Safeguarding privacy and efficacy in e-mental health: policy options in the EU and Australia

Elisabeth Steindl *

Key Points

- Inadequate data protection and privacy practices, along with a lack of demonstrated efficacy, are hindering the beneficial implementation of digital technologies in mental healthcare and the sustainable growth of an e-mental health industry.
- As the European Union (EU) develops policy actions for a comprehensive mental health strategy, it is crucial to incorporate a strong framework for e-mental health addressing these concerns from the onset.
- Australia is a frontrunner in e-mental health, its regulatory initiatives can inform the debate due to its more advanced state.
- While the EU adheres to a strict distinction between medical devices and consumer health/well-being products, Australia adapts the medical devices legislation to e-mental health tools by introducing a 'conditioned exemption'.
- Concerning matters of privacy and data protection, however, the EU has suitable legal instruments sui generis (eg a GDPR-code of conduct and/or a GDPR certification scheme)—they just need effective implementation.

Introduction

Digital technologies have made a significant impact on the mental health sector, and they are likely to continue doing so. Despite the increasing demand for e-mental health solutions, there are concerns regarding poor privacy and data protection practices, as well as a lack of evidence to support their effectiveness. Both are considered impediments to fully reaping the benefits of digital technologies in mental health.

European Union (EU) policymakers are currently developing actions for a comprehensive mental health strategy. It would be prudent to incorporate a robust regulatory framework for e-mental health from the outset in order to encourage a sustainable European industry for e-mental health. Partially, this framework can take recourse to existing legal instruments available under current EU data protection law, while also taking inspiration from recent regulatory efforts in Australia.

The focus of this article is on the grey zone between classified medical devices and simple consumer health products. Whereas the EU adheres to a strict distinction between these two categories, Australia adapts the regulations for medical devices to the needs and specificities of e-mental health tools by assigning them their own niche within the medical devices systematics under a 'conditioned exemption'. With regard to devices beyond the scope of the medical devices legislation, Australia is implementing a coordinated regime of complementary regulation of sectoral standards combined with an accreditation scheme. To a certain extent and its data protection-related aspects, this coordinated regime shows conceptual similarities with co-regulatory instruments under EU data protection law, such as a sector-specific data protection code of conduct and a data protection certificate.

Challenges for the governance of digital technologies in mental health

Concerns over data protection/privacy, coupled with a lack of demonstrated efficacy, impede the adoption of digital technologies

Digital technologies have reached the mental health sector, and they have come to stay. A general trend for

*Elisabeth Steindl, Department of Innovation and Digitalization in Law, Research Platform Governance of Digital Practices, University of Vienna, Austria. E-mail: elisabeth.steindl@univie.ac.at.

The author would like to thank Dr Piers Gooding, University of Melbourne, and Chris Boyd-Skinner R.N MIPH, MHM, Australian Commission on Safety and Quality in Health Care, for their valuable feedback and comments.

digitalization in all spheres of being as well as specific advancements in emerging mental technologies, such as emotion technology and neurotechnology, have aligned and are driving what can be called a technological revolution in mental health. The COVID19-pandemic, too, has contributed its part. A noteworthy increase in demand collided with a sector that has been suffering from undersupply already before the beginning of the pandemic; the sudden disruption of (so-far) common forms of service due to lockdowns even exacerbated the situation.[1] In addition, the media coverage has supported a growing overall awareness about mental health and a boost in e-mental health tools.

E-mental health tools have become a serious market segment. Some predict the global e-mental health market to reach USD 71.1 billion by 2030, with Europe accounting for the second-largest market share.[2] The sector is attracting considerable investments and has widely expanded into consumer health and well-being products. Private equity firms are funnelling large sums into mental health apps and related interventions.[3]

However, concerns over privacy and data protection, such as that private information could be used by insurance companies or for punitive reasons by government agencies, or that it might be shared with or sold to third parties, constitute a barrier to the effective adoption of digital technologies in mental healthcare.[4] The World Health Organization (WHO) lists 'privacy, data protection, safety and accountability' even among the key concerns when harnessing digital technologies for mental health.[5]

First experiences with the German DiGA[6] system point to a similar conclusion.[7] Many of the apps currently included in the DiGA system are in fact mental health apps. Recent studies show that the awareness about DiGAs is increasing but doctors are still reluctant to prescribe them. Asked about the biggest barriers to prescribing an app, they name concerns regarding data protection in the first place (70.6 per cent), followed by doubts about the efficacy (47.4 per cent).[8] Data protection, security, and privacy are therefore crucial for a sustainable development and growth of the sector.

A look into the actual practices in e-mental health reveals that there is indeed reason for concern. In 2019, Privacy International has analysed more than 136 popular web pages related to depression in Germany, France, and the UK and concluded that 97.78 per cent of all web pages were using third-party elements, mostly to be tracked for advertising and marketing purposes.[9] In 2022, Mozilla studied the privacy and security practices of some of the most popular mental health apps. The result was again appalling: 28 out of 32 apps were found to show concerning user data management, 25 failed to even meet minimum security standards. Mozilla researchers concluded that 'mental health and prayer apps are worse than any other product category' and that despite dealing with highly sensitive data, such as information about depression, anxiety, suicidal thoughts, domestic violence, eating disorders, or PTSD, these apps 'routinely share data, allow weak passwords, target vulnerable users with personalized ads, and feature vague and poorly written privacy policies'.[10] Similar studies[11] and reports about particularly poor practices in the e-mental health sector have been published for years,[12] ranging from Canada[13] to New

1 See eg WHO, 'World mental health report: transforming mental health for all' (2022).

2 Market Research Future, 'Global Digital Mental Health Market Overview' (2023) <https://www.marketresearchfuture.com/reports/digital-mental-health-market-11062> accessed 31 May 2023.

3 See eg Tori DeAngelis, 'Mental Health, meet Venture Capital' (2022) <https://www.apa.org/monitor/2022/01/special-venture-capital> accessed 30 January 2023.

4 World Economic Forum and Deloitte, 'Global Governance Toolkit for Digital Mental Health: Building Trust in Disruptive Technology for Mental Health', White Paper (2021), 17–18. See also Ashley Gold, 'Mental Health app Boom Raises Alarms' (2022) <https://www.axios.com/2022/05/02/mental-health-app-boom-raises-alarms> accessed 22 February 2023.

5 WHO, 'World Mental Health Report: Transforming Mental Health for All' (2022), 124. See also: Nicole Martinez-Martin and others, 'Ethics of Digital Mental Health During COVID-19: Crisis and Opportunities' (2020) 7(12) JMIR Ment Health e23776.

6 Digitale Gesundheitsanwendungen (DiGAs) are digital health applications on prescription, reimbursed by the statutory healthcare system. <https://gesund.bund.de/en/digital-health-applications-diga> accessed 10 June 2023.

7 Federal Institute for Drugs and Medical Devices, DiGA Digital Health Applications <https://www.bfarm.de/EN/Medical-devices/Tasks/DiGA-and-DiPA/Digital-Health-Applications/_node.html> 30 January 2023.

8 Regine Marxen, 'Verschreibung von DiGA: Welche Bedenken hat der Arzt?' (2022) <https://www.healthrelations.de/diga-verschreibung-arzt/> accessed 27 January 2023.

9 Privacy International, Report: 'Your mental health for sale' (2019) <https://privacyinternational.org/node/3193> 30 May 2023.

10 Mozilla, 'Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security' (2022) <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/> accessed 30 May 2023.

11 For a recent empirical investigation see also LH Iwaya and others, 'On the Privacy of Mental Health Apps' 2 (2023) Empir Software Eng 28 <https://doi.org/10.1007/s10664-022-10236-0> accessed 27 March 2023.

12 Séamus Sweeney, '"The Wild West of Health" Care: Mental Health Apps, Evidence, and Clinical Credibility' (2016) <https://amedicaleducation.wordpress.com/2016/09/10/the-wild-west-of-health-care-mental-health-apps-evidence-and-clinical-credibility/> accessed 30 May 2023.

13 CBC News, '"Wild West" Mental Health Apps offer both Gold and "digital snake oil". Apps Aim to Bridge Gaps in Access to Effective Care Across Canada' (2017) <https://www.cbc.ca/news/health/mental-health-apps-1.4101201> accessed 30 May 2023.

Zealand,[14] encompassing the USA[15] and Europe.[16] The issue is therefore not a matter of one single misconduct in time or simply a regional problem but a concern of international amplitude.

Data protection/privacy infringements in e-mental health affect particularly vulnerable data subjects and leave them even more exposed

Concerns over data privacy infringements in the field of e-mental health appear to be of even higher magnitude than compared to other fields in digital health. The data processed by e-mental health tools are perceived as being very intimate. People search and share information about their addictive behaviour, about memories of abuse or about their suicidal thoughts, traumas, and anxieties. They track their mood for a better understanding about their mental state in order to prevent it from deteriorating. They seek help during hours of loneliness while they oscillate between having a few bad hair days and slipping into a depression. Unwanted or unauthorized access to this kind of information leaves the data subjects exceedingly vulnerable.

