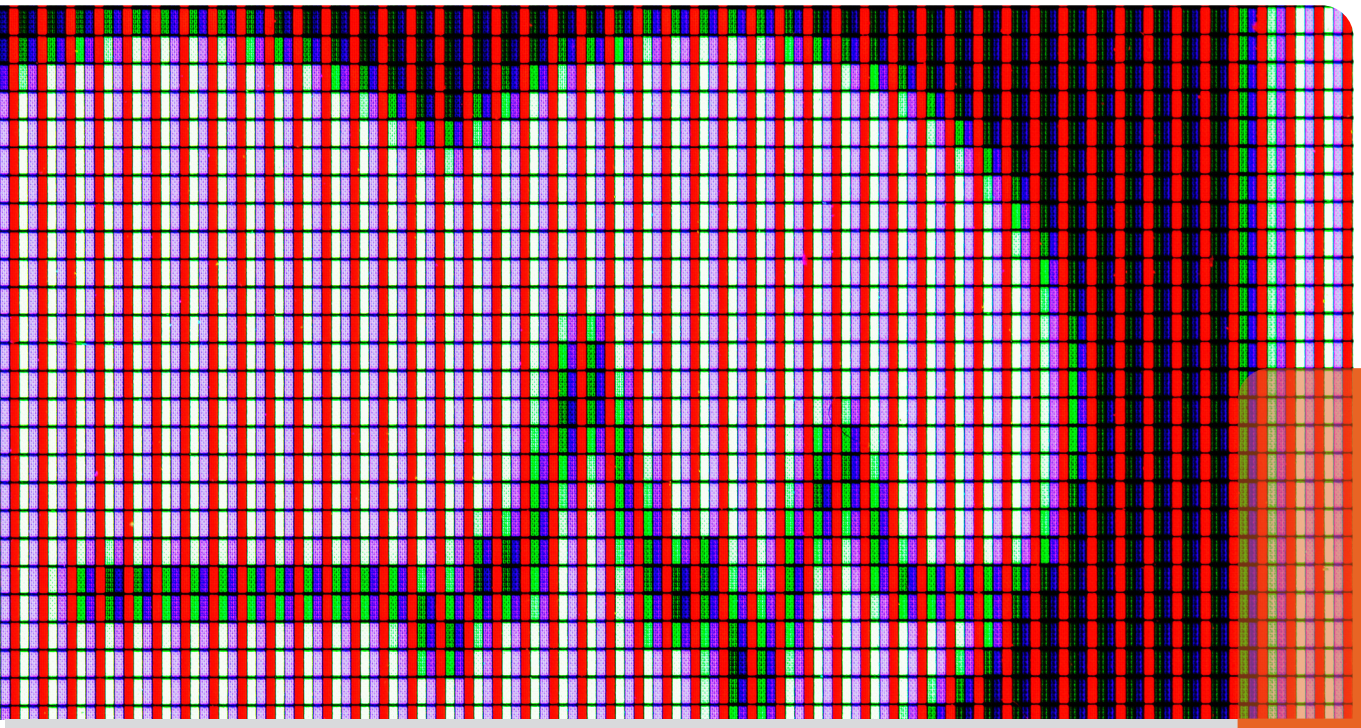
International
Comparative
Legal Guides



Digital Health

2024

Fifth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

glg Global Legal Group

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of "digital health" in Austrian law. The Austrian Federal Ministry of Health's definition (see https://www.sozialministerium.at/Themen/Gesundheit/eHealth.html) uses the term "e-health" as the general term, comprising the use of information and communication technologies in health-related products, services (including telemedicine) and processes. The Ministry uses the term "telemedicine" as referring to the provision or support of healthcare services using information and communication technologies, where the patient and the healthcare provider are not present in the same place. This is in line with the definition used by the European Commission, who suggested using the term "telehealth" as referring to health-related procedures and "telemedicine" as referring to treating people from a distance (see https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf , page 25).

1.2 What are the key emerging digital health technologies in your jurisdiction?

Key emerging technologies are, in particular, artificial intelligence (AI) applications including machine learning (ML), which can contribute, for example, to earlier disease detection and more accurate diagnosis.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health are: compliance with data protection laws (see sections 4 and 5); compliance with the requirement that only a licensed physician may give medical advice (see question 2.1); the technical requirements (see *GTelG 2012* in question 2.2); and the determination of whether a product qualifies as a medical device (see questions 2.1 and 3.1).

1.4 What is the digital health market size for your jurisdiction?

There is no reliable data available regarding the digital health market size for Austria, as the available statistics either do not refer to Austria in particular, or only consider specific segments of the total digital health market.

According to a market outlook as published by Statista (see https://de.statista.com/outlook/hmo/digital-health/oesterreich), the overall revenue for 2023 in Austria in the e-health sector amounts to approximately 649.1 million euros. According to the forecast, a market volume of 922.7 million euros will be reached in 2028, corresponding to an expected annual sales growth of 7.29%. However, this survey does not take into account the public e-health sector in Austria (which is the most relevant sector) as it only includes non-prescription e-health devices and apps.

In another study published by Roland Berger (see https://de.statista.com/statistik/daten/studie/1178751/umfrage/umsatz-auf-dem-markt-fuer-digital-health-weltweit/), the volume of the digital health market in 2026 in Germany is estimated to reach 59 billion euros. Consequently, one tenth of this (5.9 billion euros) could be assumed for Austria's digital health market volume in 2026 as a tentative estimate (due to the size ratio between Austria and Germany).

