered in the course of an industrial PhD collaboration.

2.) General provisions of the EHDS proposal and its implications for an online doctor marketplace

2.1.) Scope of application

Article 1(3) of the EHDS proposal

"This Regulation applies to:

(a) manufacturers and suppliers of EHR systems and wellness applications placed on the market and put into service in the Union and the users of such products;

(b) controllers and processors established in the Union processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;

(c) controllers and processors established in a third country that has been connected to or are interoperable with MyHealth@EU, pursuant to Article 12(5);

(d) data users to whom electronic health data are made available by data holders in the Union."

Article 1(3)(a) of the EHDS proposal refers to the subject categories of 'manufacturer', 'supplier' and 'user'. With regard to the cross-reference of Article 2(1)(d) of the EHDS proposal to Article 3(8) of Regulation (EU) 2019/1020 on market surveillance and compliance of products,[625] "'manufacturer' means any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under its name or trademark." However, the EHDS proposal does not provide corresponding definitions for 'supplier' and 'user', which creates uncertainty regarding their application. For this reason, it is unclear how the category of 'supplier' relates to the category of 'distributor', which Article 2(1)(d) of the EHDS proposal defines pursuant to Article 3(10) of Regulation (EU) 2019/1020. It is also unclear whether 'user' only means 'end user' (or 'end recipient'), or whether it also includes the intermediary category of 'deployer'. These shortcomings could lead to uncertainty, for example, in the case of an online doctor marketplace that provides a cloud-based EHR system to healthcare providers, which another entity (belonging to the same company group) developed originally. In this case, it is debatable whether the online doctor marketplace would qualify as a 'manufacturer', 'supplier', 'user', or neither of these.

[625] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>.

Similarly to the abovementioned categories, Article 1(3)(a) of the EHDS proposal uses the terms 'placing on the market' and 'putting into service', but it does not refer to the action of 'making available on the market'. In general, the EHDS proposal refers to these terms inconsistently (*cf.* Articles 1(2)(b), 1(3)(a) and 2(1)(d)). The Commission Notice "The 'Blue Guide' on the implementation of EU products rules 2016" outlines the differences between these notions, which highlights the importance of referring to these terms accurately. "A product is made available on the market when supplied for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge."[626] "A product is placed on the market when it is made available for the first time on the Union market."[627] "Putting into service takes place at the moment of first use within the Union by the end user for the purposes for which it was intended."[628]

Article 1(3)(b) states that the EHDS proposal applies to two categories of subjects—which may lead to uncertainties in specific scenarios:

1. On one hand, the EHDS proposal applies to "controllers and processors established in the Union processing electronic health data". With regard to Article 3(2) of the GDPR and the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)[629], the GDPR is applicable to such processing activities. However, there is uncertainty about whether the EHDS proposal would apply to the processing of electronic health data by a healthcare provider that is established outside the Union, but provides telemedicine service to a Union citizen or third-country national legally residing in the territory of a Member State via an online doctor marketplace established in the Union. For example, this would be the case when a Spanish-speaking psychologist licensed in a third country (e.g. Gibraltar, the UK or Venezuela) provides teleconsultation to a citizen of Spain via an online doctor marketplace operated by a legal person established in Spain.

   Furthermore, it is unclear what the applicable law would be for the delivery of healthcare service by a healthcare provider that is established outside the Union. This

[626] Commission Notice — The 'Blue Guide' on the implementation of EU products rules 2016, C/2016/1958, OJ C 272, 26.7.2016, 1–149 at 17. CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016XC0726(02)>.

[627] *Ibid*., 18.

[628] *Ibid*., 21.

[629] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), *supra* note 553, 5 *et seq*.

has far-reaching implications in terms of professional licensing, liability, social insurance, taxation issues etc. In EU law, the guiding principle for determining the jurisdiction of cross-border healthcare services is set forth under Article 3(d) of 'Directive 2011/24/EU on the application of patients' rights in cross-border healthcare'[630]: "'Member State of treatment' means the Member State on whose territory healthcare is actually provided to the patient. In the case of telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established". By way of analogy, one could argue that the state of treatment in the previous example would be the third country (e.g. Gibraltar, the UK or Venezuela). For this reason, the Terms and Conditions of an online doctor marketplace established in a Member State should warn patients about any risks emerging from the choice of a healthcare provider that is established outside that Member State, or the Union. Additionally, the online doctor marketplace should clearly indicate, if a health professional is not licensed according to the applicable law governing the Terms and Conditions and Privacy Policies (in the aforementioned example, this would be Spanish law).

2. On the other hand, the EHDS proposal applies to the processing of electronic health data of "Union citizens and third-country nationals legally residing in the territories of Member States". Conversely, the EHDS proposal does not apply to third-country nationals residing outside the EU. This would exclude from the scope of application, for example, the processing of electronic health data of a British citizen, who is on a short-term vacation in Spain, and intends to register as a patient on an online doctor marketplace operated by a legal person established in Spain. However, with regard to Article 3(2) of the GDPR and the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)[631], the GDPR would still apply in this case. This appears to be a regulatory shortcoming of the EHDS proposal, and a contradiction with the GDPR.

Article 1(3)(c) of the EHDS proposal refers to healthcare providers (acting as controllers or processors) established in a third country, which has a national contact point for international electronic health data exchange that is compliant with the requirements of MyHealth@EU pursuant to Recital 26 and Article 13(3) of the EHDS proposal. This would

---

[630] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, *see supra* note 554.

[631] EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), *supra* note 553, 14 *et seq*.

be relevant, for example, if the healthcare provider of a Member State intends to transfer (exchange) electronic health data to a healthcare provider established in a third country (or *vice versa*). In this case, the healthcare provider established in the EU Member State would have to transmit electronic health data to the national contact point of its Member State. The Member State would transfer the electronic health data via the MyHealth@EU infrastructure and platform to the national contact point of the third country. The national contact point of the third country would then transmit the electronic health data to the healthcare provider established in the third country.

Finally, Article 1(3)(d) refers to cases when a data user has lawful access to electronic health data held by a data holder for secondary use.

2.2.) Definitions

2.2.1.) Personal and non-personal electronic health data

Article 2(2) of the EHDS proposal

(a) 'personal electronic health data' means data concerning health and genetic data as defined in Regulation (EU) 2016/679, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services, processed in an electronic form;
(b) 'non-personal electronic health data' means data concerning health and genetic data in electronic format that falls outside the definition of personal data provided in Article 4(1) of Regulation (EU) 2016/679;
(c) 'electronic health data' means personal or non-personal electronic health data;

Article 2(2)(a) of the EHDS proposal provides a definition of 'personal electronic health data', which lacks alignment with the definition of 'data concerning health' under Article 4(15) of the GDPR:

1. It is unclear why 'genetic data', as defined under Article 4(13) of the GDPR pursuant to the cross-reference of Article 2(1)(a) of the EHDS proposal, is included within the scope of 'personal electronic health data' under Article 2(2)(a) of the EHDS proposal. By contrast, Recital 19 of the EHDS proposal refers to these data categories separately as 'personal health and genetic data in an electronic format'.
2. It is also unclear why Article 2(2)(a) of the EHDS proposal refers separately to 'data referring to determinants of health, or data processed in relation to the provision of healthcare services' as if they were distinct data categories from 'data concerning

health'. In the GDPR, the latter is a superset of the former data category. According to Article 4(15) of the GDPR, "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". Recital 35 of the GDPR (albeit not binding) extends this definition as follows: "[p]ersonal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services". With regard to this reasoning, 'data concerning health' encompasses all data revealing information about the health status of a natural person; data relating to prospective health insights ("future health status"); as well as data collected in the course of registration for healthcare services. This broad interpretation is in line with the CJEU's case law, notably *Lindqvist*, in which the Court held that: "the expression data concerning health [...] must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual".[632]

3. Recital 5 of the EHDS proposal provides an even wider interpretation to 'personal electronic health data': "[s]uch personal electronic health data could include personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status, 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 in question, as well as data determinants of health, such as behaviour, environmental, physical influences, medical care, social or educational factors. Electronic health data also includes data that has been initially collected for research, statistics, policy making or regulatory purposes and may be made available according to the rules in Chapter IV. The electronic health data concern all categories of those data, irrespective to the fact that such data is provided by the data subject or other natural or legal persons, such as health professionals, or is processed in relation to a natural person's health or well-being and should also include inferred and

[632] *Criminal proceedings against Bodil Lindqvist*, *supra* note 536, para. 50.

derived data, such as diagnostics, tests and medical examinations, as well as data observed and recorded by automatic means."

This meaning of 'personal electronic health data' includes data based on mere calculation, whereby the controller uses additional information ('derived data'), as well as data obtained through data analysis relying on statistical assumptions ('inferred data'). This is consistent with how the Article 29 Data Protection Working Party interpreted 'data pertaining to the health status of a data subject' in its 'Letter to the European Commission, DG CONNECT on mHealth'.[633] According to Recital 5 of the EHDS proposal, the notion of 'personal electronic health data' also encompasses data relating to environmental, social or educational factors that are determinants of health. In this regard, it is important to point out that not all environmental, social or educational data collected in a healthcare setting would automatically qualify as 'data concerning health'. As the Article 29 Data Protection Working Party pointed out, "[t]here has to be a demonstrable relationship between the raw data set and the capacity to determine a health aspect of a person, based on the raw data itself or on the data in combination with data from other sources."[634]

Article 2(2)(b) of the EHDS proposal refers to 'non-personal electronic health data' meaning "data concerning health and genetic data in electronic format that falls outside the definition of personal data provided in Article 4(1) [of the GDPR]". The EHDS proposal is without prejudice to the GDPR and applies the definitions in the GDPR (see Articles 1(4) and 2(1) of the EHDS proposal). However, data concerning health and genetic data are personal data (see Articles 4(13) and 4(15) of the GDPR). Conversely, if data does not qualify as 'personal data' under the GDPR (for example, because it is anonymised), then it cannot be 'data concerning health' or 'genetic data'. Consequently, there is a contradiction within the definition of 'non-personal electronic health data'.

In general, when the content of the foregoing data categories become clear, it will be important more than ever to use accurate legal terms to describe various health-related data categories in line with the terminology of the EHDS proposal and the GDPR. The importance of this lies in the fact that the differentiation between personal and non-personal electronic health data may have legal consequences regarding the application of other provisions of the

---

[633] Article 29 Data Protection Working Party, Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth, Annex – health data in apps and devices, *supra* note 529, 2.

[634] *Ibid*., 4.

EHDS proposal. For this reason, controllers shall facilitate the exercise of data subject rights by providing transparent information on the data categories that they are processing. In the case of an online doctor marketplace, the Privacy Policy could stipulate whether the processing of certain health-related information (e.g. health insurance, family history, IP address, platform usage data) falls under the scope of personal or non-personal electronic health data.

2.2.2.) Primary and secondary use of electronic health data

Article 2(2) of the EHDS proposal

(d) 'primary use of electronic health data' means the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services;

(e) 'secondary use of electronic health data' means the processing of electronic health data for purposes set out in Chapter IV of this Regulation. The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use;

According to Recital 1 of the EHDS proposal, the aim of the Regulation is to establish the European Health Data Space "in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data), as well as for other purposes that would benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities (secondary use of electronic health data)". However, the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' pointed out that the definitions provided in the EHDS proposal may give rise to legal uncertainty and inconsistency with the GDPR, particularly with regard to the definition of 'secondary use of electronic health data'.[635] As the concept of 'secondary use of personal data' does not appear in the GDPR, the second part of the definition under Article 2(2)(e) of the EHDS proposal deviates from the concept of 'further processing of personal data' under the GDPR.

[635] European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space (12 July 2022), para. 42. Available from: <https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf>.

The assessment of whether the further processing of personal data is compatible with the purposes specified at its collection is irrespective of the qualitative aspects of the data.[636] Although the EDPB 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' provided a definition for 'secondary use', the EDPB restricted this notion to data use consisting of the "further processing of data initially collected for another purpose".[637] This interpretation is in line with the general understanding of the meaning of 'secondary use of health data'. However, Article 2(2)(e) of the EHDS proposal would be in conflict with this interpretation as it also includes 'personal electronic health data initially collected in the context of primary use' under the scope of 'secondary use of electronic health data'.

2.2.3.) Interoperability

Article 2(2) of the EHDS proposal

(f) 'interoperability' means the ability of organisations as well as software applications or devices from the same manufacturer or different manufacturers to interact towards mutually beneficial goals, involving the exchange of information and knowledge without changing the content of the data between these organisations, software applications or devices, through the processes they support;

(g) 'European electronic health record exchange format' means a structured, commonly used and machine-readable format that allows transmission of personal electronic health data between different software applications, devices and healthcare providers;

Article 2(2)(f) provides a definition on 'interoperability' that would need clarification about its content and interaction with other relevant provisions of EU law, where interoperability is defined or referred to (*see* Medical Devices Regulation, Data Governance Act or eIDAS Regulation). For example, Article 2(26) of the Medical Devices Regulation provides the following definition: "'interoperability' is the ability of two or more devices, including software, from the same manufacturer or from different manufacturers, to:

(a) exchange information and use the information that has been exchanged for the correct execution of a specified function without changing the content of the data, and/or

---

[636] *See also* Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203) (2 April 2013), 20. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

[637] European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (21 April 2020), para. 11. Available from: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf>.

(b) communicate with each other, and/or

(c) work together as intended."

The medical technology industry agrees with this definition but believes that, by its brevity, it does not cover some relevant domains and aspects.[638] An alternative definition could be the following: "[interoperability] is the ability of different information systems, devices and applications (systems) to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organisational, regional and national boundaries, to provide timely and seamless portability of information and optimise the health of individuals and populations globally. Health data exchange architectures, application interfaces and standards enable data to be accessed and shared appropriately and securely across the complete spectrum of care, within all applicable settings and with relevant stakeholders, including the individual."[639]

The challenges of interoperability for organisations involved in the health data ecosystem (e.g. healthcare providers, online doctor marketplaces, healthcare SaaS platforms) have different focus areas depending on the level of information exchange:[640]

1. The macro level relates to an organisation's role in the broader health data ecosystem and its ability to exchange information with other organisations. This will typically rely on national eHealth interoperability frameworks specifying common standards and formats, which may in turn relay to EU common specifications. In this regard, Article 12 of the EHDS proposal establishes MyHealth@EU, the EU-level central platform for digital health that will provide services to support and facilitate the exchange of electronic health data between the national contact points of Member States. MyHealth@EU is provided through the eHealth Digital Service Infrastructure (eHDSI) that enables the exchange of health data in a secure, efficient and interoperable way.[641]

---

[638] MedTech Europe, COCIR (2021) *Interoperability standards in digital health: A White Paper from the medical technology industry*. MedTech Europe, COCIR (6 October 2021), 3. Available from: <https://www.medtecheurope.org/wp-content/uploads/2021/10/mte_interoperability_digital_health_white-paper_06oct21.pdf>.

[639] Healthcare Information and Management Systems Society (2020) *Interoperability in Healthcare*. HIMSS, Chicago (4 August 2020), 3. Available from: <https://www.himss.org/resources/interoperability-healthcare>.

[640] eHAction (2021) *Interoperability Guide*. eHAction. Available from: <https://ehaction.eu/interoperability-guide/about-the-guide/#titulo2>.

[641] European Commission (n.d.) *Electronic cross-border health services*. European Commission. Available from: <https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en> (accessed 1 October 2022).

2. The meso level of interoperability relates to the ability of information systems within the organisation to seamlessly transmit data, for example, between electronic health datasets, or for business analytics purposes.
3. At a micro level, a potential challenge for organisations is to enable not only manual data entry by health professionals, but also to permit the integration of automated recording of data by Internet of Health Things devices. In relation to this, it is important to point out that manual and automatic processing of data may pose different challenges for ensuring data quality.

Article 2(2)(g) states that the transmission of personal health data in a European electronic health record exchange format may take place between "software applications, devices and healthcare providers". The boundaries of these categories are misty, for example, in the case of an online doctor marketplace that provides SaaS for healthcare providers to process EHRs on its platform by use of the platform's software application. If a healthcare provider transmits an EHR (as a collection of personal health data) stored on the platform, then it is debatable whether that will be transmitted from the healthcare provider (user of the service), the platform's servers (place of data storage), or the platform's software application (the means applied to send the request).

2.2.4.) Health data access services

Article 2(2) of the EHDS proposal

(i) 'electronic health data access service' means an online service, such as a portal or a mobile application, that enables natural persons not acting in their professional role to access their own electronic health data or electronic health data of those natural persons whose electronic health data they are legally authorised to access;

(j) 'health professional access service' means a service, supported by an EHR system, that enables health professionals to access data of natural persons under their treatment;

Articles 2(2)(i) and 2(2)(j) of the EHDS proposal define two types of personal health data access services. By reference to Recital 7 of the EHDS proposal, the purpose of these services is to enable natural persons or health professionals to access, share and change electronic health data. The EHDS proposal prescribes that the establishment of these services is the responsibility of Member States. Article 3(5)(a) of the EHDS proposal requires Member States to establish one or more electronic health data access services at national, regional or local level. Article 4(3) of the EHDS proposal requires Member States to ensure

that access to at least the priority categories of electronic health data is made available to health professionals through health professional access services. These rules imply that the concept of a personal health data access service is essentially to function as a "one-stop shop" to access, share or change electronic health data within the health data ecosystem.

By textual interpretation, an online doctor marketplace would typically qualify as an 'electronic health data access service' and 'health professional access service'. However, as explained above, according to Article 3(5)(a) and Article 4(3) of the EHDS proposal, it is the responsibility of Member States to establish these services. This contradiction calls for a re-definition of these services. Furthermore, there is a lack of clarity about the underlying data governance mechanisms, in particular, how personal health data access services would interact with a vast number of EHR systems operated by a diverse range of entities, and what rules would govern these interactions. To illustrate the magnitude of the problem, according to an estimate given in the Impact Assessment Report accompanying the EHDS proposal, there may be 4,000-5,000 EHR systems on the EU market.[642] (Finland alone has 400 EHR systems.) The provisions of the EHDS proposal require that personal health data access services should be connected with all EHR systems in a Member State. In practice, this would have far-reaching legal implications, and would need immense technical and organisational collaboration.