When it became publicly known that the British mental health helpline 'Shout', which offered a confidential service for people struggling with suicidal thoughts, self-harm, abuse, and bullying, shared full conversation data for research purposes, there was a huge public uproar. The users had agreed to terms of service that allowed the sharing of data for research; the data in question was allegedly anonymized and aggregated; the institution that the data was shared with was a trusted academic institution—yet, affected users and the public were outraged.[17] Privacy experts questioned whether conversation data can ever be fully anonymized, and whether people at crisis point can truly comprehend what they are consenting. Data ethicists and service users stressed that even in case the practices were found legitimate, the reasonable expectations of the data subjects had been betrayed. One of the users explained: 'When you're at that crisis point, you're not thinking, "Will this information be used for research?" You can spin it in a way that makes it sound good, but it feels like they are exploiting vulnerability in a way.'[18] Such a breach of trust can have an adverse impact on the entire healing process and discourage people in need to even come forward.[19]

Requiring users in a very vulnerable mental condition to read endless pages of privacy policy, often written in 'legalese', in a moment when they are already struggling and looking for help, is an extra burden that not even people in a perfectly healthy condition take on. A study on the general attitudes and experiences with privacy policies and laws by the Pew Research Centre concluded that only 9 per cent of US Americans 'always' read the privacy policies they are asked to agree to, 13 per cent 'often' do; the majority of 38 per cent instead read them only 'sometimes' and 36 per cent 'never'.[20] Out of the roughly 60 per cent of Americans who do read the policies only 22 per cent read them 'all the way through'.[21] Among the same 60 per cent who read privacy policies, 13 per cent understand 'a great deal' of what they are reading, whereas 55 per cent comprehend 'some', 29 per cent 'very little' and 3 per cent 'none'.[22]

Shortly before, a similar case had caused a scandal in the USA, when the suicide hotline 'Crisis Text Line' was sharing data with its for-profit spinoff 'Loris.ai'. The same concerns over full anonymization were raised, and one of the chief science and digital officers boiled it down to the essence when he explained that if data is being traced back to specific individuals 'your name could be associated with a suicide hotline . . . It's a lot different than someone just understanding your cholesterol'.[23] The backlash was so intense that the suicide hotline had to end the data-sharing relationship stating: 'We understand that you don't want Crisis Text Line to share any data with Loris, even though the data is

14 Bridie Witton, 'Coronavirus: Calls to Regulate "wild west" of Mental Health Apps during Covid-19 Recovery' In: *Stuff* (New Zealand) (16 May 2020) <https://www.stuff.co.nz/national/health/coronavirus/121524709/coronavirus-calls-to-regulate-wild-west-of-mental-health-apps-during-covid19-recovery> accessed 31 May 2022.

15 Isobel Whitcomb, 'Mental Wellness Apps are Basically the Wild West of Therapy. Therapy Apps are Booming, but Mental Health Experts have Vetted Precious Few' (2022) <https://www.popsci.com/science/mental-health-apps-safety/> accessed 30 May 2023.

16 Privacy International, Report: 'Your mental health for sale' (2019) <https://privacyinternational.org/node/3193> 30 May 2023.

17 Fars News Agency, 'Report: Mental Health Helpline Funded by Royals Shared Users' Conversations' (Farsnews 20 February 2022) <https://www.farsnews.ir/en/news/14001201000732/Repr-Menal-Healh-Helpline-Fnded-by-Ryals-Shared-Users%E2%80%99-Cnversains> accessed 26 January 2023.

18 Ibid.

19 Ibid.

20 Brooke Auxier and others, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control over their Personal Information' Pew Research Center (15 November 2019) 38 <https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf> accessed 30 May 2023.

21 Ibid.

22 Ibid 39.

23 Alexandra S Levine, 'Suicide Hotline Shares Data with for-Profit Spinoff, Raising Ethical Questions' (2022) <https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617> 26 January 2023.

handled securely, anonymized and scrubbed of personally identifiable information.'[24]

The stigma around mental ill-health still weighs heavily. The kind of information processed by mental health apps is never losing relevance for a person's life and their behaviour, whenever it might be shared or processed. Unethical sharing/processing or a data breach can affect people's relationships, their career, and their reputation for the rest of their lives. When a cyberattack in October 2020 hit a Finnish mental health start-up, patients' notes including details about adultery, suicide attempts, paedophilic thoughts and abuse have found their way into the dark net. Following this, many patients, among them politicians and public figures, have been blackmailed.[25] One of the reports in the media described the fears of one of the victims:

> 'Being honest about my mental health turned out to be a bad idea,' Jere says. He worries about identity theft, about some debt collection company calling him out of the blue and demanding tens of thousands of euros. He worries that his history of teenage alcoholism, so well documented on the web, will make it hard for him to find meaningful work as an adult. And he still worries that his mother may read his file one day. It's somewhere in the ether, accessible to anyone.[26]

A robust regulatory framework for e-mental health should be incorporated into the European mental health strategy from the onset

During the COVID-19 pandemic, policymakers in the EU have started placing emphasis on mental health, likely in response to the rising costs for public health systems and the economy. Even before the start of the pandemic, statistics indicated that mental illness impacted over 84 million people in the EU (that is 1 in 6); around 5 per cent of the working-age population had a severe mental health condition with a further 15 per cent affected by a more common condition resulting in reduced employment prospects, productivity, and wages.[27] It is reasonable to assume, that these numbers have increased during the pandemic. In addition to pandemic-related stress, the war in Ukraine, rising costs of living and uncertainty about the future have added new stresses. Mental and behavioural disorders account for 4 per cent of yearly deaths in Europe and are the second leading cause of death among young people.[28]

Already in July 2020, the European Parliament called for an 'EU Action Plan 2021-2027 on mental health, with equal attention being paid to the biomedical and psychosocial factors of ill mental health'.[29] Since spring 2022, EU policy initiatives addressing mental health are gaining momentum. At the Conference on the Future of Europe in May 2022, European citizens requested new initiatives or proposals by the Commission on how to improve the understanding of mental health issues and how to better address them across Europe. Moreover, the citizens called for action by the Commission to develop an EU Action Plan on mental health that would provide a long term Mental Health Strategy.[30] In June 2022, the European Commission presented its Healthier Together Initiative to combat non-communicable diseases, which make mental health and neurological disorders a focal point. In July 2022, the European Parliament adopted a resolution on mental health in the digital world of work.[31,32] In September 2022, Commission President Ursula von der Leyen announced in her State of the Union Address 2022 a new initiative on mental health for 2023.[33] In order to gather feedback from experts and stakeholders, the European Commission has launched a Call for evidence on a comprehensive approach to mental health in early 2023.[34]

In June 2023, the Commission published a Communication on a comprehensive approach to

24 John Hendel, 'Crisis Text Line Ends Data-sharing Relationship with for-Profit Spinoff' (2022) <https://www.politico.com/news/2022/01/31/crisis-text-line-ends-data-sharing-00004001> accessed 27 January 2023.

25 See William Ralston, 'They Told Their Therapists Everything. Hackers Leaked It All' (Wired 05 April 2021) <https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/> accessed 30 May 2023.

26 Ibid.

27 European Commission, Call for Evidence for an Initiative, Ref. Ares (2023)394636 (18 January 2023), 2.

28 Ibid.

29 European Parliament resolution of 10 July 2020 on the EU's public health strategy post-COVID-19 (2020/2691(RSP)) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0205_EN.html> accessed 13 February 2023.

30 Conference on the Future of Europe, Report on the final outcome (2022) 51 <https://www.europarl.europa.eu/resources/library/media/20220509RES29121/20220509RES29121.pdf> accessed 10 June 2023.

31 European Commission, 'EU Non-communicable Diseases (NCDs) Initiative: Guidance Document' (2022) <https://health.ec.europa.eu/publications/eu-non-communicable-diseases-ncds-initiative-guidance-document_en> accessed 29 January 2023.

32 European Parliament resolution of 5 July 2022 on mental health in the digital world of work (2021/2098(INI)) <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0279_EN.html> accessed 29 January 2023.

33 Ursula von der Leyen, 'State of the Union Address 2022' (2022) <https://state-of-the-union.ec.europa.eu/system/files/2022-09/SOTEU_2022_Address_EN.pdf> accessed 29 January 2023.

34 European Commission, 'A Comprehensive Approach to Mental Health' <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13676-A-comprehensive-approach-to-mental-health_en> accessed 13 February 2023.

mental health and announced to allocate €1.23 billion to address the mental health crisis.[35]

The EU's commitment to creating a comprehensive mental health strategy is encouraging, and the initiatives resonate with recommendations by international organizations like the WHO, which has identified (i) governance and leadership, (ii) finance, (iii) public awareness, and (iv) competencies for mental health care as key areas for action.[36]

However, such a European mental health strategy should include e-mental health as one of its components. Digital tools complement traditional therapy, they offer novel research and treatment options, and they have the potential for better accessibility, availability, affordability, and scalability.[37] The Commission would be ill-advised not to consider the benefits of e-mental health for a comprehensive mental health strategy. In fact, the call for evidence itself outlines that it aims to achieve improved access to treatment and care as well as to address cross-cutting issues, such as research, development, and innovation, including the role of digital tools.[38]

The WHO considers the development of global and national frameworks critical for achieving a meaningful change in mental health.[39] As the European mental health strategy is being developed, it is crucial to incorporate a robust framework for e-mental health from the onset, rather than missing the opportunity in the planning stages. Addressing bad practices in privacy and data protection as well as doubts about efficacy will play a key role in such a framework.