1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

As pointed out in question 1.4, there are no reliable figures available on the Austrian digital health market size. Therefore, we cannot provide an overview of the five largest digital health companies by revenue.

Further, please note that a major part of digital health solutions applied in Austria are organised by the Austrian state and implemented by the Umbrella Association of Austrian Social Insurance Institutions.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Austrian Physicians Act 1998, Federal Law Gazette I 169/1998, as last amended by the Federal Law Gazette I 108/2023 (*Ärztegesetz* 1998 (*ÄrzteG*)) contains, in principle, regulations on training and admission as a physician, regulations on the exercise of the profession (e.g. group practices), prohibitions of discrimination and regulations on the organisation of the self-administration of physicians (Medical Association). Section 3 of the *ÄrzteG* stipulates that medical advice may only be given by licensed physicians. Section 49 paragraph 2 of the *ÄrzteG* further stipulates that physicians shall practice their profession "personally and directly". This provision is regarded as not generally prohibiting telemedicine, i.e. the individual diagnosis

and treatment from a distance, without direct human contact. The Austrian Medical Association has stated that telemedicine might support the relationship between physician and patient and the treatment process; and that digital monitoring and online contact might be helpful for the diagnosis as well as for the therapy, but has emphasised that a clear legal framework is required for telemedicine services. Currently, no such specific legal framework is in place. In any case, physicians are obliged to comprehensively inform the patient and get the patient's informed consent (likewise), whereas in the case of telemedicine, they need to be in full control of the patient's situation and the telehealth treatment must be for the patient's benefit.

In the context of the referral of patients through online platform operators, the prohibition of commissions according to Section 53 paragraph 2 of the *ÄrzteG* must be observed, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. According to paragraph 3 *leg cit*, activities prohibited under paragraph 2 are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors but also for other third party (natural or legal) persons.

The Austrian Medicinal Products Act, Federal Law Gazette 185/1983, as last amended by Federal Law Gazette I 72/2023, (*Arzneimittelgesetz* (*AMG*)) implements a large number of European Union (EU) directives concerning regulations on medicinal products, in particular Directive 2001/83/EC – Community code relating to medicinal products for human use. The *AMG* contains regulations on the authorisation of medicinal products, regulations regarding marketing, advertising and distribution of medicinal products as well as quality assurance requirements.

The Austrian Medical Devices Act, Federal Law Gazette 657/1996, as last amended by Federal Law Gazette I 27/2023, (*Medizinproduktegesetz* (*MPG*)) as well as the Medical Device Regulation 2017/745 on medical devices (MDR), which entered into force on May 26, 2021, after having been postponed for a year due to the COVID-19 pandemic, constitutes the major regulatory framework for medical devices. The MDR lays down rules concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the EU. The MDR also applies to clinical investigations concerning such medical devices and accessories conducted in the EU.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The General Data Protection Regulation, Regulation 2016/679 (GDPR) contains central provisions on data protection. Although the GDPR as a regulation applies uniformly and directly throughout the EU, a large number of opening clauses allow national deviations by Member States. Providers of digital health in particular must take into account the provisions on the lawfulness of the processing of health data pursuant to Article 9 of the GDPR, as well as the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, pursuant to Article 32 of the GDPR.

The Austrian Data Protection Act, Federal Law Gazette I 165/1999, as last amended by Federal Law Gazette I 148/2021, (*Datenschutzgesetz* (*DSG*)) specifies the provisions of the GDPR and, in particular, contains provisions on proceedings before the Austrian data protection authority. For the private sector, the *DSG* does not provide any provisions for the processing of health data that deviate from the GDPR.

The Austrian Health Telematics Act 2012, Federal Law Gazette I 111/2012 as last amended by Federal Law Gazette I 82/2023, (*Gesundheits-Telematikgesetz* 2012 (*GTelG 2012*)) contains special regulations for the electronic processing of health data and genetic data (please refer to Article 4 Nos 13 and 15 of the GDPR) by healthcare providers. A healthcare provider in the meaning of health telematics is a professional who, as a controller or processor (in the meaning of Article 4 Nos 7 and 8 of the GDPR), regularly processes health data or genetic data in electronic form for the following purposes:

- medical treatment or care;
- nursing care;
- invoicing of health services;
- insurance of health risks; or
- exercise of patient rights.

The *GTelG 2012* also contains detailed regulations on the operation of *ELGA* by ELGA GmbH, which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions and the federal provinces or their health funds. *ELGA*, known as *Elektronische Gesundheitsakte*, means Electronic Health Records and is available to all persons receiving care in the Austrian healthcare system (see https://www.gesundheit.gv.at/gesundheitsleistungen/elga.html). In the context of *ELGA*, other e-health services have also been introduced, such as the electronic medication prescription (e-medication), the electronic vaccination pass (e-vaccination pass; see section 24b *et seq*. *GTelG 2012*, as well as eHealth Regulation, Federal Law Gazette II 449/2020, last amended by Federal Law Gazette II 53/2023) or recently the electronic Parent-Child-Pass (E-Parent-Child-Pass Act, Federal Law Gazette I 82/2023).

