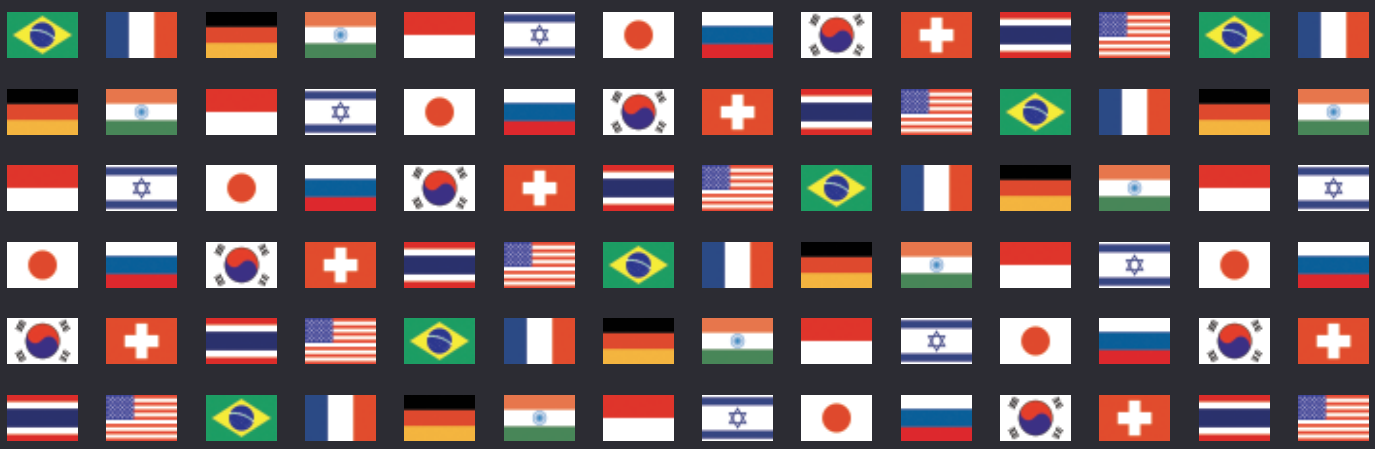
Digital Health
2021



LEXOLOGY®
Getting The Deal Through

Germany

Anja Lunze, Thanos Rammos, Tim Jonathan Schwarz, Daniel Tietjen, Stephan Doom, Nora Wessendorf and Karolina Lange-Kulmann*

Taylor Wessing

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 | Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

A variety of players are active in the German digital health market. They range from innovative, often venture-capital-backed start-ups focusing on rather specific niches, such as services geared towards a single condition or specific use case, to larger players such as global pharmaceutical and med-tech companies. The latter have recognised that digital health solutions can be very useful in accelerating product development, for example, by enabling digital clinical trials, and in extending the value chain by offering apps to be prescribed alongside regular medication.

Healthcare providers such as hospitals and outpatient chains have shown a high interest in establishing telemedicine platforms and online portals for their patients, which are often promoted by statutory and private health insurance funds. In addition, healthcare providers are working on becoming 'smarter' in general by digitising internal procedures such as clinical documentation and medication management systems and by integrating artificial intelligence in certain diagnostics.

Besides these life sciences and healthcare players, digital health has become an important area for Big Tech. These firms often transcend existing sector boundaries and pursue cross-border strategies either by acquiring local companies fitting into their strategy or by adapting existing products to the regulatory environment, for example, via higher data protection standards or by disabling selected features.

Investment climate

2 | How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The global covid-19 pandemic has acted as an accelerator to almost any digital business model, including digital health technologies. Investors are usually keen to invest in digital health, especially when the product or service scales well and is available via prescription so that costs are covered by public or private health insurance funds in Germany.

Prior to covid-19, the German parliament had already passed legislation allowing the prescription of medical apps and facilitating video consultation with physicians in the Digital Healthcare Act. Most recently, the Hospital Future Act will grant over €4 billion to modernise digital infrastructure in hospitals, which will most likely benefit digital health businesses as well.

However, aspiring digital health companies may still face challenges on their path to success. Owing to an increasing number of applications following the recent deregulation of medical apps, regulatory capacity might become a bottleneck. Eligibility to reimbursement is only granted after Germany's Federal Institute for Drugs and Medical Devices issues approval, and against the background of the covid-19 pandemic, that body is quite stressed already.