Australia is leading the way with a new regulatory regime for e-mental health

While the EU is still in the early days of developing a general comprehensive strategy for mental health, other jurisdictions, such as Australia and Canada are already taking a more refined approach and are establishing suitable regulatory frameworks for the specialized sector of e-mental health.[40]

Australia has been the first country to adopt an integrated set of specific regulatory instruments for e-mental health devices. The Australian focus on the regulation of e-mental health tools relates to a variety of reforms and policy decisions. In 2017, the Council of Australian Governments have endorsed the 5th National Mental Health and Suicide Prevention Plan.[41] In order to implement integrated planning and service delivery at the regional level in cooperation with Primary Health Networks and Local Health Networks, the Prevention Plan outlines that Governments shall identify and harness 'opportunities for digital mental health to improve integration' (Action 2). Further, Governments were asked to develop, implement and monitor national guidelines to improve coordination of treatment and support for people with severe and complex mental illness and to 'identify opportunities for the use of digital mental health and electronic health records in coordinating care' (Action 9). Finally, the Prevention Plan provides that a National Digital Mental Health Framework shall be developed (Action 32). Along with these plans, the Australian Government has provided substantial funding to digital mental health services (eg organizations that offer an app, telehealth psychology services, online Cognitive behavioral therapy treatments, chatbots, etc.) since 2017 to support their operations. To ascertain the safety and high quality of all funded services, the Government initiated the development of a safety and quality assurance framework.

The following analysis of the prevailing legal framework for e-mental health tools in the EU will draw inspiration from selected parts of the new Australian regulatory regime. A glance beyond European legislation can perhaps inform the debate on possible policy options to bridge eventual regulatory shortcomings.

Data protection law and product safety law together build the basic legal framework

A framework for e-mental health needs to address both critical factors: maintaining good data protection and privacy practices, and adopting an evidence-based approach to ensure patient safety and efficacy. In the EU, these factors are safeguarded through laws governing data protection and product safety. The General Data

35 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a comprehensive approach to mental health', COM(2023) 298 final.

36 WHO, 'World Mental Health Report: Transforming Mental Health for All' (2022), xvii.

37 World Economic Forum and Deloitte, 'Global Governance Toolkit for Digital Mental Health: Building Trust in Disruptive Technology for Mental Health', White Paper (2021), 15.

38 European Commission, Call for Evidence for an Initiative, 3.

39 WHO, 'World Mental Health Report: Transforming Mental Health for All' (2022), xvii.

40 The Mental Health Commission of Canada is currently introducing a National Assessment Framework for e-Mental Health Apps.

41 Commonwealth of Australia as represented by the Department of Health, 'The Fifth National Mental Health and Suicide Prevention Plan' (2017) <https://www.mentalhealthcommission.gov.au/getmedia/0209d27b-1873-4245-b6e5-49e770084b81/Fifth-National-Mental-Health-and-Suicide-Prevention-Plan.pdf> accessed 27 January 2023.

Protection Regulation (hereinafter referred to as 'GDPR') [42] builds the general legislation for the protection of personal data, and the Medical Devices Regulation (hereinafter referred to as 'MDR')[43] is the applicable product safety law for medical devices. While the GDPR is a horizontal legislation and applies to all personal data, regardless of the sector, industry or activity in which the data is being processed, the MDR is a sectoral law and applies only to classified medical devices.

Within or beyond the scope of the medical devices legislation?

The MDR establishes a stringent framework of documentation and monitoring to ensure a thoroughly regulated environment, which determines the level of oversight to guarantee a patient's safety. Product safety laws that apply to the specific medical sector typically require providing clinical evidence. The MDR stipulates that all admitted medical devices have to undergo clinical evaluation as part of the general safety and performance documentation requirements.[44]

Article 1 MDR determines the scope of the regulation: The MDR lays down the rules for placing on the market, making available on the market or putting into service of medical devices. Article 2(1) MDR defines (digital) medical devices as any 'software ... intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes'. The next section lists medical purposes, such as 'diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease', and thus includes the common features and objectives of e-mental health tools.

Products that do not have an intended medical purpose are instead beyond the scope of the MDR. Recital 19 MDR states explicitly that 'software intended for lifestyle and well-being purposes is not a medical device'. None of the requirements under the MDR applies to applications that only have a lifestyle or well-being purpose. With regard to product safety, mental well-being tools for the consumer health market are therefore subject to only minimal requirements by the General Product Safety Directive (2001/95/EC, hereinafter referred to as 'GPSD').[45] The GPSD is the lex generalis for product safety in the EU and serves as a horizontal safety net: The directive applies to all consumer products when there are no specific provisions. Due to its nature as a general directive rather than a sectoral norm, the GPSD does not foresee any sector-specific requirements such as, for example, proof of clinical evaluation. Sector-specific requirements must be incorporated in sectoral legislation.

The EU adheres to a strict distinction between medical devices and consumer health products ignoring the grey zone there between

The main decision whether an application will or can be admitted as a medical device or not lies with the manufacturer (argumentum: 'as intended by the manufacturer' Article 2 MDR). The intended purpose of a device is further specified in Article 2(12) MDR 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'. Evidently, the provision points to choices made by the manufacturer.[46]

The MEDDEVs, the medical devices documents, provide some further explanation with regard to the 'intended purpose'. MEDDEVs are not legally binding; however, they represent a guidance document and are expected to be followed.[47] They are drafted by authorities charged with safeguarding public health and stakeholders (eg industry associations, health professionals associations, notified bodies, and European standardization organizations). MEDDEV 2.1/6 clarifies that '[i]t should be noted that only the intended purpose as described by the manufacturer of the product is relevant for the qualification and classification of any device and not by virtue of the way it may be called'.[48] It is therefore the manufacturer, and no one else, who determines the intended purpose of a device.

If a manufacturer decides on an intended medical purpose and begins the process of obtaining medical device certification, the requirements vary depending on

42 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 2016 L 119/1.

43 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 (hereinafter referred to as MDR), OJ 2017 L117/1.

44 Art 61 MDR.

45 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ 2001 L 11.

46 See also Friederike von Zezschwitz, 'Neue regulatorische Herausforderungen für Anbieter von Gesundheits-Apps' (2020) 38 MedR 196–201 <https://doi.org/10.1007/s00350-020-5482-6> accessed 30 May 2023.

47 Guidance MEDDEVs <https://health.ec.europa.eu/system/files/2022-01/md_guidance_meddevs_0.pdf> accessed 27 January 2023.

48 European Commission, 'Medical Devices: Guidance document. MEDDEV 2.1/6' (2016), 9 <https://ec.europa.eu/docsroom/documents/17921/attachments/1/translations> accessed 27 January 2023.

the level of risk associated with the device. For manufacturers of digital devices, the implementation of the MDR has introduced some unfavourable provisions compared to the former Medical Devices Directive (93/42/EEC).[49] Previously, digital devices lacked specific regulations concerning the appropriate risk class. In the absence of specific rules, digital devices were mostly classified as low-risk class I devices. The MDR updated the details for the appropriate risk class with regard to software and imposed a significantly more rigorous regulatory framework. Rule 11 Annex VIII MDR now determines the risk classification of software as follows:

> Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause:
>
> death or an irreversible deterioration of a person's state of health, in which case it is in class III;
> or a serious deterioration of a person's state of health or surgical intervention, in which case it is classified as class IIb.
>
> Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring of vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.
> All other software is classified as class I.[50]

By applying a broad interpretation, any e-mental health device with an intended medical purpose can be understood to be either 'diagnostic' or more importantly 'therapeutic'. As a result, e-mental health tools are now most likely classified under risk category IIa as software 'to provide information which is used to take decisions with diagnosis or therapeutic purposes'.[51]

The de-facto up-classification of most software from risk class I under the former directive to risk class IIa in the MDR has caused significant confusion among manufacturers and consultants.[52] The difference between risk class I and risk class IIa is essential for the manufacturer because the higher the risk class, the more demanding the requirements that must be met. Risk class I devices have only moderate requirements and involve a mere self-assessment scheme. In contrast, the requirements for risk class IIa are considerable. They include extensive technical documentation, a certified quality management system, including post-market surveillance, and the involvement of notified bodies. From a manufacturer's point of view, the requirements under risk class IIa are time-consuming, they are cost-intensive, and they take a significant amount of extra effort compared to risk class I. According to reports, risk class IIa delays the market entry of a medical device by approximately one year and generates audit costs of a mid-five-figure sum.[53]

The tempting alternative for manufacturers, particularly for manufacturers of e-mental health tools, is therefore to circumvent the strict requirements under the MDR and to bring the device on the market as a simple consumer health product.[54] Unlike physical health conditions, mental health cannot be measured, quantified, or scaled easily by exact figures. Proving manufacturers wrong when they declare their tool merely for 'well-being' purposes as opposed to a medical purpose is close to impossible. It will be feasible where it is factually obvious, such as with an invasive Brain–Computer Interface to treat psychiatric diseases, to use a drastic example, or where the labelling or the instructions describe distinct medical conditions and/or use distinct medical terms, such as 'this device is used to treat bipolar disorder'. If the device is instead operating in the grey zone, where the lines between mental health and well-being get blurry, and the manufacturer willingly avoids any of these clear indicators in the description, no close reasoning can challenge the decision of the manufacturer. The WHO describes mental health as 'a state of mental well-being that enables people to cope with the stresses of life, realize their abilities, learn well and work well, and contribute to their community' and as 'more than the absence of mental disorders'.[55] Similarly, the EU considers being mentally healthy as 'being capable of self-realisation, being at ease when forming relationships with others, contributing to community life and being productive at work'.[56] Holistic approaches like these are opposed to a clear line of distinction or clear features for mental health versus well-being. Compelling manufacturers of e-mental health devices to label their tools as medical devices against their will is therefore not a viable choice.