To meet the challenges of the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data via email and fax for healthcare providers were implemented to the *GTelG 2012* as well.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The *MPG* and the *MDR* (see question 2.1) likewise apply to consumer devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In connection with the *GTelG 2012* and Health Telematics Regulation 2013, as last amended by Federal Law Gazette II 506/2013 (*Gesundheitstelematikverordnung (GTelV 2013)*) the Federal Minister for Health is competent for notifications and for the operation of the eHealth directory service according to paragraphs 9 and 10 of the *GTelG 2012*.

In connection with the *ÄrzteG*, the competent authorities are the Austrian Medical Chamber, the respective state governor (*Landeshauptmann*) and the Federal Minister for Health.

The Federal Office for Safety in Health Care (*Bundesamt für Sicherheit im Gesundheitswesen* (*BASG*)) is the central regulatory authority for the medicinal products and medical devices industry. The BASG is responsible, among other things, for the approval of medicinal products, market surveillance and pharmacovigilance, notifications in connection with clinical trials, the control of advertising restrictions and the granting and review of operating licences.

Investigations and assessments are typically carried out by the Austrian Agency for Health and Food Safety (*Österreichische Agentur für Gesundheit und Ernährung* (*AGES*)) on behalf of the BASG.

The Austrian Data Protection Authority (*Datenschutzbehörde* (*DSB*)) is the supervisory authority, as defined in Article 4 Section 21 of the GDPR, for the monitoring of data protection law and the assertion of data subjects' rights under the GDPR.

2.5 What are the key areas of enforcement when it comes to digital health?

As far as can be seen, neither the Austrian Medical Chamber nor the *BASG* or the Federal Minister of Health recently took relevant enforcement measures in the regulatory area of digital health and healthcare IT.

In 2018, the *DSB* rendered a major decision regarding the communication between physicians and patients (DSB-D213.692/0001-DSB/2018): according to the *DSB*, patients cannot consent to the (unencrypted) transmission of health data (e.g. medical reports) by physicians. The *DSB* reasoned that the choice of the communication method is a technical/organisational measure according to Article 32 of the GDPR, and that no consent can be provided to insufficient technical/organisational measures.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

According to Recital 19 of the MDR, software qualifies as a medical device when it is specifically intended by the manufacturer to be used for one or more medical purposes, while software for general purposes, even when used in a healthcare setting, or software intended for lifestyle and well-being purposes is not a medical device. The qualification of software, as either a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device. Therefore, as a general rule, software for general purposes, even if used in the healthcare sector, is not a medical device. The manufacturer determines the intended use, which is essential for software for general purposes to be differentiated from a medical device.

According to the MDR, manufacturers of medical devices are obliged to carry out a clinical evaluation for all their products – regardless of the risk class – which also includes a post-market clinical follow-up. Such clinical evaluation is an essential task of the manufacturer and an integral part of a manufacturer's quality-management system (Article 10 paragraphs 3 and 9f of the MDR). The clinical evaluation is a systematic and planned process for the continuous generation, collection, analysis and evaluation of clinical data for a device. Through the clinical evaluation, the manufacturer verifies the safety and performance of his device, including the clinical benefit.

Furthermore, Regulation No. 207/2012 on electronic instructions for use of medical devices must be observed when providing electronic instructions for use.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

The terms "AI" or "ML" are generic and rather technology-neutral terms, as they represent a wide range of different kinds of technologies. To date, there is no definitive legal definition available in the Austrian or European jurisdiction and the European legislator is aiming to issue its AI Regulation (COM 2021/206) based on a rather technology-neutral level. *De lege lata*, the same regulations apply to AI and ML as to all other technologies, which means that for the healthcare sector, in particular, the MDR as well as the GDPR are relevant.

3 Digital Health Technologies

3.1 What are the core legal or regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Furthermore, the physician must decide in each individual case of such telehealth consultation, if he can sufficiently control possible dangers despite the lack of physical contact with the patient and whether he has a sufficient information basis for his decisions. In case the physician fears that he does not have a sufficient basis for his medical decision due to lack of physical patient contact, he must advise the patient to physically see a physician.
  Austrian law does not contain rules for the provision of telemedicine or virtual care services in general, but a specific regulation has been issued regarding the provision of teleradiology services: the Medical Radiation Protection Regulation, Federal Law Gazette II 375/2017, last amended by Federal Law Gazette II 353/2020 (*Medizinische Strahlenschutzverordnung*) provides that teleradiology is permitted within the framework of basic and special trauma care, as well as in dispersed outpatient primary care facilities of acute hospitals and otherwise only in order to maintain night, weekend and holiday operations for urgent cases.
  According to paragraphs 3 and 4 of the *GTelG 2012*, health service providers may transfer health data and genetic data only if:
  - the transmission is permitted under Article 9 of the GDPR;
  - the identity of those persons whose health data or genetic data is to be transmitted is proven;
  - the identity of the healthcare providers involved in the transmission is proven;
  - the roles of the healthcare providers involved in the transmission are demonstrated;
  - the confidentiality of the transmitted health data and genetic data is guaranteed; and
  - the integrity of the transmitted health data and genetic data is guaranteed.