2.2.5.) Telemedicine

Article 2(2) of the EHDS proposal

(l) 'telemedicine' means the provision of healthcare services, including remote care and online pharmacies, through the use of information and communication technologies, in situations where the health professional and the patient (or several health professionals) are not in the same location;

Article 2(2)(l) of the EHDS proposal sets forth a definition for 'telemedicine' that is not in line with the general understanding of this term. As mentioned in the Introduction, there is a growing body of literature which argues that 'telemedicine' is reserved for the use of ICT to deliver clinical services at a distance, while 'telehealth' is a more generic term that also

[642] Commission Staff Working Document Impact Assessment Report Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final - SEC(2022) 196 final - SWD(2022) 130 final - SWD(2022) 132 final', *supra* note 43.

includes the delivery of non-clinical services to promote health and well-being.[643] Consequently, 'online pharmacies' would not fall under the scope of 'telemedicine', and neither would 'remote care' (which, as a matter of note, has more of a social dimension, and is not an equivalent term to 'remote healthcare'). In this regard, Recital 21 of the EHDS proposal adds that: "[w]hen digital services accompany the physical provision of a healthcare service, the digital service should be included in the overall care provision." However, it is debatable what the vague expression 'accompanying digital services' may cover in the context of telemedicine.

As mentioned, Article 3(d) of 'Directive 2011/24/EU on the application of patients' rights in cross-border healthcare'[644] sets forth that "[i]n the case of telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established". The 'Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services' clarifies that a healthcare professional offering telemedicine needs only to be registered in the country where he/she is physically established.[645] The applicability of the service provider's Member State of establishment legislation ('country-of-origin principle') is also enshrined in Articles 3(1) and 3(2) of the e-Commerce Directive[646]. However, in the absence of a law choice clause in a telemedicine contract concluded between a healthcare provider and a patient, the law applicable in case of conflict is the country where the patient has their habitual residence as long as the healthcare provider "directs" by any means its activities to that country.[647] In case of an alleged infringement relating to the processing of the personal data of the patient (data subject) in telemedicine, Article 77(1) of the GDPR, the data subject has the right to lodge a complaint with the supervisory authority in the Member State of his or her habitual residence, place of work or place of the alleged infringement.

---

[643] *See supra* note 50.

[644] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, *see supra* note 554.

[645] Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services Accompanying the document 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions eHealth Action Plan 2012-2020 – innovative healthcare for the 21st century, COM(2012) 736 final - SWD(2012) 413 final' SWD(2012) 414 final, Brussels (6 December 2012). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012SC0414>.

[646] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, 1–16. ELI: <http://data.europa.eu/eli/dir/2000/31/oj>.

[647] Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services, *supra* note 647.

With regard to the abovementioned "blurry" boundaries of the definition of 'telemedicine', it is unclear whether an online doctor marketplace provides telemedicine services according to the provisions of the EHDS proposal (and, if yes, which functionalities of its services would fall under the definition of 'telemedicine'). The chat and teleconsultation functionalities provided by an online doctor marketplace, as well as the integrated EHR system of the platform may arguably qualify as "digital services accompanying the physical provision of a healthcare service". However, it is unclear whether its search engine functionality or the patient reviews section on the platform can be considered as "digital services accompanying the physical provision of a healthcare service". The significance of this question is that if certain digital services provided by the online doctor marketplace fall under the scope of 'telemedicine', then it may affect whether other provisions of the EHDS proposal, such as Article 8 (on telemedicine in a cross-border context) or Article 9(1) (on identification management), are applicable to the online doctor marketplace, or not.

2.2.6.) Electronic health record (EHR) and EHR system

Article 2(2) of the EHDS proposal

(m) 'EHR' (electronic health record) means a collection of electronic health data related to a natural person and collected in the health system, processed for healthcare purposes;

(n) 'EHR system' (electronic health record system) means any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records;

Article 2(2)(m) of the EHDS proposal refers to the collection of 'electronic health data' related to a natural person. This term covers the collection of both personal and non-personal electronic health data in accordance with Article 2(2)(c) of the EHDS proposal. Considering that Article 3(6) of the EHDS proposal establishes a 'right to insert data', the additional condition of "collected in the health system" set forth under Article 2(2)(m) of the EHDS proposal must be interpreted broadly to include not only medical data (collected in the clinical context), but also self-tracking data (collected by the natural person). However, if the condition of "collected in the health system" may include data generated by wellness applications, then this condition is in contradiction with the restriction that a 'wellness application' is intended to be used for "processing electronic health data for *other purposes than* healthcare" (*see* Article 2(2)(o)).

The definition of an 'EHR' under Article 2(2)(n) of the EHDS proposal may pose uncertainties for an online doctor marketplace, because the definition is too broad. In addition, it is inconsistent with the definitions of 'electronic health record', 'electronic medical record', 'clinical history' or 'medical dossier' used in the medical laws of Member States (e.g. France, Italy, Spain).[648] Article 2(2)(n) of the EHDS proposal may cover various collections of electronic health data that are usually not defined as an 'EHR'. For example, when a patient registers on an online doctor marketplace to seek an appointment with a health professional, the platform may offer the patient a functionality to create a health profile, which the patient may share with the health professional before the doctor's visit (or teleconsultation). This health profile may include self-reported information about the patient's symptoms, allergies, health insurance etc. This health profile would *de jure* satisfy the definition of an 'EHR' under Article 2(2)(m) of the EHDS proposal, but in practice, it is merely a modality to share information with a health professional.

In connection with these provisions, another uncertainty relates to the legal status of a cloud-based patient management system that an online doctor marketplace provides (as SaaS) to its registered health professionals (or clinics) in order to enable them to process patients' personal data and medical history (relating to healthcare service delivered by that health professional or clinic). Patient records in these systems would qualify as an 'EHR' under Article 2(2)(m) of the EHDS proposal. However, it not clear in the EHDS proposal what the legal, technical and data governance relationship would be between this EHR (system) processed on the healthcare platform and the central (regional or national level) EHR (system) processed in the eHealth infrastructure of a Member State.

2.2.7.) Data holder, data user and data recipient

Article 2(2) of the EHDS proposal:

(k) 'data recipient' means a natural or legal person that receives data from another controller in the context of the primary use of electronic health data;"

(y) 'data holder' means any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or

---

[648] *See also* Comandé G (2020) Italy. *In*: Nys H (ed) *International Encyclopaedia of Laws: Medical Law*. Kluwer Law International, Alphen aan den Rijn, 234 *et seq* [para. 804 *et seq*.]. Available from: <https://kluwerlawonline.com/EncyclopediaChapter/IEL+Medical+Law/MEDI20190018>; Bincoletto G (2021) *Data Protection by Design in the E-Health Care Sector: Theoretical and Applied Perspectives*. Nomos, Baden-Baden, 243 *et seq*. Available from: <https://www.nomos-elibrary.de/10.5771/9783748929895.pdf>.

national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data;"

(z) 'data user' means a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use;

Article 2(2)(y) of the EHDS proposal defines the subject category of 'data holder', but as the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' explained, this definition is so broad that it does not allow to clearly identify who would qualify as 'data holder'.[649] Furthermore, it hinders the understanding of how it interacts with the definitions of 'data holder' provided under Article 2(6) of the Data Act and Article 2(8) of the Data Governance Act. If the definition does not clarify who acts as data holder, then this may lead to uncertainty as to who has the obligation to make data available for secondary use under Articles 33(1) of the EHDS proposal, which in turn, might undermine the rights to privacy and data protection of data subjects. Similarly, Article 2(2)(y) provides a definition of 'data user'. However, the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' pointed out that it is unclear how it relates to the definition of 'data recipient' under Article 2(2)(k) of the EHDS proposal.[650] It also lacks clarity how it interacts with the notions of 'data user' under Article 2(9) of the Data Governance Act and 'recipient' under Article 2(9) of the GDPR. Despite these legal uncertainties, an online doctor marketplace will typically qualify as a 'data holder', because it is an entity in the health sector who has the right or obligation (in the case of non-personal data, the ability) through control of the technical design of a product and related services to make available certain data. On the other hand, it will typically not qualify as a 'data user', because it does not process electronic health data for secondary use.

[649] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, *supra* note 635, para. 44.

[650] *Ibid*., para. 45.

3.) Rights of natural persons in relation to the primary use of their personal electronic health data under the EHDS proposal and implications for an online doctor marketplace

3.1.) Right to access

Article 3(1) of the EHDS proposal:

"Natural persons shall have the right to access their personal electronic health data processed in the context of primary use of electronic health data, immediately, free of charge and in an easily readable, consolidated and accessible form."

Article 3(1) of the EHDS proposal extends the 'right of access to data by the data subject', established by Article 15 of the GDPR, to the health sector. Recital 6 of the EHDS proposal explains that the EHDS builds upon the rights of natural persons in relation to the processing of their personal data set out in Chapter III of the GDPR, and further develops some of them. However, the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' pointed out that: "the EDPB and the EDPS hold major concerns regarding the interplay of such newly introduced rights with the ones provided in Articles 15-22 of the GDPR.[651] In particular, the EDPB and the EDPS are concerned regarding the overlap of the rights envisaged in the Proposal with the ones provided for in the GDPR and the risk of legal uncertainty that this may bring *vis-a-vis* the data subjects."

The relationship between Article 15 of the GDPR and Article 3(1) of the EHDS proposal exemplifies that there are misalignments that could lead to legal uncertainty:

1. Article 3(1) of the EHDS proposal introduces the 'right to immediate access', without any limitations. By contrast, Article 12(3) of the GDPR requires that the controller provides information on action taken on a request under Article 15 to the data subject without undue delay, but in any event, within one month of receipt of the request. In addition to this, Recital 63 of the GDPR sets a condition that the data subject may exercise the right of access to personal data "at reasonable intervals".
2. Article 3(1) of the EHDS proposal introduces the 'right of access free of charge', similarly, without any limitations. By contrast, Article 15(3) of the GDPR sets forth

[651] *Ibid*., para. 48.

that "[for] any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs."

It is worth recalling that the EDPB 'Guidelines 01/2022 on data subject rights - Right of access' provides more precise guidance on how the 'right of access' has to be implemented in different situations. The following points are of relevance and significance to an online doctor marketplace:

1. If the data subject makes a request using a communication channel provided by the controller that is different from the one indicated as the preferable one (e.g. instead of using the modalities in the application, the data subject sends a request to the general e-mail address provided on the website), the request shall be, in general, considered effective.[652] With reference to Article 12(6) of the GDPR, if the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject. However, such additional information should not be more than the information initially needed for the verification of the data subject's identity.[653]
2. It should be emphasised that using a copy of an identity document as a part of the authentication process is inappropriate, unless it is strictly necessary, suitable, and in line with national law.[654] Verification on the basis of an ID card may be a justified and proportionate measure, for example for entities processing special categories of personal data or undertaking data processing which may pose a risk for data subject (e.g. medical or health information).[655]
3. As the GDPR does not regulate requests made through a proxy or a legal guardian on behalf of a minor, the controller should take into account national laws governing legal representation (e.g. powers of attorney), which may impose specific requirements for demonstrating authorisation to make a request on behalf of the data subject.[656]

---

[652] European Data Protection Board, Guidelines 01/2022 on data subject rights - Right of access, *supra* note 581, para. 53.

[653] *Ibid*., para. 66.

[654] *Ibid*., para. 73.

[655] *Ibid*., para. 77.

[656] *Ibid*., para. 79 *et seq*.

4. The scope of the right to access extends to all personal data, including:[657]
    - data knowingly and actively provided by the data subject (e.g. account data submitted via forms, answers to a questionnaire);
    - observed data or raw data provided by the data subject by virtue of the use of the service or the device (e.g. activity logs such as access logs, history of website usage, search activities, location data, clicking activity);
    - data derived from other data, rather than directly provided by the data subject (e.g. classification based on common attributes of data subjects);
    - data inferred from other data, rather than directly provided by the data subject (e.g. results of a health assessment or a personalisation or recommendation process); and
    - pseudonymised data as opposed to anonymised data.
5. A layered approach in relation to the right of access means that a controller, under certain circumstances, can provide the personal data and the supplementary information required under Article 15 in different layers. The first layer should include information about the processing and data subject's rights according to Articles 15(1)(a)-(h) and 15(2) of the GDPR, as well as a first part of the processed personal data. In the second (and further layers), the controller shall provide the remaining personal data.[658]
6. The provisions on format requirements are different regarding the 'right of access' and the 'right of data portability'. While the 'right of data portability' under Article 20 of the GDPR requires that the information is provided in a machine-readable format, the 'right to information' under Article 15 does not. Hence, formats that are inadequate to comply with a data portability request, for example pdf-files, could still be suitable for complying with a request of access.[659]

In the context of an online doctor marketplace, the natural person (patient) could make a request to exercise the 'right to access' established under Article 3(1) of the EHDS proposal in relation to the processing of his or her electronic health data by either the online doctor marketplace or the healthcare provider (as two independent controllers). When a patient registers on an online doctor marketplace, the online doctor marketplace processes

[657] *Ibid*., para. 96.

[658] *Ibid*., para. 142.

[659] *Ibid*., para. 154.

the patient's data as controller. When the patient makes a booking for a doctor's visit (or teleconsultation), the online doctor marketplace shares some patient's data with the healthcare provider. After this, the healthcare provider becomes an independent controller of the patient's data. In addition to the patient's data that it receives, the healthcare provider may process further patient's data, for example, relating to a medical examination or the completion of the patient's EHR. This example highlights that it is important to inform patients that there are two independent controllers when they book an appointment with a health professional on an online doctor marketplace. (There is a particularly thin line between the processing operations of the two independent controllers when the healthcare provider uses a cloud-based EHR system provided by the online doctor marketplace, because in this case, both set of processing operations may actually take place in the cloud infrastructure of the online doctor marketplace.) For this reason, the Privacy Policy of the online doctor marketplace should inform patients on how they can exercise their 'right to access' in relation to processing operations performed by the online doctor marketplace, and differentiate the scope of accessible data from patient's data that are under the control of the healthcare provider.

3.2.) Right to obtain a copy

Article 3(2) of the EHDS proposal:

"Natural persons shall have the right to receive an electronic copy, in the European electronic health record exchange format referred to in Article 6, of at least their electronic health data in the priority categories referred to in Article 5."

Article 3(2) of the EHDS proposal establishes a separate 'right to obtain a copy'. According to the EDPB 'Guidelines 01/2022 on data subject rights - Right of access', the obligation to provide a copy under the GDPR is not an additional right of the data subject, but the modality of providing access to the data.[660] The requirement to provide a copy means that the controller must provide information on the personal data concerning the person who makes the request in a way that allows the data subject to retain all of the information and to come back to it (e.g. downloadable pdf-form).[661] The scope of the information that the controller

[660] *Ibid*., para. 23.

[661] *Ibid*., para. 25.

must include in the copy is the same as the scope of the access to the data under Article 15(1) of the GDPR.[662] However, it lacks clarity how the structural and format requirements referred to by Article 3(2) of the EHDS proposal can be implemented by an online doctor marketplace in practice. It seems as if Article 3(2) of the EHDS proposal assumes that electronic health data are always processed in a structured (EHR) format. In terms of the primary functionality of an online doctor marketplace (i.e. to enable patients to book an appointment with a health professional), the references to Articles 5 and 6 of the EHDS proposal will not have the same meaningful relevance as in the case of when a healthcare provider processes electronic health data.

3.3.) Right to insert data

Article 3(6) of the EHDS proposal:

"Natural persons may insert their electronic health data in their own EHR or in that of natural persons whose health information they can access, through electronic health data access services or applications linked to these services. That information shall be marked as inserted by the natural person or by his or her representative."

Article 3(6) of the EHDS proposal lacks clarity about the conditions under which natural persons may insert electronic health data of natural persons whose health information they can access, especially because it is unclear what "access to those persons health information" entails. Moreover, there are no provisions in the EHDS proposal regulating the data governance mechanisms between electronic health data access services and 'applications linked to these services'. The latter category would presumably include all kinds of EHR systems, as well as other software used for the collection of electronic health data. Finally, it is unclear whether the healthcare provider would have any obligation to assess the validity and quality of the data inserted by the natural person.

When a patient registers on an online doctor marketplace to seek an appointment with a health professional, the platform may offer the patient a functionality to create a health profile, which enables the patient (natural person) to insert their electronic health data concerning their medical conditions, medications, health insurance etc. As mentioned in relation to Articles 2(2)(m)-(n), legally speaking, this health profile would satisfy the

[662] *Ibid*., para. 23.

definition of an 'EHR', but in practice, it is merely a modality to share information with a health professional via a chat function integrated into the platform or through a third-party provided communications service. The novelty of Article 3(6) of the EHDS proposal is that natural persons should have the right to insert their electronic health data into the EHRs maintained by healthcare providers. According to Recital 10 of the EHDS proposal, some Member States already allow natural persons to add electronic health data to their EHRs or to store additional information in their separate personal health record that can be accessed by health professionals. In order to enable the exercise of this right, an online doctor marketplace that provides an EHR system to its registered healthcare provider users must develop a functionality to allow patients to insert their electronic health data into the EHRs maintained by healthcare providers. Additionally, the online doctor marketplace should update its Privacy Policy to inform patients about how they can exercise their 'right to insert data' with regard to the EHRs kept by healthcare providers on the platform.

3.4.) Right to rectification

Article 3(7) of the EHDS proposal:

"Member States shall ensure that, when exercising the right to rectification under Article 16 of Regulation (EU) 2016/679, natural persons can easily request rectification online through the electronic health data access services referred to in paragraph 5, point (a), of this Article."