The central pillars of a truly digitised healthcare system such as an electronic health record and electronic prescriptions have not been implemented yet in Germany. Mass adoption among both healthcare providers and patients will likely be a long-lasting process, though at the same time offering manifold opportunities for resourceful digital health players. With a population of over 83 million in 2020, Germany is the most populated country in the EU, with more than 18 per cent of the overall EU population of close to 450 million (as of 1 January 2020).

Recent deals

3 | What are the most notable recent deals in the digital health sector in your jurisdiction?

M&A activity in the digital health sector is quite high, with numerous transactions and well above average EBITDA multiples, which can reach up to 40x EBITDA. Following the recent deregulation, catch-up effects are likely, and transaction volume is further fuelled by consolidation efforts as the sector is highly fragmented.

Targets range from smaller software developers to large enterprises such as Agfa Healthcare, which was acquired by private equity firm Dedalus for close to €1 billion. However, financial investors are not the only bidders with an appetite for digital health. Strategic investors such as CompuGroup have also been involved in a high number of deals. Notably, traditional healthcare clinics and healthcare providers have also discovered an interest in digital health targets and have been involved in several transactions in the sector.

In the venture capital space, several digital health-specific funds have been announced. DvH Ventures will supply €60 million to early-stage start-ups, and private health insurers aim to set up a €100 million fund for digital health investments.

Partnerships and joint ventures are usually of interest, if both partners complement each other in order to create a new platform, for example, by combining health and technology, or specific products and services, such as a drug and health app. This mostly includes partnerships between two established players (eg, Siemens Healthineers and IBM) or a well-established company and an innovative start-up (eg, Bayer and m.Doc).

Due diligence

4 What due diligence issues should investors address before acquiring a stake in digital health ventures?

In almost all cases, a thorough legal due diligence report on a digital health venture should entail assessments from a variety of legal fields, most notably including corporate, data protection, IP and patents, and regulatory aspects.

Corporate issues may include, for example, encumbered shares or assets in cash-strapped start-ups or growth companies, which might add a claiming party to potential deals and exit proceeds in future buyout scenarios. Another typical issue in this respect are complicated corporate structures with a variety of different shareholders from small to large, which can and often do complicate finding consent in financing rounds or M&A processes.

In the wake of the General Data Protection Regulation and in the context of health data, data protection measures have become an important due diligence issue. No investor will knowingly take the risk of a venture facing a multi-million-euro fine from the authorities, reputational damage aside. Given that many digital health businesses have developed proprietary technologies as their unique selling point, underlying IP and patents are among the most valuable assets for them but also for investors. IP due diligence should therefore reveal if all patents, licences, brands and so on are legally protected. Especially for starts-ups or upscaling growth companies, competition is often very fierce and intense. Companies are often faced with IT and IP legal disputes from competitors trying to impair regular operations and to potentially force competing companies out of business in order to gain competitive advantages and market share.

On the regulatory side, the heart of a company, being its core business and value creation model, requires investigation. It needs to be properly checked whether the concrete business model and future growth plan is in compliance with (current and also expected future) regulatory aspects or not. If it becomes clear that a business model is not compliant with regulatory standards and that no easy fix is available in the near term, potential buyers should double-check their intention to invest considerable amounts of capital. If business models do not pass legal and regulatory stress tests, at least the deal structure needs to be adapted accordingly. Hence, especially digital health start-ups with disruptive business models can greatly profit in the long term from seeking legal consultation early on and ensuring regulatory compliance going forward as they scale up while regulatory and legal setups follow the evolvement of the market.

Ultimately, the scope and focus of a legal due diligence often depends on the specific business model and specific company at hand. In some cases, an employment law due diligence may be the focus, whereas in other cases, such as commercial contracts, due diligence may be more sensible.

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Many digital health ventures rely on their own capital and personal investments from founders. If they do not generate any or not enough revenue yet and have a high cash burn rate, funding is mainly secured via business angels, government financing or bank loans, though the latter is often rather complicated when the company is very mature. Only a minority of start-ups in the digital health space have received recent funding from venture capitalists, crowd investors or accelerators, although this shows that these forms of financing still have plenty of room to grow.