  In addition, the *GTelG 2012* and *GTelV 2013*, issued by the Federal Minister of Health on the basis of the *GTelG 2012*, contain detailed regulations on encryption and technical implementation of communication.
  The COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services.
  As outlined above in question 2.2, due to the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data (via email and fax) for healthcare providers have been implemented to the *GTelG 2012*.
- **Robotics**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Furthermore, robotics may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. robotics for surgical purposes).
- **Wearables**
  Wearables may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes.

- **Virtual Assistants (e.g. Alexa)**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Virtual Assistants in general would not qualify as a medical device. However, natural language processing may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes.
- **Mobile Apps**
  See question 2.6 (Software as a Medical Device).
- **Software as a Medical Device**
  See question 2.6.
- **Clinical Decision Support Software**
  See question 2.6. Further, the GDPR, in particular its provisions on automated individual decision-making (Article 22 of the GDPR), must be considered in case personal data is processed.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  See question 2.6 (Software as a Medical Device) and section 8 (AI and ML).
- **IoT (Internet of Things) and Connected Devices**
  IoT and connected devices may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. blood pressure measurement using cloud recording); furthermore, the GDPR must be considered in case personal data is processed.
- **3D Printing/Bioprinting**
  Bioprinting raises a wide range of legal and ethical questions. Currently, no *sui generis* regulatory regime governing the entire bioprinting process is in place in Austria. According to the European Commission and the European Medicines Agency, tissue-engineered products might fall under the definition of advanced therapy medicinal products (ATMPs). Additionally, IP and, in particular, patent rights questions might arise.
- **Digital Therapeutics**
  Digital therapeutics is a rather broad term used for device-controlled therapy measures. In particular, digital therapeutics may be subject to the MDR as well as provisions of the GDPR. In view of its high-risk potential, digital therapeutic software shall, according to Annex VIII; Rule 11 of the MDR, be classified as a medical device of at least risk class IIa.
- **Digital Diagnostics**
  Digital diagnostics in the sense of device-controlled diagnostic measures may be subject to the MDR as well as the GDPR.
- **Electronic Medical Record Management Solutions**
  See questions 2.2 and 10.6 for detailed information on the *ELGA*, the Austrian central digital health solution, which also serves as an electronic medical record management solution. A very recent solution that is currently being implemented is the Parent-Child-Pass (see question 2.2).
- **Big Data Analytics**
  In particular, the GDPR must be observed when applying big data analytics. The *Data Governance Act (DGA)*, which entered into force in September 2023, intends to facilitate the re-use of protected data held by the public sector (e.g. personal data and/or commercially confidential data) which could be re-used under specific EU or national legislation.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The GDPR must be observed, as well as the *GTelG 2012*; no legislation is in place specifically governing blockchain technology.
- **Natural Language Processing**
  Natural language processing generally does not qualify as a medical product (e.g. speech recognition in dictation software). However, natural language processing may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes; furthermore, the GDPR must be observed.

3.2 What are the key issues for digital platform providers?

One of the main restrictions on digital platforms for individual healthcare is that medical advice may only be given by licensed physicians (Section 3 of the *ÄrzteG*; see question 2.1).

Furthermore, online platform operators should keep in mind the prohibition of commissions in Section 53 paragraph 2 of the *ÄrzteG*, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. Moreover, these activities are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors, but also for other third party (natural or legal) persons.

Digital platforms must take appropriate (high) technical/organisational measures for data security when processing health data (Article 32 of the GDPR) and the *GTelG 2012* must be considered in case personal health data is processed.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The processing of personal data must comply with the GDPR. When processing health data, Article 9 of the GDPR applies; according to that provision, the processing of health data in connection with healthcare providers is lawful only if (only the most relevant legal grounds have been included in the following):

- the data subject has given explicit consent to the processing of their personal data for one or more specified purposes (Article 9 Section 2 letter a of the GDPR);
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Article 9 Section 2 letter c of the GDPR);
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care, treatment or the management of health or social care systems (Article 9 Section 2 letter h of the GDPR);
- pursuant to a contract with a health professional, when the personal data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy (Article 9 Section 2 letter h in connection with Section 3 of the GDPR); and
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices (Article 9 Section 2 letter i of the GDPR).

4.2 How do such considerations change depending on the nature of the entities involved?

In principle, the provisions of the GDPR apply equally to all entities. However, the legal grounds in Article 9 Section 2 letter h only apply to data processing, when the personal data is

processed by or under the responsibility of a professional subject to the obligation of professional secrecy. Therefore, entities not subject to professional secrecy cannot rely on this legal ground.

4.3 Which key regulatory requirements apply?

The general regulatory provisions of the GDPR apply, namely the principles of transparency, lawfulness, purpose limitation, data minimisation, proportionality, accuracy, data security and accountability. As in the context of digital health services, large-scale processing of sensitive personal data will be involved, the entity providing such services is required to designate a Data Protection Officer in accordance with Article 37 para 1 lit c of the GDPR. Furthermore, a data protection impact assessment might be required (e.g. according to Article 35 para 3 lit b of the GDPR) before processing is started.

4.4 Do the regulations define the scope of data use?

Yes, please refer to question 4.1. Some legal grounds of Article 9 of the GDPR impose limitations on the purpose of the processing (e.g. preventive or occupational medicine; see question 4.1). Neither the GDPR nor the *DSG* contain regulations defining the scope of data use in the context of digital health.