Article 3(7) of the EHDS proposal corresponds to Article 16 of the GDPR. According to the GDPR, the controller is responsible for ensuring the rectification of the data. However, the EHDS proposal lacks clarity about the data governance mechanism for fulfilling a rectification request when an electronic health data access service is positioned between the data subject and the respective controller. There is an additional element of uncertainty in relation to the effective exercise of this right given that an online doctor marketplace provides a cloud-based EHR system (as SaaS) for healthcare providers registered on the platform. In this case, if a data subject were to request rectification of their personal data kept in the EHR maintained by the healthcare provider, then the request made online through the electronic health data access service will actually be channelled into an online doctor marketplace's platform. Consequently, an online doctor marketplace will have to enable the exercise of the right to rectification even when the data subject's rectification request relates

to the processing of personal data by the healthcare provider that uses an online doctor marketplace's cloud-based EHR system.

3.5.) Right to data portability

Article 3(8) of the EHDS proposal:

"Natural persons shall have the right to give access to or request a data holder from the health or social security sector to transmit their electronic health data to a data recipient of their choice from the health or social security sector, immediately, free of charge and without hindrance from the data holder or from the manufacturers of the systems used by that holder.

Natural persons shall have the right that, where the data holder and the data recipient are located in different Member States and such electronic health data belongs to the categories referred to in Article 5, the data holder shall transmit the data in the European electronic health record exchange format referred to in Article 6 and the data recipient shall read and accept it. [...]

Natural persons shall have the right that, where priority categories of personal electronic health data referred to in Article 5 are transmitted or made available by the natural person according to the European electronic health record exchange format referred to in Article 6, such data shall be read and accepted by other healthcare providers."

Article 3(8) of the EHDS proposal establishes the right of the data subject to transmit their electronic health data to a data recipient of their choice. However, the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' noted that the provision does not set forth a corresponding obligation for the data holder to perform this action.[663] In connection with this, it is not clear how the data holder has to identify the data recipient, for example, to determine whether the entity receiving the data really belongs to the health or social security sectors. The 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' also pointed out that Article 3(8) of the EHDS proposal does not explicitly ensure that the data subject can decide which data may (not) be transmitted to the data recipient, in the same line as Article 3(9) of the EHDS proposal regulates the 'right to restrict access'.[664]

Article 3(8) of the EHDS proposal corresponds to Article 20 of the GDPR. It is important to note that the GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or contract. For this

[663] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, *supra* note 635, para. 57.

[664] *Ibid*., para. 56.

reason, there is uncertainty as to whether the 'right to data portability' under Article 3(7) of the EHDS proposal would extend to cases where the processing of personal data are based on other legal grounds (e.g. controller's legitimate interests). This matter is of significance to online doctor marketplaces, because their legitimate interests typically constitute an independent legal basis for the processing of certain categories of personal data.

The 'Article 29 Data Protection Working Party Guidelines on the right to data portability' clarified that when providing the required information, controllers must ensure that they distinguish the 'right to data portability' from other rights, and clearly explain the differences between the types of data that a data subject can receive through the rights of access and data portability.[665] In this regard, the WP29 also recommended that controllers always include information about the right to data portability before data subjects close any account they may have. This practice can allow users/patients to take stock of their personal data, and to transmit the data to their own storage place, or to another online doctor marketplace or healthcare provider.

In order to give full value to the 'right to data portability' under the GDPR, the WP29 clarified that data "provided by" the data subject should also include personal data that are observed from the activities of users, such as activity logs, history of website usage or search activities. By contrast, inferred or derived data (e.g. algorithmic results) based on the analysis of data provided by the data subject (through his actions) does not fall under Article 20 of the GDPR.[666] With regard to this authoritative interpretation, it is unclear whether the same interpretation would apply to the 'right to data portability' under Article 3(8) of the EHDS proposal.

3.6.) Right to restrict access

Article 3(9) of the EHDS proposal:

"Notwithstanding Article 6(1), point (d), of Regulation (EU) 2016/679, natural persons shall have the right to restrict access of health professionals to all or part of their electronic health data. Member States shall establish the rules and specific safeguards regarding such restriction mechanisms."

---

[665] Article 29 Data Protection Working Party, Guidelines on the right to data portability, *supra* note 578, 13.

[666] *Ibid*., 10.

Article 3(9) of the EHDS proposal provides natural persons the 'right to restrict access', which enables them to selectively share their electronic health data. However, this provision lacks clarity for several reasons. First, it is dubious whether "their electronic health data" refers to only 'personal electronic health data', or to both 'personal and non-personal electronic health data'. Second, as the provision prescribes Member States to regulate restriction mechanisms, this may lead to a fragmentation in the implementation of this right. In this regard, it is not clear which jurisdiction would be applicable in cross-border scenarios where a patient intends to restrict access to his or her electronic health data in relation to which health professionals from different Member States have had access to. Third, it is not clear how this right would interact with the provisions regulating access by health professionals to personal electronic health data. On one hand, Article 4(1)(a) of the EHDS proposal ensures that health professionals shall have access to the electronic health data of natural persons under their treatment. On the other hand, Article 4(3) of the EHDS proposal prohibits that the provider or professional is informed of the content of the electronic health data, even if they are aware of the existence and nature of the restricted electronic health data. In this regard, it lacks clarity in the EHDS proposal as to whether an EHR system should make unavailable the existence and nature of restricted electronic health data to unauthorised health providers and health professionals, or whether it is sufficient to restrict access merely to the content of the restricted electronic health data.

A possible challenge to implementing the 'right to restrict access' in an EHR system maintained by a healthcare provider is that the controller of the patient's electronic health data in their EHR is often the clinic, and not only a single health professional. Furthermore, with reference to Article 3(f) of the 'Directive 2011/24/EU on the application of patients' rights in cross-border healthcare'[667], the concept of 'health professional' encompasses a great variety of professions of distinct nature and requiring different kinds of involvement, decision-making and responsibilities. Therefore, the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' recommended that not all electronic health data be made available to all health professionals indiscriminately, but only to those for which access is deemed necessary and proportionate in order to perform a specific task.[668] The implementation of these principles in the design of an EHR system

[667] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, *see supra* note 554.

[668] EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, *supra* note 635, para. 62.

could be challenging, because access permissions may differ patient-by-patient. For example, when a clinic has a user account on a healthcare platform and makes use of its cloud-based EHR system, then all health professionals affiliated with the clinic should have sub-user accounts in order to guarantee that a health professional may (not) access all or part of the electronic health data of the clinic's patients.

3.7.) Right to obtain information

Article 3(10) of the EHDS proposal:

"Natural persons shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare. The information shall be provided immediately and free of charge through electronic health data access services."

Article 3(10) of the EHDS proposal ensures a new mechanism that enables natural persons to identify potential unlawful access to their electronic health data. In essence, this right to obtain information overlaps with Article 15(1)(c) of the GDPR, which guarantees that the right of access shall include information about "the recipients or categories of recipient to whom the personal data have been or will be disclosed". However, it is not clear from Article 3(10) of the EHDS proposal whether the natural person may exercise the 'right to obtain information' only through electronic health data access services, and whether the data holder shall ensure this right "immediately and free of charge" only when the request is made through an electronic health data access service. Moreover, it is not clear whether the 'right to obtain information' should be ensured by means of an automatic notification procedure whenever there is access to the data, or only possible upon request. In this regard, the 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' recommended the implementation of the first option, as it is the most adequate solution to empower data subjects.[669]

[669] *Ibid*., para. 58.

CONCLUSIONS

Relevance and significance

This study discusses privacy and data protection-related regulatory and compliance challenges posed by digital transformation in healthcare in the wake of the COVID-19 pandemic. As the research project was carried out between November 2019 and October 2022, the study provides an account of the impact of the public health crisis on the increased use of telehealth services. In particular, it focuses on technological, policy and legislative developments relating to two key phenomena: the uptake of IoT-enabled medical devices and digital consumer health products (wellness applications), and the platformisation of healthcare services in the form of online doctor marketplaces and healthcare SaaS platforms. The work fills a gap in literature, because Internet of Health Things and healthcare platforms have not attracted the same level of engagement by legal scholars as other areas of digital health. This lack of attention is a concern considering the number of people affected by the subject matter: as mentioned, there were around 830 million downloads of health and fitness apps in Europe in 2020, while the company group with which the project collaborated had itself more than 750.000 registered doctors on its online doctor marketplaces across Europe in 2022.

According to the results of EU surveys on the subject, the public considers privacy breaches as the most significant risks undermining digital health services, and believe that telehealth entails additional risks. For this reason, the research sought to investigate privacy and data protection-related requirements governing the deployment of IoT-enabled (and AI-supported) telehealth applications. It also examined how privacy and data protection affect healthcare platforms (online doctor marketplaces and healthcare SaaS platforms) regarding their offering of teleconsultation services and their preparations for the European Health Data Space. As the timing of the research project coincided with the EU's legislative actions of drawing a new regulatory landscape for the use of data and digital technologies, the study presents a critical assessment of how these legal proposals (together with existing ones) may affect the implementation of privacy and data protection requirements in the focus areas. The main benefit of conducting an interdisciplinary legal research was that it helped to grasp the forces that influence how legal acts may operate in specific technological and healthcare

contexts. This enabled the analysis to pinpoint normative provisions that suffer from deficiencies when projected into the context of the research.

Internet of Healthcare and its implications in telehealth

The promise of an Internet of Healthcare is that the intelligent interconnection of people, things, data and processes in digital health could increase medical intelligence and support decisions affecting health and well-being. The Internet of Healthcare aims to exploit the new wave of "data in motion" by enhancing and leveraging the availability, interoperability, sharing and analyses of data concerning health. In addition to this, "anytime-and-anywhere connectivity" could shift the delivery of certain healthcare services from clinical settings to remote environments, while the integration of clinical (in-person) and telehealth (virtual) services could lead to the creation of hybrid healthcare models. These developments could drive the "smart transformation" of healthcare from a "traditional", provider-centric and reactive system to a "new", patient-centric, data-driven and partially automated system that provides personalised healthcare, real-time monitoring and response solutions, as well as prospective insights. In turn, this could enable the reorganisation of healthcare from a fee-for-service (capitated) system to a value-based system that measures outcomes and encourages proactive prevention.

The study provided a state-of-the-art overview of the technological aspects of key enabling technologies that are catalysing the development of an Internet of Healthcare in the narrower context of telehealth. This overview focuses on Internet-connected medical devices and digital consumer health products (Internet of Health Things [IoHT] devices), which possess communications and human-physiological and/or –biochemical sensing capabilities. IoHT devices consist of a (physical) hardware device and (physically embedded or externally located) interconnected software. Due to the resource constraints of IoHT devices, IoT-enabled telehealth systems require the integration of external computing resources and data science capabilities. Although the development of more scalable, distributed and adaptive computing may bring a wide range of benefits, further research is required on how shifting computing resources along the "cloud-to-thing continuum" may affect the security of processing in IoT-enabled telehealth systems. On the other hand, the integration of data science capabilities (practically, in the form of AI systems) could help to transform real-world "raw" big data generated by the use of IoHT devices into "smart" and "actionable" data in order to gain new insights into health and well-being. Future analyses could explore

whether there are any privacy and data protection implications of utilising the integration of these technologies in order to create digital representations (virtual simulations) of patients in the form of 'human digital twins'.

Privacy and data protection issues in IoT-enabled (and AI-supported) telehealth

In order to fall under the scope of the general or specific legal regime prescribing safety, health and quality requirements, an IoHT (hardware) device or interconnected software (AI system) needs to be, legally speaking, either a 'product' or a 'medical device'. This qualification also determines the application of corresponding data protection, cybersecurity, information security and AI governance rules. Despite the significance of the matter, it is questionable why only soft law governs many aspects of this qualification assessment. It would be important to define the line between medical devices and wellness applications (digital consumer health products) with more clarity. Furthermore, it would be essential to ensure that the General Product Safety Regulation proposal fulfils its "safety net" function intactly in terms of providing general safety, health and quality requirements for wellness applications (digital consumer health products) and interconnected software not covered by specialised legislations.

If a software interconnected with an IoHT hardware device possesses AI functionalities, then the AI Act proposal may be relevant to its deployment. However, the study explained that the AI Act proposal suffers from flaws when its basic definitions, AI governance functional roles, risk-based approach and other data protection-related provisions are projected to telehealth. Moreover, the study showed that the AI Act proposal lacks interplay with the GDPR and the MDR, because AI-enabled medical devices would be subject to parallel regulatory frameworks. Certain provisions of the AI Act proposal would be supplementary; other provisions would be overlapping, with some of them diverging and potentially conflicting. These may increase compliance costs for manufacturers/providers, which may hinder innovation, and ultimately, deprive European patients from state-of-the-art digital health technologies. Although the healthcare industry has flagged many legislative shortcomings, the research found that the legislative procedure did not integrate effectively stakeholder feedbacks provided during the public consultation. This is a reoccurring problem also in other ongoing EU legislative procedures addressed in this study.

The analysis found that there is a lack of clarity about the link between privacy and data protection in international human rights law (under the framework of the UN and the

Council of Europe) and EU fundamental rights protection, which may affect their consistent application in the context of IoT-enabled telehealth. Under EU law, there is further uncertainty about the scope of 'data concerning health' in IoT-enabled telehealth systems. The study also found that due to the fragmented implementation and interpretation of the GDPR in Member States, the legal bases for processing data concerning health generated by the use of IoHT differ case-by-case depending on the national regulatory framework. Regarding new legislative developments, the study explained that there are inconsistencies between the rights of users to access, use and share data generated by the use of IoHT devices under the Data Act Proposal and the corresponding provisions of the Database Directive and the GDPR. Similarly, the implementation of the Data Governance Act in the context of IoT-enabled telehealth systems raises inconsistencies with the GDPR. Although the EDPB and the EDPS raised concerns about the lack of interplay between these new and existing regulations, the legislative procedures have not addressed their criticisms.

Privacy and data protection matters affecting healthcare platforms

Considering that digital transformation of healthcare requires the implementation of resource-intensive and complex technologies, infrastructures and systems, many healthcare providers opt to use cloud-based applications offered by healthcare online marketplaces and SaaS (Software-as-a-Service) platforms. One of the key functionalities of these healthcare platforms is that they enable users of the platform (patients and healthcare providers) to conduct teleconsultations (online doctor visits) via an integrated video communications API service. In order to allocate legal responsibilities among parties in this context, the study analysed the data protection role of healthcare platforms in relation to healthcare providers and video communications API services providers based on the factual circumstances of the particular case. The study also explained the rationale and demonstrated the key steps of carrying out a data protection impact assessment (DPIA) in this context.

The analysis concluded that the healthcare platform and the video communications API service provider are independent controllers in processing the personal data of the users of the healthcare platform (i.e. patients and health professionals) for establishing a video connection between them. In terms of the processing of the personal data of patients in the course of an online doctor visit, the healthcare provider acts as controller, whereas the healthcare platform is its processor, while the video communications API service provider is a sub-processor. Regarding the customer relationship between the healthcare platform and

the video communications API service provider, the latter acts as controller with respect to the processing of the personal data of the customer's authorised agents and employees. These delineations may assure consistent and comprehensive implementation of data protection rules in teleconsultation. However, it is important to note that slightly different factual circumstances, strategic considerations and legal arguments may lead to a different conclusion in terms of the data protection role of a healthcare platform.

In the second case study, this study analysed the data protection-related implications of the European Health Data Space (EHDS) proposal for an online doctor marketplace that also provides healthcare SaaS functionalities. The analysis found that the definition of 'personal electronic health data' lacks alignment with the definition of 'data concerning health' under the GDPR. Similarly, the rights of natural persons in relation to the primary use of their personal electronic health data under the EHDS proposal lacks interplay with the corresponding rights of data subjects under the GDPR. There is also uncertainty about the interaction between the notions of 'data holder', 'data user' and 'data recipient' under the EHDS proposal with the corresponding notions set forth by the GDPR and the Data Governance Act. In addition to these flaws, the study explained that the definition of 'EHR system' provided by the EHDS proposal is too broad, while the definitions of the two new types of health data access services are misleading and there is lack of clarity about their underlying data governance mechanisms. Overall, in its current state, the EHDS proposal may create significant uncertainties for an online doctor marketplace.

In order to resolve these problems, it would be important that the co-legislators not only address the aforementioned legal deficiencies of the EHDS proposal, but that the EU improves coordination and offers more support. For example, the EDPB and the EDPS underlined in their Joint Opinion that the Commission did not conduct a DPIA on the EHDS proposal. The research also found that the second public consultation came too soon and was too short for stakeholders to give detailed feedbacks on the complex requirements set forth by the EHDS proposal. Furthermore, it would be important to pay greater attention in the drafting process that healthcare across the EU is legally and technically extremely diverse and fragmented. Ultimately, whether the EHDS functions effectively will depend on its technical implementation by the entire European health data ecosystem. Stakeholders such as online doctor marketplaces will need clear guidance and sufficient preparatory time for the technical implementation of the EHDS proposal and the Commission's accompanying implementing act(s). If the EU will not manage this legislative procedure with due care, then,

as the EDPB and the EDPS pointed out, the EHDS proposal may even weaken the protection of the rights to privacy and data protection.

BIBLIOGRAPHY AND LIST OF SOURCES

Legislative sources

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (adopted 8 November 2001, entered into force 1 July 2004), ETS No. 181, Council of Europe, Strasbourg. Available from: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626>.

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, 391–407. ELI: <http://data.europa.eu/eli/treaty/char_2012/oj>.

Commission Regulation (EU) No 207/2012 of 9 March 2012 on electronic instructions for use of medical devices, OJ L 72, 10.3.2012, 28–31. ELI: <http://data.europa.eu/eli/reg/2012/207/oj>.

Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953), ECT No. 5, Council of Europe, Rome. Available from: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985), CETS No. 108, Council of Europe, Strasbourg. Available from: <https://rm.coe.int/1680078b37>.

Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices, OJ L 189, 20.7.1990, 17. ELI: <http://data.europa.eu/eli/dir/1990/385/oj>.

Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12.7.1993, 1. ELI: <http://data.europa.eu/eli/dir/1993/42/oj>.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, 20–28. ELI: <https://data.europa.eu/eli/dir/1996/9/2019-06-06>.

Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices, OJ L 331, 7.12.1998, 1. ELI: <http://data.europa.eu/eli/dir/1998/79/oj>.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce,

in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, 1–16. ELI: <http://data.europa.eu/eli/dir/2000/31/oj>.

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2001, 4. ELI: <http://data.europa.eu/eli/dir/2001/95/2010-01-01>.

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, OJ L 88, 4.4.2011. ELI: <https://data.europa.eu/eli/dir/2011/24/oj>.

Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) vom 09.12.2019 (BGBl. I 2019 S. 2562).

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976), A/RES/21/2200, United Nations Treaty Series 999:171. Available from: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text (128th Session of the Committee of Ministers, 17–18 May 2018), ETS No. 223, Council of Europe, Elsinore. Available from: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>.

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 (23 February 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN>.

Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, Strasbourg (3 May 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197>.

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 (Second Presidency compromise text). Presidency of the Council of the European Union (2021/0106(COD), 11124/22) (15 July 2022). Available from: <https://data.consilium.europa.eu/doc/document/ST-11124-2022-INIT/en/pdf>.

Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council (Mandate for negotiations with the European Parliament). General Secretariat of the Council of the European Union (2021/0170(COD), 11469/22) (20 July 2022). Available from: <https://data.consilium.europa.eu/doc/document/ST-11469-2022-INIT/en/pdf>.

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022) 454 final), Brussels (15 September 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454>.

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, 27.5.2014, 1. ELI: <http://data.europa.eu/eli/reg/2014/536/2014-05-27>.

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), OJ L 119, 4.5.2016, 1–88. ELI: <http://data.europa.eu/eli/reg/2016/679/oj>.

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, OJ L 117, 5.5.2017, 1. ELI: <https://eur-lex.europa.eu/eli/reg/2017/745/oj>.

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117, 5.5.2017, 176. ELI: <https://eur-lex.europa.eu/eli/reg/2017/746/oj>.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, 39. ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, 15. ELI: <http://data.europa.eu/eli/reg/2019/881/oj>.

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, 1–44. ELI: <https://data.europa.eu/eli/reg/2022/868/oj>.

Universal Declaration of Human Rights (adopted 10 December 1948), 217 A (III), Paris. Available from: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale

Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020 (BGBl. I S. 768), die durch Artikel 1 der Verordnung vom 22. September 2021 (BGBl. I S. 4355) geändert worden ist.

Case law

Amann v. Switzerland (no. 27798/95), European Court of Human Rights, Judgment (16 February 2020), ECLI:CE:ECHR:2000:0216JUD002779895. Available from: <https://hudoc.echr.coe.int/eng?i=001-58497>.

Brain Products GmbH v. BioSemi VOF and Others (C-219/11), Opinion of Advocate General Mengozzi (15 May 2012), Court Reports – Court of Justice, ECLI:EU:C:2012:299. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-219/11>.

Brain Products GmbH v. BioSemi VOF and Others (C-219/11), Judgment of the Court (Third Chamber) (22 November 2012), Court Reports – Court of Justice, ECLI:EU:C:2012:742. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-219/11&language=EN>.

Criminal proceedings against Bodil Lindqvist (C-101/01), Court of Justice of the European Communities, Judgment, (6 November 2003), *European Court Reports 2003 I-12971*, ECLI:EU:C:2003:596. CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62001CJ0101>.

EL CORTE INGLÉS, S.A., Agencia Española de Protección de Datos [Data Protection Authority of Spain], case no. E/03882/2020, resolution of 25 May 2020. Available from: <https://www.aepd.es/es/documento/e-03882-2020.pdf>.

Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV (C-40/17), Judgment of the Court (Second Chamber) (29 July 2019), Court Reports – General Court, ECLI:EU:C:2019:629. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-40/17>.

Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP) (C-444/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10549, EU:C:2004:697. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-444/02>.

Fixtures Marketing v Oy Veikkaus AB (C-46/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10365, EU:C:2004:694. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-46/02>.

Fixtures Marketing v Svenska Spel AB (C-338/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10497, EU:C:2004:696. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-338/02>.

Gebruik van warmtebeeldcamera's op de luchthaven Brussels South Charleroi Airport in de strijd tegen COVID-19 [Use of thermal cameras at Brussels South Charleroi Airport in the framework of the fight against COVID-19], Gegevensbeschermingsautoriteit [Data Protection Authority (Belgium)], case no. 47/2022, decision of 4 April 2022. Available from: <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-47-2022.pdf>.

I v. Finland (no. 20511/03), European Court of Human Rights, Judgment (17 July 2008), ECLI:CE:ECHR:2008:0717JUD002051103. Available from: <https://hudoc.echr.coe.int/eng?i=001-87510>.

L'association InterHop et les autres, Conseil d'État [Council of State (France)], case no. 441065, decision of 26 June 2020. Available from: <https://www.conseil-etat.fr/decisions-de-justice/dernieres-decisions/conseil-d-etat-26-juin-2020-cameras-thermiques-a-lisses>.

Laboratoires Lyocentre v Lääkealan turvallisuus– ja kehittämiskeskus, Sosiaali– ja terveysalan lupa– ja valvontavirasto (C-109/12), Opinion of Advocate General Sharpston (30 May 2013), Court Reports – Court of Justice, ECLI:EU:C:2013:353. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-109/12>.

L.H. v. Latvia (no. 52019/07), European Court of Human Rights, Judgment (29 April 2014), ECLI:CE:ECHR:2014:0429JUD005201907. Available from: <https://hudoc.echr.coe.int/fre?i=001-142673>.

M.M. v the United Kingdom (no. 24029/07), European Court of Human Rights, Judgment (13 November 2012), ECLI:CE:ECHR:2012:1113JUD002402907. Available from: <https://hudoc.echr.coe.int/eng?i=001-114517>.

M.S. v. Sweden (no. 74/1996/693/885), European Court of Human Rights, Judgment (27 August 1997). Available from: <https://hudoc.echr.coe.int/eng?i=001-58177>.

METRO BILBAO, S.A., Agencia Española de Protección de Datos [Data Protection Authority of Spain], case no. E/03884/2020, resolution of 24 May 2020. Available from: <https://www.aepd.es/es/documento/e-03884-2020.pdf>.

'Oliver Medical' SIA v Valsts ieņēmumu dienests (C-547/13), Judgment of the Court (Tenth Chamber) (4 March 2015), Court Reports – Court of Justice, ECLI:EU:C:2015:139. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-547/13>.

Qualification opinion on ingestible sensor system for medication adherence as biomarker for measuring patient adherence to medication in clinical trials, European Medicines Agency Committee for Medicinal Products for Human Use (EMA/CHMP/SAWP/513571/2015) (15 February 2016). Available from <https://www.ema.europa.eu/documents/regulatory-procedural-guideline/qualification-

opinion-ingestible-sensor-system-medication-adherence-biomarker-measuring-patient_en.pdf>.

Patrick Breyer v Bundesrepublik Deutschland (C-582/14), Judgment of the Court (Second Chamber) (19 October 2016), Court Reports – Court of Justice, ECLI:EU:C:2016:779. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-582/14>.

S. and Marper v. the United Kingdom (nos. 30562/04 and 30566/04), European Court of Human Rights, Judgment (4 December 2008), ECLI:CE:ECHR:2008:1204JUD003056204. Available from: <http://hudoc.echr.coe.int/eng?i=001-90051>.

Surikov v. Ukraine (no. 42788/06), European Court of Human Rights, Judgment (26 January 2017), ECLI:CE:ECHR:2017:0126JUD004278806. Available from: <https://hudoc.echr.coe.int/eng?i=001-170462>.

Syndicat national de l'industrie des technologies médicales (Snitem), Philips France v Premier ministre, Ministre des Affaires sociales et de la Santé (C-329/16), Opinion of Advocate General Campos Sánchez-Bordona (28 June 2017), Court Reports – Court of Justice, ECLI:EU:C:2017:501. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-329/16>.

Syndicat national de l'industrie des technologies médicales (Snitem), Philips France v Premier ministre, Ministre des Affaires sociales et de la Santé (C-329/16), Judgment of the Court (Fourth Chamber) (7 December 2016), Court Reports – Court of Justice, ECLI:EU:C:2017:947. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-329/16>.

The British Horseracing Board Ltd and Others v William Hill Organization Ltd. (C-203/02), Judgment of the Court (Grand Chamber) (9 November 2004), European Court Reports 2004 I-10415, EU:C:2004:695. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-203/02>.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Judgment of the Court (Grand Chamber) (C-210/16) (5 June 2018), Court Reports – Court of Justice, ECLI:EU:C:2018:388, para. 38. InfoCuria: <https://curia.europa.eu/juris/liste.jsf?num=C-210/16>.

Z v. Finland (no. 22009/93), European Court of Human Rights, Judgment (25 February 1997), ECLI:CE:ECHR:1997:0225JUD002200993. Available from: <https://hudoc.echr.coe.int/eng?i=001-58033>.

Soft law

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) (16 February 2010). Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>

Article 29 Data Protection Working Party, Letter from the Article 29 Working Party addressed to Ms Le Bail to deliver input to the Commission on the current practices at national level, the problems encountered in implementing the Directive as well as some suggestions for improvements or changes in relation to special categories of data ("sensitive data"), notification and the practical implementation of the Article 28(6) of the Directive 95/46/EC, Advice Paper on special categories of data ("sensitive data") (20 April 2011). Available from: <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf>.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203) (2 April 2013). Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP 223) (16 September 2014). Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

Article 29 Data Protection Working Party, Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth, Annex – health data in apps and devices (5 February 2015), 3. Available from: <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf>.

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (4 April 2017 as last revised and adopted 4 October 2017). Available from: <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711>.

Article 29 Data Protection Working Party, Guidelines on the right to data portability (rev. 01) (5 April 2017). Available from: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44099>.

Article 29 Data Protection Working Party, Letter of the Chair of the ART 29 WP to eHEALTH: Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services (11 April 2018). Available

from: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52057>.

Article 29 Data Protection Working Party, Letter of the Chair of the ART 29 WP to mHEALTH: your letter of 7th December 2017 and a new draft code of conduct with the request of a positive opinion from the WP29 under the Data Protection Directive, (11 April 2018). Available from: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52056>.

Bundesamt für Sicherheit in der Informationstechnik (2017): *BSI-Standard 200-2: IT-Grundschutz-Methodik*. Bundesamt für Sicherheit in der Informationstechnik, Bonn. Available from <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html>.

Communication from the Commission on effective, accessible and resilient health systems, COM/2014/215 final, Brussels (4 April 2014). CELEX: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52014DC0215>.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, COM(2017) 228 final, Brussels (10 May 2017). CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017DC0228>.

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, COM/2018/233 final, Brussels (25 April 2018). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:233:FIN>.

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, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066>.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Shaping Europe's digital future", COM(2020) 67 final, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52020DC0067>.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Establishing a European Declaration on Digital rights and principles for the Digital Decade", COM(2022) 27 final, Brussels (26 January 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0027>.

Communication from the Commission to the European Parliament and the Council "A European Health Data Space: harnessing the power of health data for people, patients and innovation", COM(2022) 196 final, Strasbourg (3 May 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0196>.

Commission Notice — The 'Blue Guide' on the implementation of EU products rules 2016, C/2016/1958, OJ C 272, 26.7.2016, 1–149. CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016XC0726(02)>.

Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services Accompanying the document 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions eHealth Action Plan 2012-2020 – innovative healthcare for the 21st century, COM(2012) 736 final - SWD(2012) 413 final' SWD(2012) 414 final, Brussels (6 December 2012). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012SC0414>.

Commission Staff Working Document "Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 147 final", SWD(2018) 146 final, 25 April 2018, 35. Available from: <https://ec.europa.eu/newsroom/dae/redirection/document/51764>.

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"), SWD/2014/0135 final. CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014SC0135>.

Commission Staff Working Document Accompanying the Document '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 COM(2018) 233 final', SWD(2018) 126 final, Brussels (25 April 2018). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0126>.

Commission Staff Working Document Accompanying the Document 'Report from the Commission to the Council and the European Parliament: Final report - Sector inquiry into consumer Internet of Things, COM(2022) 19 final', SWD(2022) 10 final, Brussels (20 January 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0010>.

Commission Staff Working Document Accompanying the Document "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", SWD(2022) 34 final (23 February 2022), 45. CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN>.

Commission Staff Working Document Impact Assessment Report Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final - SEC(2022) 196 final -

SWD(2022) 130 final - SWD(2022) 132 final', SWD(2022) 131 final, Strasbourg (3 May 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0131>.

Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final – SEC(2020) 405 final – SWD(2020) 296 final, SWD(2020) 295 final (25 November 2020). Available from: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71225>.

Council of Europe, 5.1 Steering Committee on Media and Information Society (CDMSI), Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (1342nd meeting, 27 March 2019), Council of Europe, para. 38. Available from: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093397f8>.

Court of Justice of the European Union Research and Documentation Directorate (2021) *Field of Application of the Charter of Fundamental Rights of the European Union*. Court of Justice of the European Union, Luxembourg (March 2021). Available from: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf>.

European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI) (12 July 2019). Available from: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_en.pdf>.

European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (11 March 2021). Available from: <https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf>.

European Data Protection Board, European Data Protection Supervisor, EDPB–EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (18 June 2021). European Data Protection Board, European Data Protection Supervisor, Brussels. Retrieved from <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf>.

European Data Protection Board, European Data Protection Supervisor, 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) (4 May 2022). Available from: <https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf>.

European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space

(12 July 2022). Available from: <https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf>.

EU initiative on a European Health Data Space (EHDS): Public Consultation Factual Summary Report, Ref. Ares(2022)636543 - 27/01/2022. Available from: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Digital-health-data-and-services-the-European-health-data-space/public-consultation_en>.

European Commission (2016) *Clinical Investigation: A Guide for Manufacturers and Notified Bodies under Directives 93/42/EEC or 90/385/EEC. Guidelines on Medical Devices* (MEDDEV 2.7/1 revision 4) (June 2016).

European Commission (n.d.): *Guidance - MDCG endorsed documents and other guidance*. Available from <https://ec.europa.eu/health/md_sector/new_regulations/guidance_en> (accessed 1 October 2022).

European Court of Human Rights (2020) Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence. Council of Europe, Strasbourg (31 August 2020). Available from: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>.

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (v. 2.1) (12 November 2019). Available from: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf>.

European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (21 April 2020). Available from: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf>.

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (v. 1.1) (4 May 2020). Available from: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (2 September 2020). Available from: <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>.

European Data Protection Board, Guidelines 01/2022 on data subject rights - Right of access (18 January 2022). Available from: <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf>.

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission proposals for a Regulation on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and a Regulation on in vitro diagnostic medical devices. Brussels (8 February 2013). Available from <https://edps.europa.eu/sites/default/files/publication/13-02-08_in_vitro_devices_en.pdf>.

European Declaration on Digital Rights and Principles for the Digital Decade, COM(2022) 28 final, Brussels (26 January 2022). CELEX: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2022:28:FIN>.

European Telecommunications Standards Institute (2009) *ETSI TR 102 764 V1.1.1 (2009-02): eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth*. Technical Report. European Telecommunications Standards Institute, Sophia Antipolis. Available from: <https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf>.

European Telecommunications Standards Institute (2020) *ETSI TR 103 477 V1.2.1 (2020-08): eHEALTH; Standardization use cases for eHealth*. Technical Report. European Telecommunications Standards Institute, Sophia Antipolis. Available from: <https://www.etsi.org/deliver/etsi_tr/103400_103499/103477/01.02.01_60/tr_103477v010201p.pdf>.

Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, 17–35. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2007.303.01.0017.01.ENG>.

Federal Institute for Drugs and Medical Devices (2020): *The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V: A Guide for Manufacturers, Service Providers and Users*. Federal Institute for Drugs and Medical Devices, Bonn. Available from <https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.pdf;jsessionid=7AA0A5E8D2A62E1ECC39A3BA06AB1779.intranet351?__blob=publicationFile>.

Federal Institute for Drugs and Medical Devices (2021) *Information on the admissibility of data processing outside Germany in connection with the review procedure of the BfArM pursuant to Section 139e German Social Code Book V (SGB V)*. Federal Institute for Drugs and Medical Devices. Available from <https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/Data_Processing_outside_of_Germany_FAQ.pdf;jsessionid=7AA0A5E8D2A62E1ECC39A3BA06AB1779.intranet351?__blob=publicationFile>.

Formal comments of the EDPS on the Proposal for a Regulation on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council. Available from: <https://edps.europa.eu/system/files/2021-08/21-08-18_comments_product_safety_en.pdf>.

General Product Safety Regulation (GPSR) proposal: summary of the public feedback received after the adoption of the proposal. European Commission letter to the General Secretariat of the Council (26 January 2022). Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5720_2022_INIT&from=EN>.

IEEE Standards Association (2019) *IEEE 2413-2019 - IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*. IEEE Standards Association, Piscataway. Available from: <https://standards.ieee.org/standard/2413-2019.html>.

International Medical Device Regulators Forum (2013) *Software as a Medical Device (SaMD): Key Definitions* (IMDRF/SaMD WG/N10FINAL:2013) (9 December 2013). Available from <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>.

International Organization for Standardization (2013) *ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization, Geneva. Available from <https://www.iso.org/obp/ui/#iso:std:54534:en>.

International Organization for Standardization (2016) *ISO/IEC 29161:2016(en) Information technology — Data structure — Unique identification for the Internet of Things*. International Organization for Standardization, Geneva. Available from <https://www.iso.org/obp/ui/#iso:std:iso-iec:29161>.

International Organization for Standardization (2021) *ISO 13131:2021: Health informatics — Telehealth services — Quality planning guidelines*. International Organization for Standardization, Geneva. Available from <https://www.iso.org/standard/75962.html>.

International Organization for Standardization, International Electrotechnical Commission (2018) *ISO/IEC 30141:2018(en) Internet of Things (loT) — Reference Architecture*. International Organization for Standardization, Geneva. Available from: <https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en>

International Telecommunication Union (2012) *Overview of the Internet of things. Recommendation ITU-T Y.4000/Y.2060 (06/2012)*. International Telecommunication Union, Geneva. Available from: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>.