As a federal state, Germany offers financing structures on both the federal and the state level. The federal government does not offer a financing programme specifically for the digital health sector, but access to general programmes is available. They range from loans with reduced interest to non-repayable grants, equity and guarantees. Non-financial support dedicated to digital health ventures is offered via the health innovation hub, a think tank founded by the Federal Ministry of Health.

Many states offer similar financing schemes to innovative start-ups located within that specific state. In addition, several states promote health clusters, which provide networking and partnering opportunities between start-ups, mature companies, healthcare service providers and academic institutions. Early-stage companies can also profit from cheap office spaces and consultation offerings in most clusters.

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

The digital health sector in Germany is not governed by a uniform legislative framework. Which law is applicable depends, in the first place, on the products or services in question. Furthermore, the applicable legislation depends on the respective topic (eg, market access, advertising, etc). For example, health apps that are medical devices fall within the scope of the German Act on Medical Devices and Directive 93/42/EEC (Medical Device Directive) with regard to regulatory requirements for market access (in particular). The Medical Device Directive will be repealed by Regulation (EU) 2017/745 (Medical Devices Regulation) as of 26 May 2022, which will then prevail the German Act on Medical Devices as well.

As regards reimbursement within the Statutory Health Insurance System, the legislative framework is regulated in the Fifth Social Security Code. Advertisements in the digital health sector are governed by the Drug Advertisement Act and the Unfair Competition Act. Data protection requirements are governed by Regulation (EU) 2016/679 (General Data Protection Regulation) as well as various national data protection laws supplementing the General Data Protection Regulation.

Professional Codes for Physicians of the 'Federal States' Associations of Physicians' govern remote medical treatments by means of distance communication in specific cases. The specific boundaries of remote treatments, however, differ between the federal states.

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

In Germany, various regulatory and enforcement bodies have jurisdiction over the digital health sector. Which body is competent depends, inter alia, on the local jurisdiction, in particular the question of whether a federal or state authority is competent. Germany's federal structure assigns certain competencies to the federal states and others to the state government. On the other hand, the fragmentation across several bodies is also largely due to the fact that significant parts of the regulation and enforcement are outsourced to self-governing bodies such as the Federal States' Associations of Physicians, the Associations of SHI physicians or the Federal Joint Committee.

Having said that, jurisdiction also depends on the product or service concerned. As regards health apps that are medical devices, the Federal Institute for Drugs and Medical Devices is responsible for the assessment of incident reports (eg, owing to product defects), the approval of clinical trials and the classification of medical devices on request of the competent state authority, a notified body or the manufacturer. Notified bodies are state-authorised bodies, which – depending on the

risk class of the medical devices – carry out tests and assessments as part of the conformity assessment to be performed by the manufacturer, and certify their correctness according to uniform assessment standards. Responsible for the designation and monitoring of notified bodies in Germany is the Central Authority of the Federal States for Health Protection with regard to Medicinal Products and Medical Devices. Regarding the enforcement of drug advertising and data protection law, mainly the administrative authorities of the federal states are competent.

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

The requirements depend on the type of product. Health apps as medical devices may generally only be placed on the market or put into operation in Germany if they are CE certified, which presupposes that the essential requirements according to section 7 of the German Act on Medical Devices in conjunction with the Medical Device Directive Annex I have been fulfilled and a conformity assessment procedure prescribed for the respective medical device has been carried out. Furthermore, medical devices generally are assigned to classes. Classification has to be carried out in accordance with the classification rules set out in Annex IX to the Medical Device Directive. The conformity assessment of class I medical devices, which are not marketed sterile and have no measuring function, can be performed by the manufacturer under its sole responsibility (self-certification with a declaration of conformity). For all other medical devices, third-party certification by a notified body is required in addition to the declaration of conformity issued by the manufacturer.

As regards telemedicine, only physicians with a specific licence to practise medicine are allowed to provide medical services to patients. Therefore, a digital provision of medical services to patients via telephone, video, apps or other digital means always has to comply with this general limitation of medical services to the provision by accredited doctors. Additional requirements may apply, especially with respect to the medical service provision within the Statutory Health Insurance System.