49 Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ 1993 L 169.

50 Rule 11 Annex VIII MDR.

51 Art 51(1) MDR in conjunction with Annex VIII, rule 11.

52 Oliver Eidel, 'The MDR Class I Software Situation' (2023) <https://openregulatory.com/mdr-class-i-software-situation/> accessed 29 January 2023.

53 Ibid.

54 See eg Helen Yu, 'Regulation of Digital Health Technologies in the European Union, Intended versus Actual Use' (2022) <https://doi.org/10.1017/9781108975452.009> accessed 27 January 2023.

55 WHO, 'Mental Health: Strengthening our Response' <https://www.who.int/news-room/fact-sheets/detail/mental-health-strengthening-our-response> accessed 26 January 2023.

56 European Commission, Mental Health <https://health.ec.europa.eu/non-communicable-diseases/mental-health_en> accessed 26 January 2023.

Nevertheless, it may be advantageous to strive for a wider range of e-mental health devices to be governed by the MDR. A certification under the MDR indicates that manufacturers are committed to complying with a variety of quality-related requirements. Although the MDR does not directly address the needs of the immediate patient/end-user, it places significant obligations on manufacturers, which, in return, contributes to advanced overall market security and indirectly benefits end-users. The MDR is the only sector-specific legislation that provides for the demonstration of efficacy. Moreover, reports suggest that the problems described in the e-mental health sector, including privacy-related issues, are more common with apps that do not include clinical intervention and are not subject to health regulation.[57]

With specific regard to confidentiality and data protection, the MDR stipulates that all parties involved 'shall respect the confidentiality of information and data obtained in carrying out their tasks'.[58] Article 110 MDR points to the General Data Protection Directive, now replaced by the GDPR. Annex I MDR specifies the general safety and performance requirements. Therein, section 17.2 stipulates that 'software shall be developed and manufactured in accordance with the state of the art taking into account the principles of the development life cycle, risk management, including information security, verification and validation'. In addition, manufacturers of medical devices have to respect minimum requirements concerning hardware, IT network characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended according to section 17.4. As for active devices and devices connected to them, section 18.8 provides that they need to be designed and manufactured in order to 'protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended'. Beyond regular GDPR requirements, the MDR therefore puts an additional emphasis on enhanced information security.

As it currently stands, however, the up-classification of risk levels for software in the MDR reduces the attractiveness of certifying an e-mental health tool as a medical device, especially for borderline cases where the intended purpose of the device falls somewhere in between a clear medical purpose and a more general well-being purpose.

Australia integrates e-mental health tools and consumer e-health products into the medical devices system by exempting them

Australia's ambitions and activities to engage in e-mental health services have a longer tradition compared to most European countries. Australia's response to the regulatory challenge described above might therefore show new pathways with regard to the regulation of e-mental health tools. Similar to the European framework, Australia, too, has regulated medical devices separately. Chapter 4 of the Therapeutic Goods Act (hereinafter referred to as 'TGA')[59] relates to medical devices; matters to ensure the safety and satisfactory performance of medical devices are regulated therein. Details concerning classification rules, essential principles and conformity assessment procedures are specified in the Therapeutic Goods (Medical Devices) Regulations 2002.[60]

According to section 1(a) of provision 41BD of the TGA, a medical device is 'any instrument, apparatus, appliance, software, ... intended, by the person under whose name it is or is to be supplied, to be used for human beings for the purpose of one or more of the following: (i) diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease'.[61] Essentially, this includes the devices that are covered by the MDR in the EU. In section 2, the 'purpose' is legally defined. Again, the similarities with the MDR are evident:

> For the purposes of paragraph (1)(a), the purpose for which an instrument, apparatus, appliance, software, ... is to be used is to be ascertained from the information supplied, by the person under whose name the main equipment is or is to be supplied, on or in any one or more of the following: (a) the labelling on the main equipment; (b) the instructions for using the main equipment; (c) any advertising material relating to the main equipment; (d) technical documentation describing the mechanism of action of the main equipment.

Typically, manufacturers are responsible for the design, production, packaging, and labelling of the device.[62]

The regulation based on the TGA explains in more detail the 'intended purpose' of a medical device: The intended purpose is defined therein as 'the purpose for which the manufacturer of the device intends it to be used, as stated in: (a) the information provided with the device; or (b) the instructions for use of the device; or

57 See Ashley Gold, 'Mental Health App Boom Raises Alarms' (2022) <https://www.axios.com/2022/05/02/mental-health-app-boom-raises-alarms> accessed 22 February 2023.

58 Art 109 MDR.

59 Therapeutic Goods Act 1989. Act No 21 of 1990 as amended, <https://www.legislation.gov.au/Details/C2023C00076> accessed 30 May 2023.

60 Therapeutic Goods (Medical Devices) Regulations 2002. Statutory Rules No. 236, 2002 made under the Therapeutic Goods Act 1989. <https://www.legislation.gov.au/Details/F2023C00032> accessed 30 May 2023.

61 Provision 41BD Section 1 lit (a) TGA.

62 See provision 41BG (1) TGA.

(c) any advertising material applying to the device; or (d) any technical documentation describing the mechanism of action of the device'.[63] Again, it is therefore the information supplied by the manufacturer that determines the purpose of use.

Similar to well-being devices under the MDR, health and lifestyle apps that are only sources of information or tools to manage a healthy lifestyle or contain other software that does not meet the definition of a medical device under Australian regulation, are not within the scope of the TGA.

In an attempt to better capture the regulatory needs and specificities of software-based devices, Australia has responded with a number of exclusions and an exemption for specific types of software products. The reforms entered into force in February 2021. Following the reform, consumer health products for the prevention, management as well as follow-up devices not providing specific treatment or treatment suggestions are among the software-based devices that have been excluded from TGA regulatory requirements.

Based on subsection 7AA(1) TGA, the Therapeutic Goods (Excluded Goods) Determination 2018 specifies the goods that are to be excluded from the TGA requirements.[64] Schedule 1 of the Determination excludes numerous consumer health products. Notably, digital mental health tools are addressed separately—and not as a mere subsection of consumer health and wellness products. The list encompasses consumer health devices for self-management (section 14A), consumer health and wellness products (section 14B), behavioural change and coaching software (section 14C), and, explicitly, digital mental health tools (section 14E):

14A software that is:

(a) intended by its manufacturer to be used by a consumer for the self-management of an existing disease, condition, ailment or defect that is not a serious disease or serious condition, ailment or defect; and

(b) not intended by its manufacturer to be used:
  (i) in clinical practice; or
  (ii) in relation to a serious disease or serious condition, ailment or defect; or
  (iii) for the purpose of diagnosis, treatment, or making a specific recommendation or decision about the treatment, of a disease, condition, ailment or defect that is not a serious disease or serious condition, ailment or defect

14B software, or a combination of software and non-invasive hardware, that is:

(a) intended by its manufacturer to be used by a consumer to promote or facilitate general health or wellness by measuring or monitoring (through non-invasive means) a physical parameter, such as movement, sleep, heart rate, heart rhythm, temperature, blood pressure or oxygen saturation; and

(b) not intended by its manufacturer to be used:
  (i) in clinical practice; or
  (ii) for the purpose of diagnosis, screening, prevention, monitoring, prediction, prognosis, alleviation, treatment, or making a recommendation or decision about the treatment, of a serious disease or a serious condition, ailment or defect

14C software that is:

(a) intended by its manufacturer to be used by a consumer to improve general health or wellness by coaching, or encouraging behavioural change, in relation to personal or environmental factors, such as weight, exercise, sun exposure or dietary intake; and

(b) not intended by its manufacturer to be used:
  (i) in clinical practice or to provide information to the consumer that would generally be accepted to require the interpretation of a health professional; or
  (ii) for the purpose of diagnosis, prognosis, or making a decision about the treatment, of a disease, condition, ailment or defect . . .