International Telecommunication Union (2014) *Information technology – Cloud computing – Overview and vocabulary. Recommendation Y.3500 (08/14)*. International Telecommunication Union, Geneva. Available from: <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3500-201408-I!!PDF-E&type=items>.

International Telecommunication Union (2015) *Big data – Cloud computing based requirements and capabilities. Recommendation Y.3600 (11/2015)*. International Telecommunication Union, Geneva. Available from: <https://www.itu.int/rec/T-REC-Y.3600/en>.

International Telecommunication Union (2016) *Requirements of the network for the Internet of things. Recommendation ITU-T Y.4113 (09/2016)*. International Telecommunication Union, Geneva. Available from: <https://www.itu.int/rec/T-REC-Y.4113-201609-I/en>.

Iorga M, Feldman L, Barton R, Martin MJ, Goren N, Mahmoudi, C (2018) *Fog Computing Conceptual Model. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 500-325. U.S. Department of Commerce,

National Institute of Standards and Technology, Washington. DOI: <https://doi.org/10.6028/NIST.SP.500-325>.

Joint Conclusions of the European Parliament, the Council of the European Union and the European Commission on Policy Objectives and Priorities for 2020-2024. 2021/C 451 I/02 (OJ C, C/451, 29.12.2020, 4). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020Y1229(01)>.

Joint Declaration of the European Parliament, the Council of the European Union and the European Commission EU Legislative Priorities for 2022 2021/C. 514 I/01 (OJ C 514I, 21.12.2021, 1–4). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.CI.2021.514.01.0001.01.ENG>.

Medical Device Coordination Group (2019) *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR* (MDCG 2019-11) (11 October 2019). Available from <https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf>

Medical Device Coordination Group (2020) *Guidance on Cybersecurity for medical devices* (MDCG 2019-16 Rev. 1) (July 2020). Available from <https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf>.

Medical Device Coordination Group (2020) *Regulation (EU) 2017/745: Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC. A guide for manufacturers and notified bodies* (MDCG 2020-6) (23 April 2020). Available from <https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2020_6_guidance_sufficient_clinical_evidence_en.pdf>.

Medicines and Healthcare products Regulatory Agency (2021) *Guidance: Medical device stand-alone software including apps (including IVDMDs) v1.08* (8 August 2021). Available from <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/999908/Software_flow_chart_Ed_1-08b-IVD.pdf>.

mHealth Belgium (n.d.) *Technical file that describes the M2 criteria*. mHealth Belgium. Available from <https://mhealthbelgium.be/images/downloads/Criteria-mHealth-apps-ENv5.pdf> (accessed 1 October 2022).

Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (adopted by the Committee of Ministers at the 1342nd meeting of the Ministers' Deputies, 27 March 2019), Council of Europe. Available from: <https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e>.

Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics", COM(2020) 64 final, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0064>.

Statement by Mr. Joseph Cannataci, Special Rapporteur on the right to privacy (1 March 2019) (United Nations Human Rights Council, Fortieth session, 25 February – 22 March 2019), Geneva. Available from: <https://www.ohchr.org/Documents/Issues/Privacy/StatementHRC_40_Privacy.pdf>.

United Nations Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (28 September 1984), E/CN.4/1985/4. Available from: <https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf>.

United Nations General Assembly, Report of the Special Rapporteur on the right to privacy (5 August 2019), A/74/277. Available from: <https://undocs.org/A/74/277>.

United Nations Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (Thirty-second session, 8 April 1988) (henceforth: 'General Comment No. 16'). Available from: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en>.

United Nations Human Rights Committee, General Comment No. 29: States of Emergency (Article 4) (31 August 2001), CCPR/C/21/Rev.1/Add.11. Available from: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.11&Lang=en>.

United Nations Human Rights Committee, Statement on derogations from the Covenant in connection with the COVID-19 pandemic (30 April 2020), CCPR/C/128/2. Available from: <https://www.ohchr.org/Documents/HRBodies/CCPR/COVIDstatementEN.pdf>.

United Nations Human Rights Office of the High Commissioner, Emergency Measures and COVID-19: Guidance (27 April 2020). Available from: <https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf>.

United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, Recommendation on the Protection and Use of Health-related Data (5 December 2019). Available from: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf>.

United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, Explanatory Memorandum to the Recommendation on the Protection and Use of Health-related Data (4 October 2019), Geneva. Available from: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf>.

White Paper "On Artificial Intelligence - A European approach to excellence and trust", COM(2020) 65 final, Brussels (19 February 2020). CELEX: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065>.

Books, articles and other publications

Aceto G, Persico V, Pescapé A (2020) Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *Journal of Industrial Information Integration* 18:100129. DOI: <https://doi.org/10.1016/j.jii.2020.100129>.

Aggarwal AK, Travers S (2001) E-commerce in healthcare: changing the traditional landscape. *Journal of Healthcare Information Management* 15(1):25–36. Available from: <https://pubmed.ncbi.nlm.nih.gov/11338906>.

Ahmadi H, Arji G, Shahmoradi L, Safdari R, Nilashi M, Alizadeh M (2019) The application of internet of things in healthcare: a systematic literature review and classification. *Universal Access in the Information Society* 18:837–869. DOI: <https://doi.org/10.1007/s10209-018-0618-4>.

Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials* 17(4):2347–2376. DOI: <https://doi.org/10.1109/COMST.2015.2444095>

Al-Jaroodi J, Mohamed N, Abukhousa E (2020) Health 4.0: On the Way to Realizing the Healthcare of the Future. *IEEE Access* 8:211189–211210. DOI: <https://doi.org/10.1109/ACCESS.2020.3038858>.

Alliance for Internet of Things Innovation (AIOTI) (2021) *Feedback from Alliance for Internet of Things Innovation*. Feedback to Artificial intelligence – ethical and legal requirements. Alliance for Internet of Things Innovation, Brussels (2 August 2021), 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665207_en>.

Andreu Y, Chiarugi F, Colantonio S *et al*. (2016) Wize Mirror – a smart, multisensory cardio-metabolic risk monitoring system. *Computer Vision and Image Understanding* 148:3–22. DOI: <https://doi.org/10.1016/j.cviu.2016.03.018>.

Anmulwar S, Gupta AK, Derawi M (2020) Challenges of IoT in Healthcare. *In*: Gupta N, Paiva S (eds) *IoT and ICT for Healthcare Applications*. Springer, Cham, 11–20. DOI: <https://doi.org/10.1007/978-3-030-42934-8_2>.

Arrieta AB, Díaz-Rodríguez N, Del Ser J *et al*. (2020) Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion* 58:82–115. DOI: <https://doi.org/10.1016/j.inffus.2019.12.012>.

AstraZeneca (2021) *Feedback provided by AstraZeneca: Artificial intelligence – ethical and legal requirements*. Feedback to Artificial intelligence – ethical and legal requirements. AstraZeneca, Groot Bijgaarden (4 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665331_en>.

Auffray C, Balling R, Barroso I *et al*. (2016) Making sense of big data in health research: Towards an EU action plan. *Genome Medicine* 8(71):1–13. DOI: <https://doi.org/10.1186/s13073-016-0323-y>.

Azimi I, Rahmani AM, Liljeberg P, Tenhunen H (2017) Internet of things for remote elderly monitoring: a study from user-centered perspective. *Journal of Ambient Intelligence and Humanized Computing* 8:273–289. DOI: <https://doi.org/10.1007/s12652-016-0387-y>.

Baker SB, Xiang W, Atkinson I (2017) Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* 5:26521–26544. DOI: <https://doi.org/10.1109/ACCESS.2017.2775180>.

Bayer (2021) *Feedback from Bayer*. Feedback to Artificial intelligence – ethical and legal requirements. Bayer, Leverkusen (29 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663359_en>.

BBC (2022) *Cambridge: Artificial pancreas hailed success for diabetic children*. BBC (20 January 2022). Available from: <https://www.bbc.com/news/uk-england-cambridgeshire-60069369>.

Beckers R, Kwade Z, Zanca F (2021) The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. *Physica Medica* 83:1–8. DOI: <https://doi.org/10.1016/j.ejmp.2021.02.011>.

Beregi R, Pedone G, Mezgár I (2019) A novel fluid architecture for cyber-physical production systems. *International Journal of Computer Integrated Manufacturing* 32(4–5):340–351. DOI: <https://doi.org/10.1080/0951192X.2019.1571239>

Bestsennyy O, Gilbert G, Harris A, Rost J (2021) *Telehealth: A quarter-trillion-dollar post-COVID-19 reality?* McKinsey & Company (9 July 2021). Available from: <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>.

BEUC – The European Consumer Organisation, ANEC – European Association for the Co-ordination of Consumer Representation in Standardisation (2020) *BEUC and ANEC views for a modern regulatory framework on product safety: Achieving a higher level of consumer safety through a revision of the General Product Safety Directive*. Feedback to General Product Safety Directive – review. BEUC–ANEC, Brussels (26 August 2020). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review/F545598_en>.

BEUC – The European Consumer Organisation (2021) *Regulating AI to Protect the Consumer: Position Paper on the AI Act*. Feedback to Artificial intelligence – ethical and legal requirements. BEUC – The European Consumer Organisation, Brussels (7 October 2021). Available from <https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf>.

Beyrouthy, T, Al Kork S, Korbane JA, Abouelela A (2017) EEG Mind Controlled Smart Prosthetic Arm – A Comprehensive Study. *Advances in Science, Technology and Engineering Systems Journal* 2(3):891–899. DOI: <https://doi.org/10.25046/aj0203111>.

Bhaskar S, Bradley S, Chattu VK *et al*. (2020) Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). *Frontiers in Public Health* 8(556720):1–15. DOI: <https://doi.org/10.3389/fpubh.2020.556720>.

Bhat PI (2019) *Idea and Methods of Legal Research*. Oxford University Press, New Delhi. DOI: <https://doi.org/10.1093/oso/9780199493098.001.0001>.

Bianchini E, Francesconi M, Testa M, Tanase M, Gemignani V (2019) Unique device identification and traceability for medical software: A major challenge for manufacturers in an ever-evolving marketplace *Journal of Biomedical Informatics* 93:103150. DOI: <https://doi.org/10.1016/j.jbi.2019.103150>.

Bincoletto G (2021) *Data Protection by Design in the E-Health Care Sector: Theoretical and Applied Perspectives*. Nomos, Baden-Baden. Available from: <https://www.nomos-elibrary.de/10.5771/9783748929895.pdf.

Biswas AR, Dupont C, Pham C (2017) IoT, Cloud and BigData Integration for IoT Analytics. *In*: Soldatos J (ed) *Building Blocks for IoT Analytics*. River Publishers, Aalborg, 11–38. DOI: <https://doi.org/10.13052/rp-9788793519046>.

Bogucki A, Engler A, Perarnaud C, Renda A (2022) *The AI Act and emerging EU digital acquis: Overlaps, gaps and inconsistencies*. CEPS, Brussels (14 September 2022). Available from <https://www.ceps.eu/download/publication/?id=37468&pdf=CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf>.

Bojanova I, Hurlburt G, Voas J (2014) Imagineering an Internet of Anything. *Computer* 47(6):72–77. DOI: <https://doi.org/10.1109/MC.2014.150>.

Bradley J, Barbier J, Handler D (2013) *Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience*. White Paper. CISCO Internet Business Solutions Group, San Jose. Available from: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf>.

Bresnick J (2016) *Can Healthcare Exploit the $7 Trillion Internet of Everything?* Health IT Analytics (19 December 2016). Available from: <https://healthitanalytics.com/news/can-healthcare-exploit-the-7-trillion-internet-of-everything>.

Brkan M (2019) The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal 20*(6):864–883. DOI: <https://doi.org/doi:10.1017/glj.2019.66>

Brown D (2020) *Are Germany's DiGAs the Blueprint for DTx Reimbursement in Europe?* Smart Patient (2 December 2021). Available from <https://www.smartpatient.eu/blog/frontiers-health-2020-germanys-diga-as-blueprint-for-european-dtx-reimbursement>.

Bryson JJ (2022) *Europe Is in Danger of Using the Wrong Definition of AI*. Wired (2 March 2022). Available from <https://www.wired.com/story/artificial-intelligence-regulation-european-union>.

Busch-Vishniac IJ (1999) *Electromechanical Sensors and Actuators*. New York, Springer. DOI: <https://doi.org/10.1007/978-1-4612-1434-2_1>.

Carfagno J (2019) *First AI Medical Monitoring Wearable Approved by FDA for Home Use.* DocWireNews (24 April 2019). Available from: <https://www.docwirenews.com/docwire-pick/future-of-medicine-picks/first-ai-wearable-approved-by-fda-for-home-use-monitoring-vitals>.

Catarinucci L, Donno DD, Mainetti L *et al*. (2015) An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal* 2(6):515–526. DOI: <https://doi.org/10.1109/JIOT.2015.2417684>.

Centre for Data Ethics and Innovation (2021) *Unlocking the value of data: Exploring the role of data intermediaries. An exploration of the role intermediaries could play in supporting responsible data sharing*. Centre for Data Ethics and Innovation, London (22 July 2021). Available from <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf>.

CEPS, ICF, Wavestone (2021) *Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe.* Final Report. European Commission Directorate-General for Communications Networks, Content and Technology, Brussels. Available from <https://op.europa.eu/s/whEA>.

Chanchaichujit J, Tan A, Meng F, Eaimkhong S (2019) An Introduction to Healthcare 4.0. *In*: Chanchaichujit J, Tan A, Meng F, Eaimkhong S (eds) *Healthcare 4.0: Next Generation Processes with the Latest Technologies*. Palgrave Pivot, Singapore, 1–15. Available from: <https://doi.org/10.1007/978-981-13-8114-0_1>.

Chandel RS, Sharma S, Kaur S, Singh S, Kumar R (2022) Smart watches: A review of evolution in bio-medical sector. *Materials Today: Proceedings* 50(5):1053–1066. DOI: <https://doi.org/10.1016/j.matpr.2021.07.460>.

Chapple C (2021) *Mobile Health & Fitness App Spending Jumped 70% Last Year in Europe to a Record $544 Million*. Sensor Tower (January 2021). Available from: <https://sensortower.com/blog/european-health-and-fitness-app-growth-2020>.

CMS (2020) *CMS Expert Guide to digital health apps and telemedicine*. CMS. Available from: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-digital-health-apps-and-telemedicine>.

Comandé G (2020) Italy. *In*: Nys H (ed) *International Encyclopaedia of Laws: Medical Law*. Kluwer Law International, Alphen aan den Rijn. Available from: <https://kluwerlawonline.com/EncyclopediaChapter/IEL+Medical+Law/MEDI201900018>.

Csizmadia I, Láng R, Kis M (2020) *D5.1 - Report on policy action on innovative use of big data in health*. Information note: WP5 Innovative Use of Health data (v. 0.3) (2 February 2020). 17th eHealth Network meeting (June 2020). eHAction: Joint Action to support the eHealth Network. Available from: <http://ehaction.eu/wp-content/uploads/2020/08/03.06.2020_eHN-adopted_eHAction-D5.1-Report-on-policy-action-on-innovative-use-of-big-data-in-health_v0.3-1.pdf>.

Cummins G (2021) Smart pills for gastrointestinal diagnostics and therapy. *Advanced Drug Delivery Reviews* 177(113931):1–22. DOI: <https://doi.org/10.1016/j.addr.2021.113931>.

Da Costa CA, Pasluosta CF, Eskofier B, da Silva DB, da Rosa Righi R (2018) Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards. *Artificial Intelligence in Medicine* 89:61–69. DOI: <https://doi.org/10.1016/j.artmed.2018.05.005>

Dei M, Aymerich J, Poitto M, Bruschi P, Javier del Campo F, Serra-Graells F (2019) CMOS Interfaces for Internet-of-Wearables Electrochemical Sensors: Trends and Challenges. *Electronics* 8(2):150. DOI: <https://doi.org/10.3390/electronics8020150>.

Deloitte Centre of Health Solutions (2020) *Digital transformation: Shaping the future of European healthcare*. Deloitte Centre of Health Solutions, London. Available from: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-shaping-the-future-of-european-healthcare.pdf>.

Dey N, Ashour AS, Bhatt C (2017) Internet of Things Driven Connected Healthcare. *In*: Bhatt C, Dey N, Ashour AS (eds) *Internet of Things and Big Data Technologies for Next Generation Healthcare*. Springer, Cham, 3–12. DOI: <https://doi.org/10.1007/978-3-319-49736-5_1>.

DIGITALEUROPE (2019) *Reflection Paper on regulatory frameworks for digital health technologies in Europe*. DIGITALEUROPE, Brussels (5 April 2019). Available from <https://www.digitaleurope.org/resources/reflection-paper-on-regulatory-frameworks-for-digital-health-technologies-in-europe>.

DIGITALEUROPE (2021) *DIGITALEUROPE's initial findings on the proposed AI Act*. Feedback to Artificial intelligence – ethical and legal requirements. DIGITALEUROPE, Brussels (10 August 2021). Available from <https://www.digitaleurope.org/resources/digitaleuropes-initial-findings-on-the-proposed-ai-act>.

DIGITALEUROPE (2022) *DIGITALEUROPE comments on the proposed General Product Safety Regulation*. DIGITALEUROPE, Brussels (18 January 2022). Available from <https://www.digitaleurope.org/resources/digitaleurope-comments-on-the-proposed-general-product-safety-regulation>.

DigitalHealthEurope, Kolitsi Z, Kalra D, Wilson P *et al*. (2021): *DigitalHealthEurope recommendations on the European Health Data Space. Supporting responsible health data sharing and use through governance, policy and practice*. DigitalHealthEurope.

Available from <https://digitalhealtheurope.eu/wp-content/uploads/DHE_recommendations_on_EHDS_July_2021.pdf>.

Digital Therapeutics Alliance (2021) *Digital Therapeutics Alliance Consultation Response: Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements (6 August 2021). Digital Therapeutics Alliance, Brussels. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665561_en>.