4.5 What are the key contractual considerations?

If the processing is based on explicit consent of the data subject, such valid and fully informed consent must be given by the patient/data subject. Furthermore, according to Article 28 of the GDPR, any data controller must conclude a written data processing agreement with processors, which must contain the minimum contents specified therein. In the event where more than one controller jointly decides on the respective processing, an agreement on joint controllership must be concluded between these controllers.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues and therefore greatest challenge with regard to securing comprehensive rights to personal data is that the personal data must be collected in accordance with the principles pursuant to Article 5 of the GDPR and that a corresponding legal basis must be guaranteed for each processing at all times. Successfully facing those legal issues is not only important because of the severe penalties for the unlawful processing of personal data provided for in the GDPR (Article 83 of the GDPR); it is also vital for any digital (health) application using personal data to safeguard that such use is lawful as otherwise the application risks being shut down by the data protection authority at any time.

However, the GDPR is only applicable to personal data. Therefore, if no personal data according to Article 6 or Article 9 of the GDPR is processed, a specific right to process the data is not necessary from a data protection point of view.

4.7 How are issues with data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

A data subject may request the respective data controller to correct any inaccurate or incomplete personal data. If the data is not corrected by the processor or if the data subject is of the opinion that the processing of the personal data violates the GDPR, the data subject may file a complaint with the data protection authority and/or a (civil) lawsuit against the controller requiring the correction of the inaccuracy.

The Federal Act on Equal Treatment, Federal Law Gazette I 66/2004, as last amended by Federal Law Gazette I 115/2023 (*Gleichbehandlungsgesetz* (*GlBG*)) focuses on equal treatment in the world of work and in other areas. No one shall be discriminated because of his gender, age, ethnical affinity, religion or belief or sexual orientation. A person who is subject to discrimination can claim the establishment of the non-discriminatory condition and compensation for the pecuniary loss and for the personal impairment suffered.

The Federal Act on the Equality of Persons with Disabilities, Federal Law Gazette I 82/2005, as last amended by Federal Law Gazette I 32/2018 (*Bundes-Behindertengleichstellungsgesetz* (*BGStG*)) aims to eliminate or prevent discrimination against persons with disabilities. This is to ensure equal participation of persons with disabilities in society and to enable them to lead a self-determined life.

No one may be discriminated against on the basis of a disability. In the event of a violation of this prohibition, the person concerned is in any case entitled to compensation for the pecuniary loss and for the personal impairment suffered.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

The normal legal framework applies to data usage (i.e. GDPR, *GTelG 2012*, the Copyright Act with the text and data mining exception being implemented in section 42h Copyright Act) since, so far, no specific AI legal framework has been implemented.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Sharing health data between healthcare professionals is subject to the *GTelG 2012* (see question 3.1 for the conditions of sharing under the *GTelG 2012*), sharing of data between individuals other than healthcare professionals is solely subject to the GDPR; see question 4.1 for sharing within the EU. For sharing with an individual located outside the EU/EEA, the GDPR provisions on the transfers of personal data to third countries or international organisations apply.

5.2 How do such considerations change depending on the nature of the entities involved?

Sharing of data between individuals other than healthcare professionals is solely subject to the GDPR (see question 4.1). In this case, the *GTelG 2012* does not apply.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please refer to questions 4.3 and 5.1.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

One of the aims of the DGA, which entered into force in September 2023, is facilitating the re-use of protected data held by the public sector (e.g. personal data and/or commercially confidential data) which could be re-used under specific EU or national legislation. The DGA provides for rules and safeguards to enable such re-use of data whenever it is possible under other legislation.

Another European initiative, which builds upon the DGA, is the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, which intends to address health-specific challenges to electronic health data access and sharing by providing a framework for the secondary use of electronic health data.

5.5 What are the key issues to consider with respect to federated models of healthcare data sharing?

Federated models follow a relatively new ML approach, where each federated device shares its local model parameters instead of sharing the whole dataset used to train it (see https://edps.europa.eu/press-publications/publications/techsonar/federated-learning_en). As a consequence of the federated structure, key issues to consider are whether the local model parameters constitute personal data and if so, how data security, data accuracy, data integrity and confidentiality are handled. Please refer also to questions 4.3 and 5.1.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Technical inventions that are novel, that, considering the state of the art, are not obvious to a person skilled in the art, and that can be applied in the industry, can be subject to patent protection under the Austrian Patent Act 1970, Federal Law Gazette I 259/1970, as last amended by Federal Law Gazette I 51/2023 (*Patentgesetz 1970 (PatG 1970)*). If and insofar as a digital health technology meets the above-mentioned requirements, it can be subject to patent protection. Only a natural person can qualify as an inventor.

The inventor can either file a patent himself or transfer his right to a third party. The patent owner has the exclusive right to manufacture, put into circulation, offer for sale and use the patented invention for the duration of the patent, namely up to 20 years. A "prolongation" of the patent protection can only be achieved by virtue of a Supplementary Protection Certificate, a *sui generis* IP right available for specific medicines and plant protection products.

Software programs as such cannot be subject to patent protection.