14E software that is a digital mental health tool (including a cognitive behaviour therapy tool) based on established clinical practice guidelines that are referenced and displayed in the software in a manner that is reviewable by the user . . .[65]

Accordingly, digital mental health tools that do meet the definition of medical devices (see above) are excluded from having to comply with the TGA requirements provided they:

- [follow] established clinical practice guidelines; and
- the guidelines are referenced and the reference to them is displayed in the tool; and

63 Section 'Dictionary' of the Therapeutic Goods (Medical Devices) Regulations 2002. <https://www.legislation.gov.au/Details/F2023C00032> accessed 30 May 2023.

64 Therapeutic Goods (Excluded Goods) Determination 2018 made under section 7AA of the Therapeutic Goods Act 1989 <https://www.legislation.gov.au/Details/F2022C00980> accessed 30 May 2023.

65 Schedule 1 Therapeutic Goods (Excluded Goods) Determination 2018.

- the user can clearly view the guidelines[66]

The criteria are mandatory and have to be met cumulatively.

The 'established clinical practice guidelines' are described as guidelines that have been published by health professional representative bodies and/or accredited health care providers, such as hospitals.[67] By introducing mandatory clinical practice guidelines as a precondition, Australia ensures that expert knowledge and sound evidence for digital mental health tools must be observed regardless of the exclusion from the majority of the requirements under the TGA. This is further illustrated in explanatory notes giving examples of software that is excluded versus software that remains to be fully regulated under the TGA. According to the notes, a new machine learning tool to diagnose, for example, severe depression from facial expressions and patient movement would remain under full regulation of the TGA as long as clinical trials have not yet been completed and no published guidelines are yet available.[68]

Australia thereby takes an interesting and innovative approach to accommodate software-based digital mental health tools under the existing regulatory framework for medical devices, by exempting them from what might seem an excessive amount of requirements and imposing some 'softer' requirements instead. The Australian legislator thus finds a way to integrate digital mental health tools within the systematics of the medical devices market and to retain oversight where deemed necessary.

Applied to the European legal framework, a similar special solution of 'conditioned exemption' for e-mental health tools could involve relieving manufacturers from a significant amount of requirements under the MDR, while at the same time imposing a limited number of substitutional ones. Dropping requirements perceived as disproportionate and focusing on a few substantial ones instead, could encourage manufacturers to not circumvent admittance for their devices as medical devices—and it could possibly help in keeping more devices within the systematics of medical devices, which allows for better oversight and overall standards in the sector.

Considering the two major concerns with regard to e-mental health devices—the lack of clinical evidence and the bad data protection practices—such a 'conditioned exemption' under the medical devices legislation could potentially even cover both aspects: mandatory proof of efficacy paired with a mandatory demonstration of data protection compliance. In fact, the list of substitutional requirements for the 'conditioned exemption' would be an excellent opportunity to introduce—mandatory—specifications addressing privacy, data protection and security. The Australian approach to mandate clinical practice guidelines in their 'conditioned exemption' for digital mental health tools could be further enhanced in the European context by requiring a mandatory demonstration of compliance with good data protection standards, for example, by implementing a co-regulatory instrument under the GDPR (eg a sector-specific data protection code of conduct or certificate as discussed in the following section).

In a broader sense, it can even be argued that requiring a mandatory demonstration of good data protection practices under a conditioned MDR exemption is consistent with the objectives of the MDR. The MDR's main objective is to 'ensure the smooth functioning of the internal market as regards medical devices, taking as a base a high level of protection of health for patients and users'.[69] The functioning of the market (for medical devices) and the protection of health are therefore at the heart of the MDR. Inadequate data protection practices have been shown to impede the ability to fully utilize the advantages of digital technologies for mental healthcare, ultimately causing harm to both personal and public health. The current practices encourage unethical data sharing or unauthorized access to the data, which can harm the health and recovery of patients: For example, it can reduce their confidence in therapy and have a negative impact on their healing process; it can even restrain them from seeking help and confronting their mental health issues. Furthermore, an EU-wide sector-specific co-regulatory tool to demonstrate compliance (eg an EU-wide data protection certificate) would facilitate the seamless movement of high-quality apps across Europe and thus improve the functioning of the internal market as regards classified e-mental health devices.

66 Department of Health Therapeutic Goods Administration (2022), 'Digital mental health: Software based medical devices' 1 <https://www.tga.gov.au/sites/default/files/digital-mental-health-software-based-medical-devices.pdf> 24 June 2022.

67 Department of Health Therapeutic Goods Administration (2022), 'Digital mental health: Software based medical devices' 2 <https://www.tga.gov.au/sites/default/files/digital-mental-health-software-based-medical-devices.pdf> 30 May 2023.

68 Australian Government Department of Health Therapeutic Goods Administration (2021), 'Examples of Regulated and Unregulated Software (Excluded) Software Based Medical Devices', Therapeutic Goods Administration (TGA) (Text, 11 October 2021) 14 <https://www.tga.gov.au/resource/examples-regulated-and-unregulated-software-excluded-software-based-medical-devices> accessed 30 May 2023.

69 Recital 2 MDR.

Complementing governance instruments for e-mental health tools

Compared to other jurisdictions, the EU has a reasonably robust data protection framework to rely on. Provided the data is personally identified or identifiable, the data being processed is within the scope of the GDPR, and all the principles and rights enshrined in the GDPR apply. Considering that the data in question is used for mental health purposes, the data meets the definition for data concerning health, ie 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about his or her health status'.[70] The Article 29 Working Party has laid the foundation for a very broad interpretation of the concept of health data in apps and devices, irrespective of whether the devices are considered as medical devices.[71] Consequently, the data meets the criteria for sensitive data according to Article 9(1) GDPR and thus enjoys the highest level of protection under the GDPR.[72]

Evidently though, the sector of e-mental health is suffering from severe compliance weaknesses with prevailing data protection law: As demonstrated above, users are frequently facing privacy policies that are vague, incomprehensible, or change over time, and they are confronted with a common habit of data sharing with third parties. Therefore, policy options that support better compliance with data protection law should be discussed proactively for the use case of e-mental health.

Co-regulation enshrined in European data protection law: code of conduct versus certification scheme

The EU has been exploring a more diverse legislative governance, including complementary models of governance, already since 2001.[73] Complementing governance models, such as soft or self- or alternative or co-regulation, present themselves as an additional option when the traditional command-and-sanction model of hard law leaves room for compliance weaknesses.[74] Understood as a regulatory tool to mediate between the binding nature of the strict rule of hard law and voluntary agreements between private actors, soft or co-regulation has become an integral part of the EU's toolbox for governance since then. Moreover, models of soft, self- or co-regulation do not require a legislative act, thus they avoid potential uncertainties and impasses that are all too familiar for legal procedures on community level.

In the EU data protection context, legislators have envisioned rather a model of co-regulation than pure self-regulation.[75] Co-regulation (or 'conditioned self-regulation'[76] or 'enhanced self-regulation'[77]), typically, fosters the implementation of a specific piece of legislation that has already been adopted. Hard law provides the legal framework, whereas the respective co-regulation instruments serve to add the details and to specify the framework. In addition, co-regulation regularly involves participation of a public actor for monitoring and overseeing the outcomes.

The two main co-regulatory instruments in the GDPR to mend a lack of compliance are the data protection code of conduct (CoC) and the data protection certification scheme.[78] Both constitute a complementary regulatory tool to increase compliance with the requirements of the GDPR.[79] Both require regulators to seek approval for the requirements for accreditation as well as for the certification criteria and to accredit private certification and monitoring bodies, which then certify and monitor the pre-approved criteria. Both can be taken on a European-wide regulatory level. Both could be a useful policy instrument to foster more compliance in the e-mental health market.

70 Art 4(15) GDPR.

71 See Art 29 Working Party, Annex - health data in apps and devices (2015) <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> accessed 23 February 2023.

72 The CJEU itself has expanded the scope of special category personal data concerning Article 9 GDPR in *Vyriausioji tarnybinės etikos komisija* (Case C-184/20), Judgment of 1 August 2022 (Grand Chamber), (ECLI:EU:C:2022:601).

73 See also Linda Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?' (2005) 9(1) Electronic Journal of Comparative Law.

74 See also Irene Kamara, 'Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'mandate'', (2017) 8(1) European Journal of Law and Technology.

75 For the regulatory approaches underpinning EU data protection law see: Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford (OUP 2015); Raphaël Gellert, *The Risk-Based Approach to Data Protection*, Oxford (OUP 2020).

76 Linda Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?' (2005) 9.1 Electronic Journal of Comparative Law 12.

77 Rotem Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-Regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review 10(3) <https://doi.org/10.14763/2021.3.1577> accessed 30 May 2023.

78 Art 40 GDPR and Art 42 GDPR.

79 For a detailed comparison between code of conduct and certification according to the GDPR see: Rotem Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review <https://doi.org/10.14763/2021.3.1577> accessed 30 May 2023.