Soft law and guidance

9 Is there any notable 'soft' law or guidance governing digital health?

There is a guideline from the Federal Institute for Drugs and Medical Devices regarding the application for the directory for digital healthcare applications according to section 139e of the Fifth Social Security Code. In this guideline, the Institute explains how it will regularly interpret the normative requirements from the Digital Healthcare Act and the Digital Healthcare Regulation. Furthermore, the guideline offers a comprehensive explanation of the requirements. The listing in the Federal Institute for Drugs and Medical Devices directory is one requirement, among others, for the reimbursement of digital healthcare applications.

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

By way of example of digital healthcare applications, a physician who prescribes the app could generally be held liable under contract or tort law. Furthermore, the manufacturer of the app could also be held liable under contract or tort law, whereas it is not entirely clear yet whether and under what conditions product liability law is applicable to apps.

Furthermore, physicians who use an app on patients or instruct them to use it and app manufacturers have data protection obligations, confidentiality obligations and must guarantee secure processing. Enforcement is based on a system of sanctions consisting of administrative fines and compensation for damages (material and immaterial), as well as the possibility of enforcing infringements by means of injunctions in the event of non-compliance.

Having said that, according to the applicable Professional Code for Physicians of the respective Federal State's Association of Physicians, every practising physician in Germany must have sufficient professional liability insurance.

DATA PROTECTION AND MANAGEMENT

Definition of `health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Health data is a legally defined term in Germany. Health, biometric and genetic data are subject to specific protection. According to article 4 No. 15 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), 'health data' means 'personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status'. This includes information such as numbers or symbols that are assigned to a natural person in order to identify that person for health purposes, all data derived from the testing or examination of a body part of that person, including genetic data and biological samples, as well as all information on, for instance, a disease or the medical history of that person. German data protection authorities have a broad understanding of this and regularly assume that, for example, a photo with prescription glasses qualifies as 'health data'. This means that personal data collected by a health app, a wearable or smartwatch that relates to the individual's physical or mental health status is also included in the protection of 'health data'.

There is no specific definition of 'anonymised' health data. Rather, the general principle applies. According to Recital 26 of the GDPR, anonymous information is 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. Personal data that has been anonymised is not subject to the GDPR.

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Under the EU's data protection laws, the permissibility of data processing is generally governed by the GDPR, unless the GDPR contains an opening clause according to which EU member states can enact supplementary regulations at member state level. Some national laws contain specific provisions that afford a different level of protection to health data.

GDPR requirements

According to the GDPR, the processing of 'health data' is in principle prohibited (article 9(1) GDPR), unless legal justification pursuant to article 9(2) GDPR applies. The processing of health data is permitted, for example, if the data subject has consented to the processing (article 9(2)(a) GDPR).

In addition, article 9(2) GDPR contains specific opening clauses, according to which the EU member states may enact national laws for the processing of health data, such as:

- for 'the provision of health or social care or treatment or the management of health or social care systems and services' (article 9 (2)(h) GDPR);
- 'reasons of public interest in the area of public health' (article 9(2)(i) GDPR);
- 'archiving purposes in the public interest, scientific or historical research purposes or statistical purposes' (article 9(2)(j) GDPR); and
- to 'maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health' (article 9(4) GDPR).

National law requirements

In light of the above, the lawfulness of the processing of health data largely depends on national member states laws. These include various federal laws governing the processing of health data, such as:

- the Federal Data Protection Act (eg, sections22 and 27);
- the Infection Protection Act (section9 ff);
- the Medicinal Products Act (section40);
- the Act on Medical Devices (section20); and
- the Social Security Code (eg, section33a, 139e, 284 ff, section67a ff, section93 ff).

In addition, there are also various state laws, such as. state data protection acts and state hospital laws, and special laws such as the Mental Health Act.

In Germany, there are further legislative efforts to drive forward the digitisation of the healthcare system. The recently enacted Digital Healthcare Act, the Digital Health Applications Ordinance and the Patient Data Protection Act will make it easier for doctors to hold online video consultations, reimburse patients for using prescribed digital healthcare applications and ensure that all stakeholders have access to a secure healthcare data network for treatment.

Owing to the large number of national laws governing the processing of health data, the legal situation in Germany is very complex, which is why it is usually necessary to carry out a comprehensive examination of whether the applicable data protection laws are being observed when processing health data.