6.2 What is the scope of copyright protection for digital health technologies?

Under Austrian law (the Austrian Federal Law on Copyright in Works of Literature and Art and on Neighbouring Rights, Federal Law Gazette I 111/1936, as last amended by Federal Law Gazette I 244/2021 (*Urheberrechtsgesetz (UrhG)*)), a work is defined as an "original intellectual creation" (Section 1 paragraph 1 of the *UrhG*). The author has the exclusive right to use his work in the way defined by the law (in particular: reproduction right; distribution right; rental and lending right; broadcasting right; right of public performance; and of communication to the public of a performance, making available right). Protection starts in the very moment of creation, which means that no registration with any authority is required for protection under the Copyright Act. According to Section 1 paragraph 1 of the *UrhG*, works can be original intellectual creations in the area of literature (including computer programs), musical arts, visual arts and cinematography. Digital health technologies can especially fall under the category "computer programs". In principle, only creations of human beings are regarded as works and protected by copyright; and the legislator has so far not provided for specific rules for "computer-generated works". According to current doctrine, computer-generated works may still be subject to copyright protection. The programmer as the author, although not directly involved in the creation of the work, has created the creative framework for it by programming the appropriate autonomy.

The Copyright Act further grants exclusive rights to performers (such as singers, dancers and actors) as well as phonogram producers, photographers, broadcasters and the producers of a database (*sui generis* right).

6.3 What is the scope of trade secret protection for digital health technologies?

The Unfair Competition Act, Federal Law Gazette I 448/1984, as last amended by Federal Law Gazette I 99/2023 (*Bundesgesetz gegen unlauteren Wettbewerb,* (*UWG*)) contains in its Sections 26a *et seq.* civil law and civil procedural law rules for the protection of trade secrets. According to the legal definition in Section 26b of the *UWG*, information that is:

- secret, namely not known or readily accessible by persons that normally deal with the respective information;
- of commercial value because of its secrecy; and
- subject to reasonable measures to be kept secret,

qualifies as a trade secret.

It must be proven that reasonable measures have been taken; these may include specific IT security measures and the restricted accessibility of secret information (e.g. only accessible to particularly trustworthy employees).

A variety of information may be regarded as a trade secret, for example, inventions and designs (if not protected as a patent or design) as well as not otherwise protected information such as production processes, customer information, business models or the like.

The owner of a trade secret is particularly entitled to claims of forbearance, removal and damages against anyone who unlawfully acquires, uses or discloses his trade secrets.

Section 26h of the *UWG* contains specific rules to ensure the protection of trade secrets in civil proceedings.

6.4 What are the rules or laws that apply to or regulate academic technology transfers in your jurisdiction?

Universities may claim any service invention made by one of its employees within three months of notification of the invention (see Section 106 paragraph 2 of the University Act 2002, Federal Law Gazette I 120/2002, as last amended by Federal Law Gazette I 52/2023, (*Universitätsgesetz 2002* (*UG 2002*)) in connection with the Patent Act's rules on service inventions); the employee is generally entitled to a special remuneration if the university makes use of that right. If the university does not claim the

invention, the general rule applies, namely, the inventor is entitled to the invention. Regarding the commercialisation of technology developed by its researchers, Austrian universities pursue different strategies – from outlicensing to transferring IP and increasingly, additionally acquiring shares in its spin-out companies.

6.5 What is the scope of intellectual property protection for software as a medical device?

There are no specific rules for Software as a Medical Device from an IP protection point of view, i.e. the software as such will be protected by copyright law; whether patent protection can be sought must be assessed individually.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

Exclusively natural persons can be named and registered as an inventor for patents, as the legal institution of an "e-person" is not recognised in Austrian law. If an AI device should "invent" a patentable product, this goes back to the actual inventor (natural person) of the AI device. According to the Patent Act, only human beings can qualify as inventors.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

In principle, the rules of the Patent Act regarding service inventions (section 7 *et seq.* Patent Act) apply to inventions made within academic (see question 6.4), or other public-funded institutions (see e.g. the Federal Act on General Matters Pursuant to Article 89 of the GDPR and the Research Organization (*Forschungsorganisationsgesetz*, (*FOG*)), Federal Law Gazette I 341/1981, as amended by Federal Law Gazette I 52/2023, and Federal Act on the Institute of Science and Technology Austria (*IST-Austria-Gesetz* (*ISTAG*)), Federal Law Gazette I 69/2006, as amended by Federal Law Gazette I 75/2020).

7 Commercial Agreements

7.1 What considerations should parties consider when dealing with collaborative improvements?

If not otherwise regulated, collaborative improvements belong to the respective inventors of such improvement, whereas the ownership of the basis technology will not change following such improvements. The ownership, and eventually licences regarding the use of such collaborative improvements, is therefore usually regulated precisely and meticulously in the respective agreements containing the regularities for the collaboration.

7.2 What considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Besides regulatory considerations (see question 2.1), the general principles apply, namely Austrian law's (federal) rules on commercial contracts, providing regulations on the general principles and specific contract types.

The general principles of contracts, as well as a large number of specific contracts, are regulated in the Civil Code (*Allgemeines Bürgerliches Gesetzbuch*) and in the Commercial Code (*Unternehmensgesetzbuch*).

7.3 What considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Parties should in general consider data governance. Please refer to questions 4.3, 5.1 and 5.5. In terms of data licensing, see question 8.2.

7.4 What considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties will need to consider that, according to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. See also above question 3.1 (in particular regarding *Telemedicine/ Virtual Care* and *Virtual Assistance*).

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Many digital health devices use ML (such as, e.g. in the field of radiology, and generally in diagnosing). ML is substantial for developing smart digital health solutions and is said to have the potential to substantially transform healthcare both for patients and medical professionals.