CoCs as a regulatory tool for enhancing compliance with data protection regulations have a longer tradition in the EU. They have been laid out already in Article 27 of the Data Protection Directive (Directive 95/46/EC).[80] With regard to consumer health apps, the European Commission presented a draft for a 'Code of Conduct on privacy for mHealth apps' in 2016; first preparations for the draft started even in 2015 in response to the Commission's mobile health green paper consultation.[81] The proposal aimed at bridging some of the data protection gaps, which had become apparent already in the pre-GDPR era. The ultimate goal was to promote trust among the users and to provide a competitive advantage for the companies who were to apply the CoC.

Drafted by members of industry stakeholders with the support and supervision of the Commission and designed as a voluntary framework, the Code of Conduct on privacy for mHealth apps addressed some of the most pressing issues. The list of topics included guidelines for consent, purpose limitation, data minimization, privacy by design/default, data subjects rights and information requirements, data retention, security measures, principles on advertising in mHealth apps, the use of personal data for secondary purposes, disclosing data to third parties for processing operations, data transfers, personal data breach, and data gathered from children.

After the first critical feedback from the Article 29 Working Party, a reworked draft was submitted requesting approval under the Data Protection Directive in 2017. In 2018, the Article 29 Working Party published their assessment, and approval was denied. Since then, the activities around a CoC for mHealth apps have seemingly come to a halt, although the idea itself has not completely ceased to exist in the health sector.[82]

Different to the CoC, certifications according to Article 42 GDPR have been introduced only with the GDPR.[83] Moreover, the GDPR seems to have been only a cornerstone to a general trend for certification schemes as a legal instrument in EU law to foster and increase compliance; many of the new legislative pieces, such as the NIS Directive, the Cybersecurity Act, and the Artificial Intelligence Act were to follow this path.

Whereas the CoC is designed to be an instrument of specification and concretization of the principles and requirements of the GDPR,[84] data protection certificates are designed primarily to demonstrate compliance. Certifications are generally a stricter and more formalized way to realize and demonstrate GDPR compliance.[85] In comparison with CoCs, certifications might therefore also be slightly more expensive and more time consuming for a certain product or service to achieve.

Certification schemes help to show that the data protection responsibilities of the controller are respected, they demonstrate compliance by default and design and with the provisions on data protection, as well as adequacy of both technical and organizational measures.[86] In addition, certifications demonstrate sufficient guarantees for a processor and support the transmission of personal data to third countries by way of appropriate safeguards.[87] Moreover, they are considered indicators of risk mitigation and risk negotiation in case of sanctions.[88] The 'dual function' of data protection certifications—they allow 'controllers to achieve and demonstrate compliance to the regulatory authorities' and, at the same time, provide 'transparency to the market'—is one of the intriguing features of certifications under the GDPR.[89]

Data protection certifications improve general standards by setting a best practice model and serving as an accountability framework, they promote both legal compliance and transparency. However, and different

80 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281. For the history of code of conducts in the European data protection framework see eg: Rotem Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review <https://doi.org/10.14763/2021.3.1577> accessed 30 May 2023.

81 European Commission, Privacy code of conduct on mobile health apps <https://digital-strategy.ec.europa.eu/en/policies/privacy-mobile-health-apps> accessed 30 May 2023.

82 The Spanish Data Protection Authority has approved the first national industry code of conduct to enable compliance of clinical research and pharmacovigilance with the GDPR in 2022. <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-aprueba-primer-codigo-conducta-sectorial-desde-entrada-vigor-rgpd> accessed 10 june 2023.

83 For European-wide predecessors to the current data protection certifications according to Art 42 GDPR, such as the US–EU Safe Harbor Agreement (SHA) and the European Privacy Seal (EuroPriSe), see Rotem Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review <https://doi.org/10.14763/2021.3.1577> accessed 30 May 2023.

84 BeckOK DatenschutzR/Eckhardt, *DS-GVO*, (40. Ed. 1.11.2021), Art 42, Margin number 17, 18; Rainer Knyrim (ed), *Der DatKomm. Praxiskommentar zum Datenschutzrecht, DGSVO und DSG*, Wien (Manz 2018) art 42, Margin number 2.

85 It is, however, important to point out that mere demonstration of compliance is not equivalent to actual compliance.

86 Art 24(3) GDPR, Art 25(3) GDPR, Art 32(3) GDPR.

87 Art 28(5) GDPR, Art 46(2) GDPR. See also EDPB, 'EDPB Adopts Guidelines on Certification as a Tool for Transfers and an Article 65 Dispute Resolution Binding Decision Regarding Accor' (2022) <https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-certification-tool-transfers-and-art-65-dispute-resolution_en> accessed 30 May 2023.

88 Art 83(2) lit j GDPR.

89 Christopher Kuner and others, *The EU General Data Protection Regulation (GDPR), A Commentary* (Print publication date: 2020. Published to Oxford Scholarship Online 2021), Article 42, DOI: 10.1093/oso/9780198826491.001.0001.

from the CoC, certificates are not designed as a governance tool on an industry level. They rather focus on a single corporate level. Certificates are not for sectoral guidance but they are targeting individual organizations, developers, and manufacturers. Whereas a CoC only thrives when the entire sector, or at least a significant number of the entire group, understands the benefit from following best practices in their specific sector, certification schemes put an emphasis on the decision of individual companies.[90]

Most significantly and again in contrast with CoCs, data protection certifications are addressed specifically to data subjects, ie the users/consumers. Recital 100 GDPR is very clear in that certification mechanisms are directed towards the data subjects: their objective is to allow 'data subjects to quickly assess the level of data protection of relevant products and services'.[91] Data protection certifications, seals, and marks could thus contribute to facilitating consumer choice.[92] A sector-specific data protection certification for mental health apps would provide easier orientation for consumers and mental health professionals in a market that, at present, is very heterogeneous.

Certification marks or seals are an already well-established instrument in the consumer market. Whether it be for fair trade or organic products, consumers recognize the marks and they accredit a certain level of trust to the product. Studies suggest that companies who advertise products certified with an established seal or mark can achieve higher market prices for the same product; data protection certificates could thus become a stimulus for competition, companies that demonstrate compliance with a high level of data protection could benefit economically from their competitive advantage.[93] In the use case of e-mental health, trust and confidence in the product are valuable asset. A data protection certification could therefore even bear a financial advantage.

A data protection certification for e-mental health tools could serve multiple purposes at the same time, creating benefits for the users, individual companies, and, provided a critical number of manufacturers seek certification, the market sector.

Data protection certification schemes, contrary to CoCs, require third-party assessment. In fact, assessment by a certified body is one of the core elements of the certification scheme according to Article 42 GDPR. For the use case of mental health tools, third-party assessment for data protection compliance seems to be an essential feature considering the current compliance failures. It would be a much-needed additional level of protection for users in a space so notorious for its bad practices.

Unless enshrined as a mandatory requirement for a 'conditioned exemption' (as suggested above), certification schemes (as well as CoCs) rely on a voluntary basis—but once certified, strict mandatory requirements under close monitoring of the certifying authority have to be fulfilled.[94] Certificates are issued for a maximum of 3 years and can be withdrawn, should the criteria of the scheme no longer be met.[95] For consumers, this would be another layer of assurance compared to the CoC, which is valid until being revoked.

To this day, data protection certification schemes according to Article 42 GDPR have not yet fully enfolded their potential within the European data protection framework. Reasons given include, inter alia, a lack of awareness of such certification schemes, a lack of (public) incentives, and a lack of plurilingual information about them.[96] Moreover, stakeholders indicate that clear incentives for initiating a certification procedure will be needed. A study by the European Commission concluded that '[i]ndustry associations considered both financial incentives, training opportunities, better information (availability, market requirements) and certainty about the legal effect very significant.' [97]

However, the concept appears to be gaining momentum. Between January 2020 and February 2023, the European Data Protection Board (EDPB) issued altogether 21 opinions on approval of accreditation for accreditation of certifying bodies.[98] In the UK, which is no longer a member of the EU but is relying on a data

90 See Rotem Medzini, 'Governing the Shadow of Hierarchy: Enhanced Self-regulation in European Data Protection Codes and Certifications' (2021) 10(3) Internet Policy Review<https://doi.org/10.14763/2021.3.1577> accessed 30 May 2023.

91 Recital 100 GDPR.

92 See Ronald Leenes, 'Article 42 Certification' in Kuner and others (n 87).

93 Boris Paal and Daniel Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG*, München (3rd edn, C.H.BECK 2021), art 42; Knyrim (n 82) Margin number 4.

94 Art 42(3) GDPR.

95 Art 42(7) GDPR.

96 See Maximilian Kröpfl, 'Datenschutzrechtliche Zertifizierungen' in Dietmar Jahnel (ed), *Jahrbuch 19 - Datenschutzrecht*, Wien Graz (NWV Neuer Wissenschaftlicher Verlag 2019) 163–222, 167..

97 Irene Kamara and others, 'Data Protection Certification Mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Final Report' (2019), 157.