Dinc E, Kuscu M, Bilgin BA, Akan OB (2019) Internet of Everything: A Unifying Framework Beyond Internet of Things *In*: Cardoso PJS, Monteiro J, Semião J *et al*. (eds) *Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities*. IGI Global, Hershey, 1–30. DOI: <https://10.4018/978-1-5225-7332-6.ch001>.

Dobinson I, Johns F (2017) Legal Research as Qualitative Legal Research. *In*: McConville M, Chui WH (eds) *Research Methods for Law* (Second Edition). Edinburgh University Press, Edinburgh, 18–47. DOI: <https://www.jstor.org/stable/10.3366/j.ctt1g0b16n.7>.

Docksey C, Hijmans H (2019) The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law. *European Data Protection Law Review* 5(3):300–316. DOI: <https://doi.org/10.21552/edpl/2019/3/6>.

Doom L (2020) *Will the MDR improve regulatory oversight of AI solutions?* Aidence, Amsterdam (30 June 2020). Available from: <https://www.aidence.com/articles/mdr-oversight-of-ai-solutions>.

Dove ES, Chen J (2020) To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices? *European Journal of Risk Regulation The Journal of Law, Medicine & Ethics* 48(S1):187–195. DOI: <https://doi.org/10.1177/1073110520917046>.

Drexl J, Banda C, Otero BG *et al*. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act).* Max Planck Institute for Innovation and Competition, Munich. Available from: <https://pure.mpg.de/rest/items/item_3388757/component/file_3395639/content>.

eHAction (2021) *Interoperability Guide*. eHAction. Available from: <https://ehaction.eu/interoperability-guide/about-the-guide/#titulo2>.

Eidel O (2022) *MDR Class 1 Devices: Do They Exist (as software)?* OpenRegulatory (updated 29 September 2022). Available from: <https://openregulatory.com/do-software-mdr-class-1-devices-exist>.

EIT Health (2021) *EIT Health AI consultation response*. Feedback to Artificial intelligence – ethical and legal requirements (29 July 2021). EIT Health, Munich. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663361_en>.

Elhayatmy G, Dey N, Ashour AS (2018) Internet of Things Based Wireless Body Area Network in Healthcare. *In*: Dey N, Hassanien AE, Bhatt C (eds) *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. Springer, Cham, 3–20. DOI: <https://doi.org/10.1007/978-3-319-60435-0_1>.

Emerline (2020) *Marketplace Platforms for Healthcare to Foster Medical and Insurance Processes*. Emerline, Mountain View (16 June 2020). Available from: <https://emerline.com/blog/marketplace-platforms-for-healthcare-to-foster-medical-and-insurance-processes>.

Eurofound (2021) *Living, working and COVID-19 dataset*. Eurofound, Dublin (5 July 2021). Available from: <https://www.eurofound.europa.eu/data/covid-19/quality-of-public-services>.

European Association of Hospital Pharmacists (2021) *Feedback from European Association of Hospital Pharmacists*. Feedback to Artificial intelligence – ethical and legal requirements (2 August 2021). European Association of Hospital Pharmacists, Brussels. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665208_en>.

European Cancer Organisation (2021) *Feedback from European Cancer Organisation*. Feedback to Artificial intelligence – ethical and legal requirements. European Cancer Organisation, Brussels (6 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665530_en>.

European Commission (n.d.) *eHealth and COVID-19*. European Commission website. Available from <https://health.ec.europa.eu/ehealth-digital-health-and-care/ehealth-and-covid-19_en> (accessed 1 October 2022).

European Commission (n.d.) *Electronic cross-border health services*. European Commission. Available from: <https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en> (accessed 1 October 2022).

European Commission (n.d.) *Public Health: Overview*. European Commission website. Available from <https://ec.europa.eu/health/ehealth-digital-health-and-care/overview_en> (accessed 1 October 2022).

European Commission Directorate-General for Communications Networks, Content and Technology (2018) *Consultation: Transformation health and care in the digital single market. Synopsis report*. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2759/18589>.

European Commission Directorate-General for Communications Networks, Content and Technology (2020) *Shaping the Digital Transformation in Europe*. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2759/294260>.

European Commission Directorate-General for Communications Networks, Content and Technology, Karanikolova K, Chicot J, Gkogka A *et al*. (2018) *Study in support of the*

evaluation of Directive 96/9/EC on the legal protection of databases. Annex 1: In-depth analysis of the Database Directive, article by article. Publications Office of the European Union, Luxembourg, 60. DOI: <https://data.europa.eu/doi/10.2759/04895>.

European Commission Directorate-General for Communications Networks, Content and Technology, Hartmann C, Allan J, Hugenholtz P *et al*. (2020) *Trends and developments in artificial intelligence : challenges to the intellectual property rights framework.* Final report. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2759/683128>.

European Commission Directorate-General for Communications Networks, Content and Technology, Peijl S, Denny E, Koring E *et al*. (2020) Study to support an impact assessment on enhancing the use of data in Europe. Report on Task 1 – Data governance. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2759/759296>.

European Commission Directorate-General for Communications Networks, Content and Technology, PwC (2021) *Study on eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union Lot 2: Artificial Intelligence for health and care in the EU.* Final Study Report. Publications Office of the European Union, Luxembourg. Available from: <https://ec.europa.eu/newsroom/dae/redirection/document/80948>.

European Commission Directorate-General for Communications Networks, Content and Technology, Maier N, De Michiel F, Peter V *et al*. (2022) *Study to support an impact assessment for the review of the database directive.* Final report. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2759/647387>.

European Commission Directorate-General for Health and Food Safety (2018) *Market study on telemedicine*. Publications Office of the European Union, Luxembourg. DOI: <https://health.ec.europa.eu/system/files/2019-08/2018_provision_marketstudy_telemedicine_en_0.pdf>.

European Commission Directorate-General for Health and Food Safety (2022) *State of Health in the EU: Companion report 2021*. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2875/835293>.

European Commission Directorate-General for Health and Food Safety, Lupiáñez-Villanueva F, Gunderson L, Vitiello S (2022) *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2875/702007>.

European Commission Directorate-General for Justice and Consumers, Civic Consulting (2021) *Study for the preparation of an Implementation Report of the General Product Safety Directive.* Final report. Part 1: Main report. European Commission, Brussels (29 September 2021). Available from <https://ec.europa.eu/info/sites/default/files/final_report-gpsd-part1-main_report-final-corrected2.pdf>.

European Commission Directorate-General for the Information Society and Media (Sundmaeker H, Guillemin P, Friess P, Woelfflé S (eds) (2010) *Vision and Challenges for Realising the Internet of Things*). Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2759/26127>.

European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry (COCIR) (2021) *COCIR Feedback: Commission proposal for a European Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry, Brussels (2 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2660588_en>.

European Federation of Pharmaceutical Industries and Associations (EFPIA) (2021) *EFPIA Position Paper on Artificial Intelligence*. Feedback to Artificial intelligence – ethical and legal requirements (30 July 2021). European Federation of Pharmaceutical Industries and Associations, Brussels. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663395_en>.

European Observatory on Health Systems and Policies *et al*. (2021) *Use of digital health tools in Europe: before, during and after COVID-19*. World Health Organization Regional Office for Europe, Copenhagen. Available from: <https://apps.who.int/iris/handle/10665/345091>.

European Patients' Forum (EPF) (2021) *EPF's Response & Accompanying Statement: Public consultation on the White Paper on Artificial Intelligence*. Feedback to Artificial intelligence – ethical and legal requirements. European Patients' Forum, Brussels (6 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665528_en>.

European Patients' Forum (EPF) (2021) *Public consultation on European Health Data Space – EPF accompanying paper*. Feedback to Artificial intelligence – ethical and legal requirements. European Patients' Forum, Brussels (26 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665528_en>

European Society of Radiology (2021) *ESR Statement: European Commission proposal for a European Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. European Society of Radiology, Vienna (2 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665222_en>.

Evans D (2012) *The Internet of Everything: How More Relevant and Valuable Connections Will Change the World*. CISCO Internet Business Solutions Group, San Jose. Available from: <https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf>.

Fan K, Jiang W, Li H, Yang Y (2018) Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE Transactions on Industrial Informatics* 14(4):1656–1665. DOI: <https://doi.org/10.1109/TII.2018.2794996>.

Fortune Business Insights (2021) *Telemedicine Market Size, Share & COVID-19 Impact Analysis, By Type (Products and Services), By Modality (Store-and-forward (Asynchronous), Real-time (Synchronous), and Others), By Application (Teleradiology, Telepathology, Teledermatology, Telecardiology, Telepsychiatry, and Others), By End User (Healthcare Facilities and Homecare), and Regional Forecast, 2020-2027.* Fortune Business Insights. Available from: <https://www.fortunebusinessinsights.com/industry-reports/telemedicine-market-101067>.

Fraden J (2015) *Handbook of Modern Sensors: Physics, Designs, and Applications* (Fifth Edition). Cham, Springer. DOI: <https://doi.org/10.1007/978-3-319-19303-8_1>.

Friedel E, Goraya T (2018) *CJEU rules on prescription support software as a medical device.* Taylor Wessing (March 2018). Available from: <https://www.taylorwessing.com/synapse/march18.html>.

Fuster GG (2014) Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection. *Birkbeck Law Review* 2(2):263–278. Available from: <http://www.bbklawreview.org/uploads/1/4/5/4/14547218/263_fighting-for-your-right-to-what-exactly_2-2.pdf>.

Fuster GG, Gutwirth S (2014) A legal tool for the prospective assessment of EU fundamental rights compliance. *In*: Fuster GG, Gutwirth S, Somody B, Székely I (eds) *Consolidated legal report on the relationship between security, privacy and personal data protection in EU law* (Deliverable 5.2). The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making (PRISMS), 9–27. Available from: <https://www.researchgate.net/publication/289539808_Consolidated_legal_report_on_the_relationship_between_security_privacy_and_personal_data_protection_in_EU_law_PRISMS_Deliverable_52>.

Fuster GG, Hijmans H (2019) The EU rights to privacy and personal data protection: 20 years in 10 questions (Discussion paper). *Exploring the Privacy and Data Protection connection: International Workshop on the Legal Notions of Privacy and Data Protection in EU Law in a Rapidly Changing World* (14 May 2019). Available from: <https://cris.vub.be/files/45839230/20190513.Working_Paper_Gonza_lez_Fuster_Hijmans_3_.pdf>.

Garattini L, Badinella Martini M, Mannucci PM (2021) Improving primary care in Europe beyond COVID-19: from telemedicine to organizational reforms. *Internal and Emergency Medicine* 16:255–258. DOI: <https://doi.org/10.1007/s11739-020-02559-x>.

Gellert R, Gutwirth S (2013) The legal construction of privacy and data protection. *Computer Law & Security Review* 29(5):522–530 at 526–527. DOI: <https://doi.org/10.1016/j.clsr.2013.07.005>.

Gerke S (2021) Health AI for Good Rather Than Evil? The Need for a New Regulatory Framework for AI-Based Medical Devices. *Yale Journal of Health Policy, Law, and Ethics* 20(2):432–512. Available from: <https://yaleconnect.yale.edu/get_file?pid=fd7fce9fbc17724a4b17d7f1ce4581a33c87d962fbbae12115c3217cdb56240>.

German Medical Technology Association (BVMed) (2021) *BVMed positions on the draft of the "Artificial Intelligence Act" (AIA)*. Feedback to Artificial intelligence – ethical and legal requirements. BVMed, Berlin (5 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665476_en>.

Gesundheit Österreich Forschungs- und Planungs (2016) *Study on Big Data in Public Health, Telemedicine and Healthcare*. Final Report. Publications Office of the European Union, Luxembourg. Available from: <https://op.europa.eu/s/w3wW>.

Giacalone A, Marin L, Febbi M, Franchi T, Tovani-Palone MR (2022) eHealth, telehealth, and telemedicine in the management of the COVID-19 pandemic and beyond: Lessons learned and future perspectives. *World Journal of Clinical Cases* 10(8):2363–2368. DOI: <https://doi.org/10.12998/wjcc.v10.i8.2363>.

Giannoutakis KM, Spanopoulos-Karalexidis M, Papadopoulos CKF, Tzovaras D (2020) Next Generation Cloud Architecture. *In*: Lynn PT, Mooney J, Lee B, Endo P (eds) *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles*. Palgrave Macmillan, Cham, 23–39. DOI: <https://doi.org/10.1007/978-3-030-41110-7_2>.

GlobalData Healthcare (2021) *France to enable rapid market access for digital therapeutics*. Healthcare IT News (5 February 2021). Available from <https://www.healthcareitnews.com/news/emea/france-enable-rapid-market-access-digital-therapeutics>.

Google (2020) *Google's response to the Inception Impact Assessment (IIA) on the General Product Safety Directive*. Feedback to General Product Safety Directive – review. Google, Brussels (1 September 2020). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review/F547535_en>.

Google (2021) *Consultation on the EU AI Act Proposal: Google's submission*. Feedback to Artificial intelligence – ethical and legal requirements. Google, Brussels (15 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662492_en>.

Goraya T (2019) *Border issues: medical devices, wellbeing and lifestyle apps*. Taylor Wessing (1 March 2019). Available from: <https://www.taylorwessing.com/interface/2019/bodytech/border-issues-medical-devices-wellbeing-and-lifestyle-apps>.

Greco L, Percannella G, Ritrovato P (2020) Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern Recognition Letters* 135:346–353. DOI: <https://doi.org/10.1016/j.patrec.2020.05.016>.

Hashiguchi TCO (2020) *Bringing health care to the patient: An overview of the use of telemedicine in OECD countries*. OECD Health Working Paper No. 116, OECD Publishing, Paris. DOI: <https://doi.org/10.1787/8e56ede7-en>.

Healthcare Information and Management Systems Society (2017) *HIMSS Dictionary of Health Information Technology Terms, Acronyms, and Organizations* (Fourth Edition). CRC Press, Boca Raton.

HelloFuture (2022) *Generative AI: a new approach to overcome data scarcity*. HelloFuture (21 March 2022). Available from <https://hellofuture.orange.com/en/generative-ai-a-new-approach-to-overcome-data-scarcity>.

Hersh W (2009) A stimulus to define informatics and health information technology. *BMC Medical Informatics and Decision Making* 9(24):1–6. DOI: <https://doi.org/10.1186/1472-6947-9-24>.

High-Level Expert Group on Artificial Intelligence (2018) *A definition of AI: Main capabilities and scientific disciplines*. European Commission, Brussels (18 December 2018). Available from: <https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf>.

HIMSS – Healthcare Information and Management Systems Society (2020) *eHealth Study: Non-clinical Telehealth Services Are Most Prevalent, but COVID-19 Accelerates New Trends*. HIMSS, Chicago (7 July 2020). Available from: <https://www.himss.org/news/ehealth-study-non-clinical-telehealth-services-are-most-prevalent-covid-19-accelerates-new>.

HIMSS – Healthcare Information and Management Systems Society (2020) *Interoperability in Healthcare*. HIMSS, Chicago (4 August 2020). Available from: <https://www.himss.org/resources/interoperability-healthcare>.

Hoffmann La Roche (2021) *Roche feedback to the European Commission's proposed Regulation of Artificial Intelligence (the "AI Act")*. Feedback to Artificial intelligence – ethical and legal requirements. Hoffmann La Roche, Basel (30 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665165_en>.

Hoyt R, Muenchen R (2019) Artificial Intelligence. *In*: Hoyt R, Muenchen R (eds) *Introduction to Biomedical Data Science*. Informatics Education, Pensacola, 191–214.

Hutchinson T (2017) Doctrinal research: Researching the jury. *In*: Watkins D, Burton M (eds) *Research Methods in Law* (Second Edition). Routledge, Abingdon, 7–33. DOI: <https://doi.org/10.4324/9781315386669>.

Ienca M, Andorno R (2017) Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy* 13(5):1–27. DOI: <https://doi.org/10.1186/s40504-017-0050-1>.

Indrakumari R, Poongodi T, Suresh P, Balamurugan B (2020) The growing role of Internet of Things in healthcare wearables. *In*: Balas VE, Solanki VK, Kumar R (eds) *Emergence*

of Pharmaceutical Industry Growth with Industrial IoT Approach. Academic Press, London, 163–194. DOI: <https://doi.org/10.1016/B978-0-12-819593-2.00006-6>.

Inside Tech Media (2019) *IoT Update: Are Wearables Medical Devices Requiring a CE-Mark in the EU?* Covington (18 January 2019). Available from: <https://www.insidetechmedia.com/2019/01/18/iot-update-wearables-medical-devices-requiring-a-ce-mark-in-the-eu>.

International Telecommunication Union (2005) *ITU Internet Reports 2005: The Internet of Things*. International Telecommunication Union, Geneva. Available from: <http://handle.itu.int/11.1002/pub/800eae6f-en>.

IoT Business News (2019) *World's first IoT 'device-to-cloud' solution announced*. IoT Business News (27 November 2019). Available from: <https://iotbusinessnews.com/2019/11/27/50213-worlds-first-iot-device-to-cloud-solution-announced>.

i-Scoop (n.d.) *What the Internet of Everything really is – a deep dive*. i-Scoop. Available from: <https://www.i-scoop.eu/internet-of-things-iot/internet-of-everything-2> (accessed 1 October 2022).

Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak, KS (2015) The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* 3:678–708. DOI: <https://doi.org/10.1109/ACCESS.2015.2437951>.

Jia X, Feng Q, Fan T, Lei Q (2012) RFID technology and its applications in Internet of Things (IoT). *In: 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, (Yichang, 21–23 April 2012), 1282–1285. DOI: <https://10.1109/CECNet.2012.6201508>.

Johner C (2017) *MDR Classification Rule 11 for Medical Device Software.* Johner Institute (22 July 2017). Available from: <https://www.johner-institute.com/articles/regulatory-affairs/and-more/mdr-rule-11-software>.

Kavlakoglu E (2020) *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?* IBM (27 May 2020). Available from: <https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks>.

Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K (2015) Dynamic consent: a patient interface for twenty-first century research networks *European Journal of Human Genetics* 23:141–146. DOI: <https://doi.org/10.1038/ejhg.2014.71>.