8.2 How is training data licensed?

The protection and licensing of training data does not differ from any other protection of information, creations and data. If the training data were created in a specific way by a human being (e.g. texts for speech recognition) they may be subject to copyright protection (see question 6.2). In addition, training data may also be subject to trade secrecy protection (see question 6.3). For using such data, a licence agreement must be concluded with the respective right holder.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Software may, in principle, be protected by copyright (see question 6.2). However, copyright protection requires an "intellectual creation" which, according to Austrian law, can only originate from the thoughts of a human being. Assuming that the improvement could have only been achieved because the programmer has "instructed" the algorithms correspondingly, it could be argued that the programmer is the author of the work (in other words, the improvement, which continues to depend on the basis work). In case the improvement was indeed created without active human involvement, it does not qualify for copyright protection.

8.4 What commercial considerations apply to licensing data for use in machine learning?

For the provision of data for use in ML, the licensor is often commercially interested not only in remuneration, but will often have an interest in technical cooperation, under which the licensor

acquires rights to the results of the ML. Therefore, the provision of data for use in ML is often based on a broad cooperation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

No specific liability schemes for adverse outcomes in digital health solutions exist under Austrian law. Austrian tort law generally stipulates that the tortfeasor is obliged to compensate for those damages which he has culpably and unlawfully caused. In addition to material damages, the injured party is also entitled to receive compensation for pain and suffering in case of injuries to the body and/or health. Punitive damages are not paid in Austria. Unlawfulness in the context of the provision of health services typically results from the violation of contractual obligations (e.g. duties of care, non-valid consent to the treatment because of incorrect or insufficient information). The liability for personal injury cannot be excluded and/or limited by contract.

The Austrian Product Liability Act, Federal Law Gazette 99/1988, last amended by Federal Law Gazette I 98/2001, (*Produkthaftungsgesetz* (*PHG*)) transposes in particular Directive 1999/34/EC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. If a defect in a product kills a person, causes bodily injury or damage to health, or damages a physical object other than the product, the manufacturer, distributor and the importer shall be liable for damages under Section 1 of the *PHG*. Liability is subject to the product being defective and therefore not offering the safety that can be expected under consideration of all circumstances (Section 5 paragraph 1 of the *PHG*). However, liability shall be excluded if the manufacturer, distributor or importer proves that: (i) the defect is due to a legal provision or official order with which the product had to comply; (ii) the characteristics of the product are in accordance with the state of the art in science and technology at the time when the person making the claim put it into circulation; or (iii) where the person making the claim has manufactured only one basic material or part of a product, the defect was caused by the design of the product into which the basic material or part has been incorporated or by the instructions of the manufacturer of that product.

9.2 What cross-border considerations are there?

In case of any cross-border provision of digital health services, the respectively applicable law and the applicability of regulatory requirements must be determined.

In case it is intended that foreign doctors provide telemedical treatment to Austrian patients, these require an Austrian professional licence if their activity does not fall under Section 37 of the *ÄrzteG* (freedom to provide services). According to Section 37 of the *ÄrzteG*, nationals of EU/EEA Member States or Switzerland who lawfully exercise the medical profession in another EU/EEA Member State or Switzerland may, from their foreign professional domicile or place of employment, practice medicine in Austria only if the medical activity is temporary and occasional, which must be assessed on a case-by-case basis, in particular on the basis of the duration, frequency, regular return and continuity of the activity.

Further considerations refer to the law applicable in a cross-border scenario: the provision of health services is typically based on a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the patient) with another person acting in the exercise of his trade or profession (the medical professional). According to Article 6 Regulation 593/2008 on the law applicable to contractual obligations (Rome I) the contract as well as the contractual liability derived therefrom shall therefore be governed by the law of the country where the consumer has his habitual residence, provided that the professional: (i) pursues his commercial or professional activities in the country where the consumer has his habitual residence; or (ii) by any means, directs such activities to that country or to several countries including that country. Cross-border healthcare providers therefore typically have to comply with the laws of a large number of countries in which they offer their services.

For claims arising from product liability under the *PHG*, pursuant to Article 5 Regulation 864/2007 on the law applicable to non-contractual obligations (Rome II), the law applicable shall be: (i) the law of the country in which the person sustaining the damage had his habitual residence when the damage occurred, if the product was marketed in that country; or, failing that; (ii) the law of the country in which the product was acquired, if the product was marketed in that country; or, failing that (iii) the law of the country in which the damage occurred, if the product was marketed in that country. As a result, providers of medical devices must therefore also comply with a large number of legal systems in the area of product liability.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

As, according to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians, it must be safeguarded that any medical advice or diagnosis is only given by such licensed physician.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Like for healthcare IT in general (see question 1.3), the main legal issues for Cloud-based services for digital health are the compliance with data protection law (see sections 4 and 5), the technical requirements for telehealth (see *GTelG 2012* in question 2.1) as well as determining whether a product qualifies as a medical device (see questions 2.1 and 3.1).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The intended business model and the actual product or service that shall be offered must be carefully examined from a legal perspective, in particular from a regulatory (e.g. the Physicians Act and limitations of telemedicine, MDR) and from a data protection point of view; in addition, the applicability and requirements of the *GTelG 2012* need to be considered. Furthermore, if such is relevant, depending on the business model, it should be assessed whether reimbursement of the services in question by the state sick funds is at all possible.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