98 For a list of all Opinions in the context of legislative consultations with regard to Art 42 GDPR by the EDPB see the website of the EDPB <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en?f%5B0%5D=opinions_topics%3A748&page=0> accessed 30 May 2023. The first opinion regarded the UK (Opinion 4/2020 on the draft decision of the competent supervisory authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to art 43.3 GDPR) and was adopted on 29 January

regulation (UK GDPR) based on and (still) in utmost alignment with the GDPR, the Information Commissioner's Office (ICO) has approved the first four certification schemes, including an age check certification scheme and an age-appropriate design certification scheme.[99] The German Landeszentrum für Datenschutz Schleswig-Holstein has announced to pick up data protection certification again after a temporary stop for their (pre-GDPR) 'Datenschutz-Gütesiegel', which was induced by the entry into force of the GDPR.[100] The Luxemburg Data Protection Commission has adopted the GDPR–CARPA, the first certification mechanism to be adopted on a national and international level under the GDPR, in May 2022.[101] Finally, the EDPB has approved the very first European Data Protection Seal officially recognized in all EU Member States.[102]

The above-cited German DiGA system has recently announced their intentions for a similar regulatory initiative for DiGAs. Following the experiences over the first months into the DiGA programme, the responsible body, the Bundesinstitut für Arzneitmittel und Medizinprodukte, has published new, even stricter, data protection criteria in September 2022 that need to be met to qualify as a DiGA.[103] In order to increase data protection compliance, the respective Institution is developing a certification scheme that considers GDPR compliance in addition to the requirements under the DiGA system.[104]

Introducing a sector-specific certification mechanism for e-mental health tools that are recognized on EU-wide level would foster overall improvement of the data protection practices in a sector as sensitive as mental health and allow for smooth and free movement of quality devices across Europe. Enshrined in the medical devices legislation and/or enhanced with a variety of public incentives, it could encourage compliance so desperately needed in the sector. For manufacturers, who wish to remain beyond the scope of the medical devices legislation and bring their device to the market as consumer health product, such a certificate would still be available, albeit on a purely voluntary basis, to demonstrate their willingness to comply with good data protection standards.

Considering all arguments above and given a choice between the two instruments of co-regulation discussed, a data protection certificate appears to be the better-suited instrument for the use case of e-mental health compared to a CoC. A third option would be to combine the two instruments and to include the respective CoC as one of the criteria for the certification scheme.[105] Thereby, the EU regulators would create an even more balanced and well-orchestrated regime of co-regulatory instruments.

A comparative look into Australian regulation can again be insightful. Australia has in fact developed a co-ordinated regime of complementary regulation. This regime is specifically addressing consumer e-mental health tools beyond the scope of the medical devices legislation and introduces sectoral standards combined with an accreditation scheme. The Australian regime can be considered as an initial prototype put into practice, particularly in regards to some specific provisions for privacy and data protection.

Complementary regulation in Australia: sectoral standards and accreditation scheme

In parallel to the reforms of the TGA (see above) and with special regard to consumer e-mental health prod-

2020. The so far most recent opinion concerns Malta (Opinion 4/2023 on the draft decision of the competent supervisory authority of Malta regarding the approval of the requirements for accreditation of a certification body pursuant to art 43.3 GDPR), it was adopted on 3 February 2023.

99 For a list of all approved certification schemes by the ICO see their Certification Schemes Register <https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-register/> accessed 30 May 2023. Currently, the register contains the following approved certification schemes: ADISA ICT Asset Recovery Certification 8.0 [ICO-CSC/004:2], Age Check Certification Scheme (ACCS) [ICO - CSC /001], Age Appropriate Design Certification Scheme (AADCS) [ICO - CSC /002], UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services [ICO-CSC/005].

100 Unabhängiges Landeszentrum für Datenschutz, Datenschutz-Gütesiegel beim ULD <https://www.datenschutzzentrum.de/guetesiegel/> accessed 30 May 2023.

101 European Data Protection Board, 'The CNPD adopts the certification mechanism GDPR-CARPA' (2022) <https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en> accessed 30 May 2023.

102 European Data Protection Board, Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to art 42.5 (GDPR) <https://edpb.europa.eu/system/files/2022-10/edpb_opinion_202228_approval_of_europrivacy_certification_criteria_as_eu_data_protection_seal_en.pdf> accessed 30 January 2023.

103 German Market Access Simplified, 'BfArM Tightens Data Protection Requirements for DiGAs – A New Certification is Needed' (2022) <https://germanmarketaccesssimplified.com/bfarm-tightens-data-protection-requirements-for-digas-a-new-certification-is-needed/> accessed 27 January 2023. See also: Bundesinstitut für Arzneimittel und Medizinprodukte, DiGA und DiPA Datenschutzkriterien <https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datenschutzkriterien/_node.html;jsessionid=7A7A4826B6BB783D6F4EDBC8734A01AC.intranet261> accessed 30 January 2023.

104 See <https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datenschutzkriterien/_node.html> accessed 30 January 2023.

105 A combination of a CoC and a certification has, eg already been suggested in Knyrim (n 82), Margin 2 and 27.

ucts, Australia has released the 'National Safety and Quality Digital Mental Health (NSQDMH) Standards'.[106] The NSQDMH Standards, developed by the Australian Commission on Safety and Quality in Health Care and at present voluntary in nature, are addressed at the service providers. They intend to improve service provision and to protect service users as well as their support people from harm by offering yet another regulatory pathway for certain digital mental health services. The Standards complement the TGA regulatory provisions, they have to be seen separately, but in combination with the TGA.

Officially released on 30 November 2020, the NSQDMH Standards define digital mental health services as 'services, whether they are information services, digital counselling services, treatment services (including assessment, triage and referral services), or peer-to-peer services, and irrespective of the digital medium through which they are provided'.[107] In the supplementing 'Guide for service providers', digital mental health services are defined even more granularly as 'a mental health, suicide prevention or alcohol and other drug service that uses technology to facilitate engagement and the delivery of care. This includes services providing information, digital counselling services, treatment services (including assessment, triage, and referral services) and peer-to-peer support services via telephone (including mobile phone), videoconferencing, the web (including webchat), SMS or mobile health applications (apps)'.[108]

The three sectors mentioned in the description, ie the distinct specialist mental health, suicide prevention, as well as the alcohol and other drug sectors (and together with them the cohorts that the services are provided to), are understood to be exhaustive. Moreover, the Standards specify that they are 'not intended to apply to more generic wellness services, which are not offering specific health services'.[109]

At the same time, the Standards emphasize that due to the voluntary nature of the Standards, service providers may themselves decide whether they want to apply them to the services they offer. Therefore, 'providers of generic wellness services may use relevant components of the NSQDMH Standards to guide their service delivery expectations, especially in technical areas such as privacy, transparency, security, costs and advertising, usability, and accessibility'.[110] This allows for an application of the Standards to all consumer health, mental wellness, and well-being applications, regardless whether they fit the description or not. Thus, the Standards represent an additional, complementary regulatory link between medical devices and consumer e-mental health products.

The Standards' objective is to complement existing regulation that applies to digital mental health services or their providers, such as 'consumer law, privacy and health records laws and principles, health practitioner registration, and regulation of medical devices, including software that meets the definition of a medical device'.[111] By themselves, however, these Standards are voluntary and can be considered a soft law instrument.[112]

The Standards consist of three components: clinical and technical governance standard, partnering with consumers standard and model of care standard. The three Standards include 59 actions and target clinical as well as technical aspects. Privacy protection of users and transparency about how their data is used as well as security and stability of the digital systems are enshrined in the clinical and technical governance standard.

Demonstrating compliance with relevant legislation and regulation as well as delivering best practices are among the main objectives of the NSQDMH Standards. With particular regard to privacy, the Standards demand a Privacy Impact Assessment (PIA).[113] Concerning privacy policies, the Standards explicitly require that

106 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards' (2020) <https://www.safetyandquality.gov.au/sites/default/files/2020-11/National%20Safety%20and%20Quality%20Digital%20Mental%20Health%20Standards%20%282%29.pdf> accessed 30 May 2023.

107 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards' (2020), 6 <https://www.safetyandquality.gov.au/sites/default/files/2020-11/National%20Safety%20and%20Quality%20Digital%20Mental%20Health%20Standards%20%282%29.pdf> accessed 30 May 2023.

108 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards – Guide for service providers' (2022), 12 <https://www.safetyandquality.gov.au/sites/default/files/2022-03/nsqdmh_standards_-_guide_for_service_providers.pdf> accessed 30 May 2023.

109 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards' (2020), 4 <https://www.safetyandquality.gov.au/sites/default/files/2020-11/National%20Safety%20and%20Quality%20Digital%20Mental%20Health%20Standards%20%282%29.pdf> accessed 30 May 2023.

110 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards – Guide for service providers' (2022), 12 <https://www.safetyandquality.gov.au/sites/default/files/2022-03/nsqdmh_standards_-_guide_for_service_providers.pdf> accessed 30 May 2023.

111 Ibid 9.

112 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards' (2020), 5 <https://www.safetyandquality.gov.au/sites/default/files/2020-11/National%20Safety%20and%20Quality%20Digital%20Mental%20Health%20Standards%20%282%29.pdf> accessed 30 May 2023.