Kelly B (2012) *CJEU Clarifies Medical Device Borderline.* Covington: Inside EU Life Sciences (26 December 2012). Available from: <https://www.insideeulifesciences.com/2012/12/26/cjeu-clarifies-medical-device-borderline>.

Khalil S, Bou Abdo J (2022) Healthcare 4.0: Technologies and Policies. *In*: Makhoul A, Demerjian J, Bou Abdo J (eds) *5G Impact on Biomedical Engineering: Wireless Technologies Applications*. CRC Press, Boca Raton, 3–17. DOI: <https://doi.org/10.1201/9781003058434-1>.

Kiseleva A (2020) AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability? *European Pharmaceutical Law Review* 4:5–16. DOI: <https://doi.org/10.21552/eplr/2020/1/4>.

Kokott J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law* (3)4: 222–228. DOI: <https://doi.org/10.1093/idpl/ipt017>.

Kreutzer RT, Sirrenberg M (2020) *Understanding Artificial Intelligence: Fundamentals, Use Cases and Methods for a Corporate AI Journey*. Springer, Cham. DOI: <https://doi.org/10.1007/978-3-030-25271-7>.

Krishnamurthy V (2020) A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. *AJIL Unbound* 114:26–30. DOI: <https://doi.org/doi:10.1017/aju.2019.79>

Kulkarni A, Sathe S (2014) Healthcare applications of the Internet of Things: A Review. *International Journal of Computer Science and Information Technologies* 5(5):6229–6232. Available from: <http://ijcsit.com/docs/Volume 5/vol5issue05/ijcsit2014050551.pdf>.

Lang M (2017): Heart Rate Monitoring Apps: Information for Engineers and Researchers About the New European Medical Devices Regulation 2017/745. *JMIR Biomedical Engineering* 2(1):e2. DOI: <https://doi.org/10.2196/biomedeng.8179>.

Latif S, Qadir J, Farooq S, Imran MA (2017) How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare? *Future Internet* 9(93):1–24. DOI: <https://doi.org/10.3390/fi9040093>.

Leistner M (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. *In*: Lohsse S, Schulze R, Staudenmayer D (eds) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Münster Colloquia on EU Law and the Digital Economy III. Nomos, Baden-Baden, 25–58. Available from: <https://doi.org/10.5771/9783845288185-25>.

Liebowitz SJ, Margolis SE (1994) Network Externality: An Uncommon Tragedy. *Journal of Economic Perspectives* 8(2):133–150. DOI: <https://doi.org/10.1257/jep.8.2.133>.

Liu X, Merritt J, Tiscareno KK *et al*. (2020) *Shaping the Future of the Internet of Bodies: New challenges of technology governance*. Briefing Paper (July 2020). World Economic Forum, Geneva. Available from: <http://www3.weforum.org/docs/WEF_IoB_briefing_paper_2020.pdf>.

Lovell T (2021) *France to enable rapid market access for digital therapeutics*. Healthcare IT News (20 October 2021). Available from <https://www.healthcareitnews.com/news/emea/france-enable-rapid-market-access-digital-therapeutics>.

Lucivero F, Prainsack B (2015) The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle. *Applied & Translational Genomics* 4:44–49. DOI: <https://doi.org/10.1016/j.atg.2015.02.001>.

Ludvigsen K, Nagaraja S and Daly A (2021) When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law. *European Journal of Risk Regulation* 1–16. DOI: <https://doi.org/10.1017/err.2021.45>.

Luengo J, García-Gil D, Ramírez-Gallego S, Garcia S, Herrera F (2020) *Big Data Preprocessing: Enabling Smart Data*. Springer, Cham. DOI: <https://doi.org/10.1007/978-3-030-39105-8>.

Lynskey O (2015) *The Foundations of EU Data Protection Law*. Oxford University Press, Oxford.

Malafosse JB (2015) *Introductory Report for updating Recommendation R(97)5 of the Council of Europe on the protection of medical data*. T-PD(2015)07, Council of Europe, Strasbourg (15 June 2015). Available from: <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a601a>.

Malgieri G, Comandé G (2017) Sensitive-by-distance: quasi-health data in the algorithmic era. *Information & Communications Technology Law* 26(3):229–249. DOI: <https://doi.org/10.1080/13600834.2017.1335468>.

Margoni T, Gils T, Kun E (2022) *Chapter X of the Data Act and the Sui Generis Database Right*. KU Leuven CiTiP Blog (14 June 2022). Available from: <https://www.law.kuleuven.be/citip/blog/chapter-10-of-the-data-act-and-the-sui-generis-database-right/>.

Markvarde A (2021) *"Digital health is happening and here to stay". One Year of DiGA Fast-Track in Germany*. Digital Health Global (29 September 2021). Available from <https://www.digitalhealthglobal.com/digital-health-is-happening-and-here-to-stay-one-year-of-diga-fast-track-in-germany/>.

Martinelli A, Mina A, Moggi M (2021) The enabling technologies of industry 4.0: examining the seeds of the fourth industrial revolution. *Industrial and Corporate Change* 30(1):161–188. DOI: <https://doi.org/10.1093/icc/dtaa060>.

Masood A (2021) *Automated Machine Learning: Hyperparameter optimization, neural architecture search, and algorithm selection with cloud platforms*. Packt Publishing, Birmingham.

Matwyshyn AM (2019) The Internet of Bodies. *William & Mary Law Review* 61(1):77–168. Available from: <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3827&context=wmlr>.

Mayo M (2017) *The Current State of Automated Machine Learning*. KDnuggets (25 January 2017). Available from: <https://www.kdnuggets.com/2017/01/current-state-automated-machine-learning.html>.

Mayo M (2017) *The Data Science Puzzle, Revisited*. KDnuggets (25 January 2017). Available from: <https://www.kdnuggets.com/2017/01/data-science-puzzle-revisited.html>.

McFarland A (2022) *Telerobotic System Helps Surgeons Remotely Treat Strokes.* UniteAI (17 April 2022). Available from: <https://www.unite.ai/telerobotic-system-helps-surgeons-remotely-treat-strokes>.

McGonigle D, Mastrian K (eds) (2021) *Nursing Informatics and the Foundation of Knowledge* (Fifth Edition). Jones & Bartlett Learning, Burlington.

McMahon A, Buyx A, Prainsack B (2020) Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond, *Medical Law Review* 28(1):155–182. DOI: <https://doi.org/10.1093/medlaw/fwz016>.

Medicines and Healthcare products Regulatory Agency, BioIndustry Association (2018) *The Eighth Joint BIA/MHRA Conference Collaborative Working in the UK. Driving Innovation Forward* (5 July 2018) Medicines and Healthcare products Regulatory Agency, BioIndustry Association, London. Available from <https://www.bioindustry.org/uploads/assets/uploaded/2ceb87ee-bd78-4549-94bff0655fffa5b6.pdf>.

MedTech Europe (2020) *Innovation in Medical Technologies: Reflection Paper*. MedTech Europe, Brussels (October 2020). Available from <https://www.medtecheurope.org/wp-content/uploads/2020/10/2020_mte_innovation-in-medical-technologies_reflection-paper.pdf>.

MedTech Europe (2021) *Proposal for an Artificial Intelligence Act (COM/2021/206): MedTech Europe response to the open public consultation*. Feedback to Artificial intelligence – ethical and legal requirements (6 August 2021). MedTech Europe, Brussels. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665532_en>.

MedTech Europe (2021) *MedTech Europe comment to the proposed Regulation on General Product Safety*. Feedback to General Product Safety Directive – review. MedTech Europe, Brussels (4 October 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-General-Product-Safety-Directive-review/F2674997_en>.

MedTech Europe, COCIR (2021) *Interoperability standards in digital health: A White Paper from the medical technology industry*. MedTech Europe, COCIR (6 October 2021). Available from: <https://www.medtecheurope.org/wp-content/uploads/2021/10/mte_interoperability_digital_health_white-paper_06oct21.pdf>.

Meetoo D, Wong L, Ochieng B (2019) Smart tattoo: technology for monitoring blood glucose in the future. *British Journal of Nursing* 28(2):1–7. DOI: <https://doi.org/10.12968/bjon.2019.28.2.110>.

Meszaros J, Compagnucci MC, Minssen T (2022) The Interaction of the Medical Device Regulation and the GDPR. Do European Rules on Privacy and Scientific Research Impair the Safety and Performance of AI Medical Devices? *In*: Cohen IG, Minssen T,

Price II WN, Robertson C, Shachar C (eds) *The Future of Medical Device Regulation Innovation and Protection*. Cambridge University Press, Cambridge, 77–90. DOI: <https://doi.org/10.1017/9781108975452.007>.

mHealth Belgium (n.d.) *Validation pyramid*. mHealth Belgium. Available from <https://mhealthbelgium.be/validation-pyramid> (accessed 1 October 2022).

Minerva R, Biru A, Rotondi D (2015) *Towards a Definition of the Internet of Things (IoT)*. IEEE Internet Initiative (Rev. 1) (27 May 2015). Available from: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>.

Minoli D (2013) *Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications*. John Wiley & Sons, Hoboken. DOI: <https://doi.org/10.1002/9781118647059>.

Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10(7):1497–1516. DOI: <https://doi.org/10.1016/j.adhoc.2012.02.016>.

Miotto R, Danieletto M, Scelza JR, Kidd BA, Dudley JT (2018) Reflecting health: smart mirrors for personalized medicine. *Npj Digital Medicine* 1(62):1–7. DOI: <https://doi.org/10.1038/s41746-018-0068-7>.

Mittelstadt B (2017) From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology* 30:475–494. DOI: <https://doi.org/10.1007/s13347-017-0253-7>.

Mozilla (2022) *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security*. Mozilla (2 May 2022). Available from <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/>.

Mulder T (2019) The Protection of Data Concerning Health in Europe. *European Data Protection Law Review* 5(2):209–220. DOI: <https://doi.org/10.21552/edpl/2019/2/10>.

Naresh V, Lee N (2021) A Review on Biosensors and Recent Development of Nanostructured Materials-Enabled Biosensors. *Sensors*, 21(4):1109. DOI: <https://doi.org/10.3390/s21041109>.

Negreiro M (2021) *The rise of digital health technologies during the pandemic*. European Parliamentary Research Service Member's Research Service, 2–3. Available from: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690548/EPRS_BRI(2021)690548_EN.pdf>.

NEJM Catalyst (2017) *What Is Value-Based Healthcare?* NEJM Catalyst, Waltham (1 January 2017). Available from: <https://catalyst.nejm.org/doi/full/10.1056/CAT.17.0558>.

Ng A (2021) *Face Datasets Under Fire, Baking With AI, Human Disabilities Baffle Algorithms, Ginormous Transformers.* DeepLearning.AI: The Batch (24 February 2021). Available from: <https://www.deeplearning.ai/the-batch/issue-80>.

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford.

Noone G (2022) *Putting AI in IoT chips? It's a question of memory*. Tech Monitor (10 February 2022). Available from: <https://techmonitor.ai/technology/ai-and-automation/tinyml-putting-ai-in-iot-chips-a-question-of-memory>.

NordForsk (2019) *A vision of a Nordic secure digital infrastructure for health data: The Nordic Commons*. NordForsk, Oslo. Available from: <http://norden.diva-portal.org/smash/get/diva2:1376735/FULLTEXT01.pdf>.

Nordic Innovation (n.d.) *Nordic Digital Health & Medication Platform*. Nordic Innovation. Available from <https://www.nordicinnovation.org/programs/nordic-digital-health-medication-platform> (accessed 1 October 2022).

Novartis International (2021) *Novartis feedback on Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. Novartis International, Basel (6 August 2021), 2. Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665464_en>.

OECD (2015) *Data-Driven Innovation: Big Data for Growth and Well-Being*. OECD Publishing, Paris. DOI: <https://doi.org/10.1787/9789264229358-en>.

OECD (Anderson G, Oderkirk J (eds)) (2015) *Dementia Research and Care: Can Big Data Help?* OECD Publishing, Paris. DOI: <https://doi.org/10.1787/9789264228429-en>.

OECD (2017) *New Health Technologies: Managing Access, Value and Sustainability*. OECD Publishing, Paris. DOI: <https://doi.org/10.1787/9789264266438-en>.

OECD (2019) *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing, Paris. DOI: <https://doi.org/10.1787/276aaca8-en>.

OECD (2019) *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*. OECD Health Policy Studies. OECD Publishing, Paris. DOI: <https://doi.org/10.1787/e3b23f8e-en>.

OECD (2019) *Scoping the OECD AI principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)*. OECD Digital Economy Papers, No. 291 (November 2019). OECD, Paris. Available from: <https://doi.org/10.1787/d62f618a-en>.

OECD, European Union (2020) *Health at a Glance: Europe 2020: State of Health in the EU Cycle*. OECD Publishing, Paris. DOI: <https://doi.org/10.1787/82129230-en>.

OECD (2021) *Health at a Glance 2021: OECD Indicators*. OECD Publishing, Paris. DOI: <https://doi.org/10.1787/ae3016b9-en>.

Olesch A (2021) *A Year With Apps On Prescription In Germany*. Sidekick (19 October 2021). Available from <https://sidekickhealth.com/news/a-year-with-apps-on-prescription-in-germany>.

Olesch A (2021) *Sven Jungmann: "Is the model of reimbursable health apps in Germany a failure?"* ICT&health (1 December 2021). Available from <https://ictandhealth.com/is-the-model-of-reimbursable-health-apps-in-germany-a-failure/news>.

Paassen R (2020) *A regulatory perspective of Artificial Intelligence in Medical Devices* (23 November 2020). QServe Group, Arnhem. Available from <https://www.qservegroup.com/eu/en/i824/a-regulatory-perspective-of-artificial-intelligence-in-medical-devices>.

Paek AY, Brantley JA, Evans BJ, Contreras-Vidal JL (2021) Concerns in the Blurred Divisions Between Medical and Consumer Neurotechnology. *IEEE Systems Journal* 15(2):3069–3080. DOI: <https://doi.org/10.1109/JSYST.2020.3032609>.

Palmieri S, Walraet P, Goffin T (2021) Inevitable Influences: AI-Based Medical Devices at the Intersection of Medical Devices Regulation and the Proposal for AI Regulation. *European Journal of Health Law* 28(4):341–358. DOI: <https://doi.org/10.1163/15718093-bja10053>.

Panesar A (2019) *Machine Learning and AI for Healthcare Big Data for Improved Health Outcomes*. Apress, New York. DOI: <https://doi.org/10.1007/978-1-4842-3799-1>.

Pateraki M, Fysarakis K, Sakkalis V (2020) Biosensors and Internet of Things in smart healthcare applications: challenges and opportunities. *In*: Dey N, Ashour AS, Fong SJ (eds) *Wearable and Implantable Medical Devices: Applications and Challenges*. Academic Press, London, 25–53. DOI: <https://doi.org/10.1016/B978-0-12-815369-7.00002-1>.

Pauwels E, Denton SW (2018) The Internet of Bodies: Life and Death in the Age of AI. *California Western Law Review* 55(1):221–233. Available from: <https://scholarlycommons.law.cwsl.edu/cwlr/vol55/iss1/5>.

Pedersen I, Iliadis A (2020) Introduction: Embodied Computing. *In*: Pedersen I, Iliadis A (eds) *Embodied Computing: Wearables, Implantables, Embeddables, Ingestibles*. MIT Press, Cambridge (USA), ix–xxxix. DOI: <https://doi.org/10.7551/mitpress/11564.001.0001>.

Peppet SR (2014) Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent. *Texas Law Review* 93:85–176. DOI: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>.

Peranzo P (2022) *10 Healthcare SaaS Trends That Can Revolutionize the Medical Industry*. Imaginovation, Raleigh (7 February 2022). Available from: <https://imaginovation.net/blog/healthcare-saas-trends-that-revolutionize-medical-industry>.

Pharmaceutical Group of the European Union (PGEU) (2021) *PGEU feedback on the European Commission Proposal for an EU Regulation on Artificial Intelligence*. Feedback to Artificial intelligence – ethical and legal requirements. Pharmaceutical Group of the European Union, Brussels (20 July 2021). Available from

<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662654_en>.

Pila J, Torremans P (2019) *European Intellectual Property Law* (Second Edition). Oxford University Press, Oxford.

Pinto R, Baracsi M (2012) Creating an environment for innovative start-ups in healthcare. *Health Policy and Technology* 1(4):187–192. DOI: <https://doi.org/10.1016/j.hlpt.2012.10.006>

Priya, Pathak I, Tripathi A (2018) Big Data, Cloud and IoT: An Assimilation. *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T) (Allahabad, 21–23 September 2018)*, 34–40. DOI: <https://doi.org/10.1109/IAC3T.2018.8674024>.

Purtova N (2017) eHealth Spare Parts as a Service: Modular eHealth Solutions and Medical Device Reform. *European Journal of Health Law* 24:463–486. DOI: <https://doi.org/10.1163/15718093-12341430>.

Purtova N (2018) The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* 10(1):40–81. DOI: <https://doi.org/10.1080/17579961.2018.1452176>.

PwC (2020) *Accelerating the health economy of tomorrow: Transforming health systems and embracing innovation amid a pandemic*. PwC. Available from: <https://www.pwc.com/gx/en/industries/healthcare/publications/assets/pwc-new-health-economy.pdf>.

Quinn P, Habbig AK, Mantovani E, De Hert P (2013) The Data Protection and Medical Device Frameworks — Obstacles to the Deployment of mHealth across Europe? *European Journal of Health Law* 20:185–204. DOI: <https://doi.org/10.1163/15718093-12341267>.

Quinn P (2017) The EU commission's risky choice for a non-risk based strategy on assessment of medical devices. *Computer Law & Security Review* 33(3):361–370. DOI: <https://doi.org/10.1016/j.clsr.2017.03.019>.

Raeesi Vanani I, Amirhosseini M (2021) IoT-Based Diseases Prediction and Diagnosis System for Healthcare. *In*: Chakraborty C, Banerjee A, Kolekar M, Garg L, Chakraborty B (eds) *Internet of Things for Healthcare Technologies*. Springer, Singapore, 21–48. DOI: <https://doi.org/10.1007/978-981-15-4112-4_2>.