A comprehensive regulatory (including data protection) due

diligence is advisable in order to safeguard that the business, which the digital healthcare venture intends to undertake or already undertakes, complies with all applicable legal requirements.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

One key barrier is Section 3 of the *ÄrzteG*, according to which medical advice may only be given by licensed physicians. Furthermore, the funding and/or (non-)reimbursement of digital health solutions by the state sick funds is a major issue; non-reimbursement would be a barrier to the widespread use of digital health solutions. Since the COVID-19 pandemic, the sick funds have expanded reimbursement of telemedicine treatment.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

From a formal/legal point of view, under Austrian law, clinician certification bodies might not be of specific relevance, even though acceptance or endorsement of a specific digital health solution by such body might prove compliance with specific quality standards or recommendations issued by such body. However, within a possible legislative process, these bodies might typically be consulted. The introduction of digital health solutions is in principle exclusively governed by law.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The Austrian state provides for a central digital health solution, namely *ELGA* (see question 2.2), which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions, as well as the federal provinces or their health funds. The services that are provided within *ELGA* (e.g. e-medication) do not have to be paid separately by patients and are covered by the general health insurance. The legal requirements of *ELGA* are set forth in the *GTelG 2012*.

Any other digital health solution an individual might want to use would need to be prescribed by a physician and be appropriate in order to be reimbursable by the Umbrella Association of Austrian Social Insurance Institutions.

10.7 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services in Austria, including non-contact medication prescriptions and the COVID-specific symptom check and triaging via app. With the help of these telemedicine applications, it was possible to find rapid solutions for patient care during the pandemic.

In addition, reimbursement by sick funds for telemedicine treatments was expanded and the use of video consultations mostly for initial consultations, therapeutic discussions and review of findings increased.

These developments have proven useful and will therefore be kept and be further expanded in fields where telemedicine can be reasonably used, as telemedicine offers enormous potential for the high-quality and cost-effective provision and support of healthcare services and ensures access to high-quality healthcare throughout the country.

Furthermore, the Austrian federation has emphasised that it intends to increase the use of and is in the process of creating a legal framework for specific digital health applications, namely of evidence-based, software-driven therapeutic applications for the prevention, management or treatment of a medical disorder or disease, which shall be reimbursed by the state sick funds if prescribed by a physician (see more at https://www.digitalaustria.gv.at/Strategien/Digital-Austria-Act---das-digitale-Arbeitsprogramm-der-Bundesregierung/Einblicke-in-den-Digital-Austria-Act/Digitales-Gesundheitswesen.html).

Dr. Sonja Hebenstreit is a partner at Herbst Kinsky Rechtsanwälte GmbH, which she joined in 2005. She specialises in the fields of intellectual and industrial property law, unfair competition, life sciences and data protection. Sonja Hebenstreit represents Austrian and international clients, including biotech and tech start-ups, as well as numerous pharmaceutical and medical devices companies, in a variety of regulatory issues, licensing and other contractual matters, as well as in data protection, unfair competition and reimbursement matters.

Herbst Kinsky Rechtsanwälte GmbH
Dr. Karl Lueger-Platz 5
A-1010 Vienna
Austria

Tel: +43 1 904 2180
Email: sonja.hebenstreit@herbstkinsky.at
LinkedIn: www.linkedin.com/in/sonja-hebenstreit-76b72864

The Firm
Since its establishment in 2005, Herbst Kinsky Rechtsanwälte GmbH has become one of Austria's leading commercial law firms. Its specialised and highly committed lawyers combine many years of experience gained abroad and in reputable Austrian law firms. The Firm's practice covers a full range of services in all areas of commercial, corporate, civil and public law, including banking, insurance and capital markets, corporate and M&A, IP, IT and life sciences, merger control, antitrust and competition, data protection, real estate, dispute resolution and arbitration. The Firm has established a particularly strong presence in the field of life sciences and healthcare.

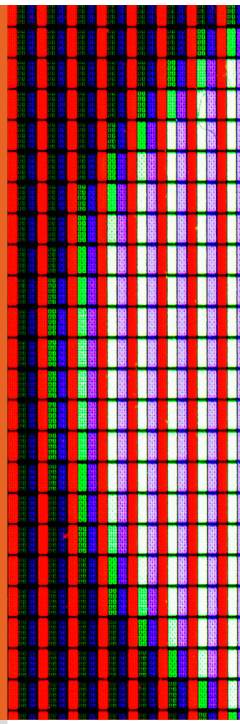
Our Clients
The Firm's clients range from large international privately held and publicly listed companies, banks, insurance companies and private equity investors to small and mid-size business entities, as well as start-ups. Clients cut across many different industries, including life sciences, energy, information technology, financial institutions and insurance.

www.herbstkinsky.at

HERBST KINSKY
RECHTSANWÄLTE GMBH

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.



Digital Health 2024 features one introductory chapter, two expert analysis chapters and 22 Q&A jurisdiction chapters covering key issues, including:

- Digital Health
- Regulatory
- Digital Health Technologies
- Data Use
- Data Sharing
- Intellectual Property
- Commercial Agreements
- Artificial Intelligence and Machine Learning
- Liability

The International Comparative Legal Guides are published by: glg Global Legal Group