113 Ibid, see Action 1.28.

the service provider has privacy policies for each service that are:
a. Easy to understand and transparent for service users and their support people
b. Uphold service users' rights and choices
c. Readily available to service users and their support people before accessing and while using the services
d. Compliant with privacy laws, privacy principles and best practice.[114]

Should changes to privacy policies occur, service providers are required to advise service users, and, where relevant, their support people in a timely and comprehensible way.[115] Data sharing with third parties is covered in Action 1.31 lit c on transparency: 'Information on who has access to their data, including through data sharing agreements, provision or sale to third parties, and if transfer of data outside of Australia occur.'

In support of the implementation of the Standards and again addressed at service providers, the Australian Commission has released a guide that provides practical advice on how to realize the NSQDMH Standards in order to improve safety and quality. The guide serves to translate the Standards and the related actions into practice.[116]

The actions concerning good practices of privacy policies have been outlined in the guide in remarkable detail. The implementing guidelines include regularly reviewing incidents, complaints and feedback from service users relating to privacy and confidentiality, setting up a mechanism that ensures that the policies and procedures are kept up-to-date and they consider possible changes to privacy legislation and regulations as well as conducting specific training for the workforce on privacy and confidentiality.[117]

As for Action 1.30 of the guide regarding the information on changes to the privacy policy, the guide gives concrete practical examples on how to materialize the Standards. It is suggested to include a specific requirement in the privacy policy to advise service users of substantial or material changes, specifying the format, which is to be used for notifications, assigning clear responsibilities for notifying service users, designing mechanism to record changes, and conducting regular audits on whether there have been changes to privacy policies and if so whether service users have been advised on that.[118]

In addition, Action 1.30 of the guide on transparency gives detailed information on typical data protection topics, such as data breaches, anonymity/pseudonymity/de-identification/re-identification of data, requests for information by external parties, and on the implications of a ceased service or in case a user dies.

Action 1.31 gives extensive but easily readable information on consent. Particularly with regard to good data-sharing practices, the guide proposes to set up a process for service users to negotiate the privacy terms, including an opt-out option of sharing. Otherwise, service users could be given a clear choice about the use of their data by specifying categories to which they give informed consent, for example, 'data used only to deliver the service', 'data shared or sold to third parties', and 'data used to assess eligibility or exclusion for products and services'.[119]

Overall and with regard to the sections dedicated to privacy and data protection, the NSQDMH Standards and the accompanying guide show a very practice-oriented approach and try to capture many of the well-known compliance weaknesses. Regarded as a complementary regulatory tool, the NSQDMH Standards set out to encourage better practices for the specific market sector of e-mental health. In that, the Standards show similarities to the intentions of a CoC.

However, the Australian regulatory framework has recognized that a voluntary standard addressed at the service providers alone might not be enough and has considered additional tools. In order to foster compliance, the Australian Commission on Safety and Quality in Health Care has developed an accreditation model for e-mental health services under the Australian Health Service Safety and Quality Accreditation (AHSSQA) Scheme, evaluation under the scheme has officially commenced in November 2022.[120] The accreditation scheme is designed for service providers and is meant to be assessed by accrediting agencies, which are approved through the AHSSQA Scheme. In alignment with the Standards, the accreditation model includes data protection and privacy features as well as sections on clinical evidence and care and consumer feedback.

114 Ibid, see Action 1.29.

115 Ibid, see Action 1.30.

116 Australian Commission on Safety and Quality in Health Care, 'National Safety and Quality Digital Mental Health Standards – Guide for service providers' (2022) <https://www.safetyandquality.gov.au/sites/default/files/2022-03/nsqdmh_standards_-_guide_for_service_providers.pdf> accessed 30 May 2023.

117 Ibid 95.

118 Ibid 96.

119 Ibid 105.

120 Australian Commission on Safety and Quality in Health Care, National Safety and Quality Digital Mental Health Standards <https://www.safetyandquality.gov.au/our-work/accreditation/australian-health-service-safety-and-quality-accreditation-scheme>; Assessment to the National Safety and Quality Digital Mental Health Standards <https://www.safetyandquality.gov.au/standards/national-safety-and-quality-digital-mental-health-standards/assessment-national-safety-and-quality-digital-mental-health-standards> accessed 30 May 2023.

Similar to the certification scheme under the GDPR discussed above, the Australian digital accreditation badge serves multiple purposes. It is a signal to the users that the service is safe and robust but equally, it can mean a competitive advantage for the individual manufacturer who demonstrates compliance. In combination with the Standards, it can foster overall better practices in the sector.

In terms of additional public incentives to increase adoption of the Standards and encourage accreditation, many state and territory governments in Australia are considering to make it mandatory for providers to implement the Standards and become accredited in order to tender for government funding. Moreover, a list of accredited providers online (a public register of every service that has undergone accreditation) will be established, which again will be pivotal for governments who fund digital mental health services and may assist service users and mental health practitioners in deciding whether to use or recommend a service.

Changes to the TGA and the introduction of NSQDMH Standards in Australia are however still in their early days. Empirical data on whether Australia's efforts will indeed be effective is therefore yet to be collected, and study results will have to be assessed thoroughly.

Conclusion

The deployment of digital technologies in mental health is facing two significant barriers: first, the current non-compliance in data protection and privacy; and secondly, the lack of demonstrated efficacy in devices that are not governed by the medical devices legislation. As EU policymakers are working on a comprehensive mental health strategy, it would be wise to integrate a robust regulatory framework for e-mental health addressing these challenges from the beginning. Such a framework would support the full utilization of digital technologies in mental healthcare and foster the sustainable development of European e-mental health industry.

This paper aimed to evaluate potential policy measures to enhance the present situation. It therefore analysed the prevailing European legal framework, assessed available co-regulatory instruments under the GDPR in response to existing shortcomings and examined recent Australian legislative reforms and regulatory initiatives to provide insight into possible solutions.

The EU approach to the regulatory grey zone between medical devices and consumer products for e-mental health is characterized by stiff adherence to two strictly differing legal regimes and by little regulation and oversight for consumer mental health tools. The MDR, the relevant sector-specific product safety law in the EU, imposes a regime of strict requirements, including the need for clinical evaluation, and a stringent framework of documentation and monitoring to ensure a highly regulated environment for classified medical devices. However, devices related to well-being and lifestyle fall outside the scope of the MDR, they are only subject to general product safety legislation.

The decisive factor that determines whether a device is admitted as a medical device, the 'intended medical purpose', is essentially based on choices made by the manufacturer. Admitting a device as a classified medical device is a costly and time-consuming process, which has become even more challenging with the introduction of new rules for software risk classification in the MDR. Manufacturers oftentimes choose to circumvent admission and bring the tool to the consumer health market as simple well-being product. The regulatory grey zone in between is left unaddressed by the EU legislator who adheres to the strict distinction between the two differing legal regimes.

Australia, in comparison, shows a more pragmatic response to this regulatory grey zone between medical devices and consumer health products. Recognizing that the typical requirements for medical devices are not entirely appropriate and fit for purpose for software in consumer health, and, in particular, in the e-mental health space, the Australian regulator has introduced a range of exceptions and exemptions—among them, exemptions for consumer health products and digital mental health tools. Noteworthy, the two sections are addressed separately. Both are now defined as specified goods according to a recent reform, and e-mental health devices are exempted from having to comply with the TGA, provided they comply with a limited list of (lighter) requirements.

If a similar approach of 'conditioned exemption' from the MDR for e-mental health tools were to be taken by the European legislator, the regulatory grey zone between medical devices and consumer mental health products could become more transparent and be managed more efficiently. By allocating e-mental health tools their special niche in the margins of medical devices and lifting the brunt of the requirements, there is a fair chance that more manufacturers would seek to stay within the systematics of medical devices. From a privacy point of view, the list of substitutional requirements for exempted e-mental health tools should be completed however by a mandatory demonstration of

compliance with data protection and privacy regulation, such as by a data protection certificate and/or a CoC. Enshrining such a co-regulatory data protection instrument in an eventual MDR exemption as a mandatory requirement would be an innovative regulatory choice in response to the current situation, initially perhaps unconventional but viable. Failing that, the implementation of these co-regulatory data protection instruments could also be encouraged by public incentives and/or remain entirely voluntary.

Meanwhile, the Australian Commission on Safety and Quality in Health Care is developing a coordinated regime of complementing regulation. At present, this regulatory regime is voluntary in Australia but a variety of public incentives is developed to further enhance implementation. The regime consists of sectoral standards and an accreditation scheme that includes, inter alia, a number of data protection and privacy features. By introducing the NSQDMH Standards, the Australian regulator proposes very detailed and practical guidelines for providers and developers. Special emphasis is put on compliance with privacy and data protection principles. The Standards are complemented by an accreditation scheme, identifiable through a badge.

Overall, aspects of the Australian legislative reforms and regulatory initiatives can provide the EU with a blueprint for how to integrate digital technologies into their comprehensive approach to mental health. Nevertheless, concerning matters of privacy and data protection, the EU has suitable legal instruments sui generis that await effective implementation.

https://doi.org/10.1093/idpl/ipad009
Advance Access Publication 27 June 2023