Raij A, Ghosh A, Kumar S, Srivastava M (2011) Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. *CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Vancouver, May 2011)*, 11–20. DOI: <https://doi.org/10.1145/1978942.1978945>.

Rak R (2022) International Transfers of Data Concerning Health After Schrems II: A Need for Sector-Specific Legal Avenues and Supplementary Measures. *In*: Casolari F, Gatti M (eds) *The Application of EU Law Beyond Its Borders*. CLEER Papers 2022/3. T.M.C.

Asser Institute, The Hague, 187–206. Available from: <https://www.asser.nl/media/795814/cleer_022-03_web_final.pdf>.

ResMed (2021) *ResMed consultation response: Artificial Intelligence Act*. Feedback to Artificial intelligence – ethical and legal requirements. ResMed, Brussels (30 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2663398_en>.

Robert Koch-Institut (n.d.) *Corona Datenspende*. Robert Koch-Institut. Available from <https://corona-datenspende.de>.

Roberts P (2017) Interdisciplinarity in Legal Research. *In*: McConville M, Chui WH (eds) *Research Methods for Law* (Second Edition). Edinburgh University Press, Edinburgh, 90–133. DOI: <https://www.jstor.org/stable/10.3366/j.ctt1g0b16n.10>.

Rockenbach MABC (2021) *Multimodal AI in Healthcare: Closing the Gaps*. Medium (13 June 2021). Available from <https://medium.com/codex/multimodal-ai-in-healthcare-1f5152e83be2>.

Rodrigues JJPC, Segundo DBDR, Junqueira, HA *et al*. (2018) Enabling Technologies for the Internet of Health Things. *IEEE Access* 6:13129–13141. DOI: <https://doi.org/10.1109/ACCESS.2017.2789329>.

Rose K, Eldridge S, Chapin L (2015) *The Internet of Things: an Overview. Understanding the Issues and Challenges of a More Connected World*. Internet Society (29 May 2020). Available from: <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf>.

Ryan J, Shrishak K (2021) *A serious loophole in Europe's draft AI Regulation?* Irish Council for Civil Liberties (27 October 2021). Available from <https://www.iccl.ie/news/scope-loophole-in-the-eu-ai-act-draft>.

Sahu SN, Moharana M, Prusti PC, Chakrabarty S, Khan F, Pattanayak SK (2020) Real-time data analytics in healthcare using the Internet of Things. *In*: Das H, Dey N, Balas VE (eds) *Real-Time Data Analytics for Large Scale Sensor Data*. Academic Press, London, 37–50. DOI: <https://doi.org/10.1016/B978-0-12-818014-3.00002-4>.

Sakr S, Elgammal A (2016) Towards a Comprehensive Data Analytics Framework for Smart Healthcare Services. *Big Data Research* 4:44–58. DOI: <https://doi.org/10.1016/j.bdr.2016.05.002>.

Samoili S, López Cobo M, Delipetrev B, Martínez-Plumed F, Gómez E, De Prato G (2021) *AI Watch. Defining Artificial Intelligence 2.0. Towards an operational definition and taxonomy for the AI landscape*. JRC Technical Reports. Publications Office of the European Union, Luxembourg. DOI: <https://data.europa.eu/doi/10.2760/019901>.

Sanofi (2021) *Feedback from: Sanofi*. Feedback to Artificial intelligence – ethical and legal requirements. Sanofi, Paris (22 July 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662846_en>.

Shabani M (2021) The Data Governance Act and the EU's move towards facilitating data sharing. *Molecular Systems Biology* 17(3):e10229. DOI: <https://doi.org/10.15252/msb.202110229>.

Schneble CO, Elger BS, Shaw DM (2020) All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent. *Journal of Medical Internet Research* 22(5):e16879. DOI: <https://doi.org/10.2196/16879>.

Shamim MZ, Parayangat M, Thafasal Ijyas VP (2021) Distributed Intelligent Networks: Convergence of 5G, AI, and IoT. *In*: Usman M, Wajid M, Ansari MD (eds) *Enabling Technologies for Next Generation Wireless Communications*. CRC Press, Boca Raton, 137–148. DOI: <https://doi.org/10.1201/9781003003472>.

Sheppard MK (2020) EU Medical Device Legislation and the Safety Implications for App Users. *In*: Iglezakis I (ed): *Legal Issues of Mobile Apps: A Practical Guide.* Kluwer Law International, Alphen aan den Rijn.

Schuh M (2020) *Focus on the intended purpose of digital health applications*. Berlin: Reuschlaw. Available from <https://www.reuschlaw.de/en/news/focus-on-the-intended-purpose-of-digital-health-applications>.

Siemens Healthineers (2021) *Siemens Healthineers' feedback to the European Commission's proposal for a Regulation laying down harmonised rules on artificial intelligence (AI Act)*. Feedback to Artificial intelligence – ethical and legal requirements. Siemens, Erlangen (6 August 2021). Available from <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665604_en>.

Siems MM (2009) The Taxonomy of Interdisciplinary Legal Research: Finding the Way Out of the Desert. *Journal of Commonwealth Law and Legal Education* 7(1):5–17. DOI: <https://doi.org/10.1080/14760400903195090>.

Simonson M (2021) *Electronic wellbeing apps in Germany – An update on the DiGA journey*. Inno Lab (1 December 2021). Available from <https://innolabllc.com/electronic-wellbeing-apps-in-germany-an-update-on-the-diga-journey.html>.

Skala K, Davidović D, Afgan E, Sovic I, Sojat Z (2015) Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing. *Open Journal of Cloud Computing* 2(1):16–24. DOI: <https://doi.org/10.19210/1002.2.1.16>.

Smits JM (2014) Law and Interdisciplinarity: On the Inevitable Normativity of Legal Studies. *Critical Analysis of Law* 1(1):75–86. DOI: <https://resolver.scholarsportal.info/resolve/22919732/v01i0001/nfp_laiotinols.xml>.

Solanas A, Patsakis C, Conti M *et al*. (2014) Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine* 52(8):74–81. DOI: <https://doi.org/10.1109/MCOM.2014.6871673>.

Soldatos J, Kefalakis N, Serrano M (2017) An Open Source Framework for IoT Analytics as a Service. *In*: Soldatos J (ed) *Building Blocks for IoT Analytics*. River Publishers, Aalborg, 99–138. DOI: <https://doi.org/10.13052/rp-9788793519046>.

Sood S, Mbarika V, Jugoo S *et al*. (2007) What Is Telemedicine? A Collection of 104 Peer-Reviewed Perspectives and Theoretical Underpinnings. *Telemedicine and eHealth* 13(5):573–590. DOI: <https://doi.org/10.1089/tmj.2006.0073>.

Stern AD, Matthies H, Hagen J, Brönneke JB, Debatin JF (2020) *Want to See the Future of Digital Health Tools? Look to Germany*. Harvard Business Review (2 December 2021). Available from <https://hbr.org/2020/12/want-to-see-the-future-of-digital-health-tools-look-to-germany>.

Sulis E, Amantea IA, Aldinucci M *et al*. (2022) An ambient assisted living architecture for hospital at home coupled with a process-oriented perspective. *Journal of Ambient Intelligence and Humanized Computing* (online first). DOI: <https://doi.org/10.1007/s12652-022-04388-6>.

Syed L, Jabeen S, Manimala S, Alsaeedi A (2019) Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques. *Future Generation Computer Systems* 101:136–151. DOI: <https://doi.org/10.1016/j.future.2019.06.004>.

Temesgen ZM, DeSimone DC, Mahmood M, Libertin CR, Varatharaj Palraj BR, Berbari EF (2020) Health Care After the COVID-19 Pandemic and the Influence of Telemedicine. *Mayo Clinic Proceedings* 95(9):S66–S68. DOI: <https://doi.org/10.1016/Fj.mayocp.2020.06.052>.

Thelisson E (2022) AI Technologies and Accountability in Digital Health *In*: Compagnucci MC, Wilson M, Fenwick M, Forgó N, Bärnighausen T (eds) *AI in eHealth: Human Autonomy, Data Governance and Privacy in Healthcare*. Cambridge University Press, Cambridge, 166–206. DOI: <https://doi.org/10.1017/9781108921923.011>.

Thorp J, Fletcher G, Wehnert J, Gessner C, Nicolas L (2015) *Report on the use of cloud computing in health*. Submitted as information to the members of the eHealth Network at their 8th meeting on 23 November 2015. Joint Action to support the eHealth Network. Available from: <https://health.ec.europa.eu/system/files/2018-02/ev_20151123_co06_02_en_0.pdf>.

Thovex C (2019) When Big Data and Data Science Prefigured Ambient Intelligence. *In*: Soldatos J (ed) *Smart Data: State-of-the-Art Perspectives in Computing and Applications*. Chapman and Hall/CRC, New York, 319–342. DOI: <https://doi.org/10.1201/9780429507670>.

Tschofenig H, ARM Ltd., Arkko J, Thaler D, McPherson D (2015) *Architectural Considerations in Smart Object Networking*. Internet Architecture Board (March 2015). Available from: <https://www.rfc-editor.org/rfc/rfc7452.txt>.

United Nations Special Raporteur on the right to privacy (n.d.) *Annual thematic reports*. United Nations Human Rights Office of the High Commissioner, Geneva. Available from: <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx> (accessed 1 October 2022).

Upadhyay D, Sharma S (2021) Convergence of Artificial Intelligence of Things: Concepts, Designing, and Applications. *In*: Sharma L (ed) *Towards Smart World: Homes to Cities*

Using Internet of Things. CRC Press, Boca Raton, 119–142. DOI: <https://doi.org/10.1201/9781003056751>.

Urias MG, Patel N, He C *et al*. (2019) Artificial intelligence, robotics and eye surgery: are we overfitted? *International Journal of Retina and Vitreous* 5:52. DOI: <https://doi.org/10.1186/s40942-019-0202-y>.

Vaquero AN (2013) Five Models of Legal Science (Bertrán EG, trans.). *Revus* 19:53–81. DOI: <https://doi.org/10.4000/revus.2449>.

Veale M, Borgesius FZ (2021) Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International* 22(4):97–112. DOI: <https://doi.org/10.9785/cri-2021-220402>.

Vermesan O, Friess P, Guillemin P *et al*. (2013) Internet of Things Strategic Research and Innovation Agenda. *In*: Vermesan O, Friess P (eds) *Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, Aalborg, 7–142. Available from: <http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf>.

Vermesan O, Coppola M, Nava MD *et al*. (2020) New Waves of IoT Technologies Research – Transcending Intelligence and Senses at the Edge to Create Multi Experience Environments. *In*: Vermesan O, Bacquet J (eds) *Internet of Things – The Call of the Edge: Everything Intelligent Everywhere*. River Publishers, Gistrup, 17–184. DOI: <https://doi.org/10.13052/rp-9788770221955>.

Viswanathan H, Lee EK, Pompili D (2012) Mobile grid computing for data- and patient-centric ubiquitous healthcare. *2012 The First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT) (Seoul, 18 June 2012)*, 36–41. DOI: <https://doi.org/10.1109/ETSIoT.2012.6311263>.

Von Mühlenen E, Melin AS (2021) *Germany's "DiGA" Digital Health Fast Track Process Is Modeling a New Way To Regulate Market Access and Reimbursement*. Sidley Austin (10 December 2021). Available from <https://www.sidley.com/en/insights/newsupdates/2021/12/germanys-diga-digital-health-fast-track-process-is-modeling-a-new-way-to-regulate-market-access>.

Wachter S (2018) The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology* 10(2):266–294. DOI: <https://doi.org/10.1080/17579961.2018.1527479>.

Wachter S, Mittelstadt B (2019) A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review* 2:1–130. DOI: <https://doi.org/10.31228/osf.io/mu2kf>.

Wåhslén J, Lindh T (2011) Smartphone-centric Wi-Fi device-to-device sensor communication for user mobility in AAL services. *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*

(Valencia, 4–8 September 2016). DOI: <https://doi.org/10.1109/PIMRC.2016.7794565>.

Walzer S (2021) *The reimbursement models in healthcare & market access in Europe*. Market Access & Pricing Strategy, Weil am Rhein (12 October 2021). Available from <https://www.nweurope.eu/media/15287/4the-reimbursement-models-in-healthcare-market-access.pdf>.

Wilkinson M, Dumontier M, Aalbersberg I *et al*. (2016) The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data* 3(16018):1–9. DOI: <https://doi.org/10.1038/sdata.2016.18>.

Williams PAH, McCauley V (2016) Always Connected: The Security Challenges of the Healthcare Internet of Things. *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (Reston, 12–14 December 2016)*, 30–35. DOI: <https://doi.org/10.1109/WF-IoT.2016.7845455>.

World Health Organization (2011) *mHealth: New horizons for health through mobile technologies*. Based on the findings of the second global survey on eHealth. Global Observatory for eHealth series - Volume 3. World Health Organization, Geneva. Available from: <https://apps.who.int/iris/handle/10665/44607>.

World Health Organization (2016) *Global diffusion of eHealth: Making universal health coverage achievable. Report of the third global survey on eHealth*. World Health Organization, Geneva. Available from: <https://apps.who.int/iris/handle/10665/252529>.

World Health Organization (2021) *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*. World Health Organization, Geneva. DOI: <https://apps.who.int/iris/rest/bitstreams/1352854/retrieve>.

World Health Organization Global Observatory for eHealth (2010) *Telemedicine: Opportunities and developments in Member States. Report on the second global survey on eHealth*. Report of the third global survey on eHealth. World Health Organization, Geneva. Available from: <https://apps.who.int/iris/handle/10665/44497>.

Wyler J (2020) *The intended purpose – or, what does your medical device do?* (4 February 2020), Decomplix, Bern. Available from <https://decomplix.com/intended-purpose-medical-device>.

Yousefpour A, Fung C, Nguyen T *et al*. (2019) All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture* 98:289–330. DOI: <https://doi.org/10.1016/j.sysarc.2019.02.009>.

Zhang T, Schoene AM, Ji S, Ananiadou S (2022) Natural language processing applied to mental illness detection: a narrative review. *Npj Digital Medicine* 5(46):1–13. DOI: <https://doi.org/10.1038/s41746-022-00589-7>.

SUMMARY

The purpose of this research study is to discuss privacy and data protection-related regulatory and compliance challenges posed by digital transformation in healthcare in the wake of the COVID-19 pandemic. The public health crisis accelerated the development of patient-centred remote/hybrid healthcare delivery models that make increased use of telehealth services and related digital solutions. The large-scale uptake of IoT-enabled medical devices and wellness applications, and the offering of healthcare services via healthcare platforms (online doctor marketplaces) have catalysed these developments. However, the use of new enabling technologies (IoT, AI) and the platformisation of healthcare pose complex challenges to the protection of patient's privacy and personal data. This happens at a time when the EU is drawing up a new regulatory landscape for the use of data and digital technologies. Against this background, the study presents an interdisciplinary (normative and technology-oriented) critical assessment on how the new regulatory framework may affect privacy and data protection requirements regarding the deployment and use of Internet of Health Things (hardware) devices and interconnected software (AI systems). The study also assesses key privacy and data protection challenges that affect healthcare platforms (online doctor marketplaces) in their offering of video API-enabled teleconsultation services and their (anticipated) integration into the European Health Data Space. The overall conclusion of the study is that regulatory deficiencies may create integrity risks for the protection of privacy and personal data in telehealth due to uncertainties about the proper interplay, legal effects and effectiveness of (existing and proposed) EU legislation. The proliferation of normative measures may increase compliance costs, hinder innovation and ultimately, deprive European patients from state-of-the-art digital health technologies, which is paradoxically, the opposite of what the EU plans to achieve.

ZUSAMMENFASSUNG

Die öffentliche Gesundheitskrise beschleunigte die Entwicklung von patientenzentrierten Modellen der Fern-/Hybrid-Gesundheitsversorgung, die verstärkt auf telemedizinische Dienste und damit verbundene digitale Lösungen zurückgreifen. Die breite Einführung von IoT-fähigen medizinischen Geräten und Wellness-Anwendungen sowie das Angebot von Gesundheitsdienstleistungen über Gesundheitsplattformen (Online-Marktplätze für Ärzte) haben diese Entwicklungen beschleunigt. Der Einsatz neuer Basistechnologien (IoT, KI) und die Plattformisierung des Gesundheitswesens stellen jedoch komplexe Herausforderungen für den Schutz der Privatsphäre und der personenbezogenen Daten der Patienten dar. Dies geschieht zu einer Zeit, in der die EU eine neue Regulierungslandschaft für die Nutzung von Daten und digitalen Technologien entwirft. Vor diesem Hintergrund präsentiert die Studie eine interdisziplinäre (normative und technologieorientierte) kritische Bewertung der Frage, wie sich der neue Rechtsrahmen auf die Anforderungen an den Schutz der Privatsphäre und den Datenschutz in Bezug auf den Einsatz und die Nutzung von Geräten des Internets der Dinge (Hardware) und vernetzter Software (KI-Systeme) auswirken könnte. Die Studie bewertet auch die wichtigsten Herausforderungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz, die Gesundheitsplattformen (Online-Marktplätze für Ärzte) bei ihrem Angebot von Video-API-gestützten Telekonsultationsdiensten und ihrer (erwarteten) Integration in den europäischen Gesundheitsdatenraum betreffen. Die allgemeine Schlussfolgerung der Studie lautet, dass regulatorische Mängel Integritätsrisiken für den Schutz der Privatsphäre und personenbezogener Daten in der Telemedizin schaffen können, da Unsicherheiten über das richtige Zusammenspiel, die rechtlichen Auswirkungen und die Wirksamkeit der (bestehenden und vorgeschlagenen) EU-Gesetzgebung bestehen. Darüber hinaus kann der Wildwuchs an normativen Maßnahmen die Kosten für die Einhaltung der Vorschriften erhöhen, Innovationen behindern und letztlich den europäischen Patienten modernste digitale Gesundheitstechnologien vorenthalten, was paradoxerweise das Gegenteil von dem ist, was die EU erreichen will.