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

Yes, in certain cases German data protection law requires health data processed to be anonymised. For example, health data processed for scientific or historical research purposes or for statistical purposes shall be rendered anonymous as soon as the research or statistical purpose permits so, unless legitimate interests of the data subject prevent this (section 27(3) of the Federal Data Protection Act).

In addition, the general principle of data minimisation according to article 5(1)(c) of the GDPR requires that personal data must be anonymised when it is no longer necessary to identify the natural person.

However, EU and German data protection laws do not specify how true anonymisation can be achieved. Recital 26 of the GDPR explains that the principles of data protection should not apply to anonymous information that 'does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'

According to the European data protection authorities, personal data must be cut off from all identifying elements so that the information can no longer be attributed to an identifiable person in order to be considered truly anonymous under the GDPR. All means that may be available for identification (eg, also from third parties) must be taken into account. If identification (eg, with potentially available information from third parties) is still possible, the data is not truly anonymised, but only pseudonymised. This means that the processing of personal data is still subject to EU and German data protection laws. Organisations should therefore exercise caution when attempting to anonymise personal data. Organisations frequently refer to personal data sets as having been anonymised when in fact this is not the case.

Helpful information on how anonymisation of data can be achieved can be found in the Consultation Paper published by the Technology, Methods and Infrastructure for Networked Medical Research, which outlines the requirements for anonymisation, as well as in the Guidelines on the Protection of Health Data published by the German Federal Ministry for Economic Affairs, which provide further information on the procedure for anonymisation of health data.

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

In general, the GDPR provides several investigative powers of the data protection authorities (such as carrying out investigations, issuing warnings, imposing a processing limitation or ban) and moreover a system of sanctions consisting of administrative fines and compensation for damages (material and immaterial), as well as the possibility of enforcing infringements by means of injunctions.

Depending on the violation, administrative fines under the GDPR can amount to €20 million or up to 4 per cent of the violator's total worldwide annual turnover, whichever is higher.

With regard to the enforcement of data protection in relation to health data, some notable fines have already been imposed in Germany, such as a fine of €105,000 on a hospital for mixing up patient data owing to technical deficiencies in the hospital's patient and privacy management, and a fine of €1,240,000 on a health insurance company for the inadequate implementation of technical and organisational measures.

In addition, the practice of publicly naming and shaming violators can cause considerable PR and other damage. In particular, the public disclosure of a start-up from the healthcare space that unlawfully transferred health data, including symptoms and the name of the health insurance company, for tracking purposes to an advertising network led to considerable issues. In such cases, there is a risk that not only the users but also other stakeholders such as shareholders, investors or cooperation partners could shy away from using the product or investing in it.

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

Early on, German data protection authorities issued guidance for app developers and providers and specifically addressed mobile apps that process sensitive data. In particular, they asked for sandboxing and other means of encryption when processing patient and health data. In addition to that, according to the new Digital Health Applications Ordinance, which applies to qualified 'digital healthcare applications' (ie, those subject to reimbursement by the health insurance), the manufacturer must meet the requirements for data security according to the state of the art, taking into account the type of data processed and the level of protection associated with it, as well as the need for protection.

The requirement refers to the protection of the confidentiality, integrity and availability of all data processed via the app. According to the Digital Health Applications Ordinance, a declaration is to be submitted on the basis of a questionnaire to the Federal Institute for Drugs and

Medical Devices. If it is an app with a very high need for protection, additional requirements such as penetration tests, sufficient encryption of the stored data or two-factor authentication when accessing health data are necessary.

In general, the requirements are based on the specifications and recommendations of the Federal Office for Information Security, as described in particular in the standards BSI 200-1 (Management Systems for Information Security), BSI 200-2 (IT-Grundschutz Methodology) and BSI 200-3 (Risk Analysis on the Basis of IT-Grundschutz) of the Federal Office for Information Security. These requirements are supplemented by modules of the IT-Grundschutz Compendium. The implementation of a management system for information security that fulfils the requirements of ISO 13485 as well as those of the BSI standards or ISO 27001 is needed for any digital healthcare applications that are to be included in the Digital Healthcare Applications Directory, no later than 1 January 2022. In addition, the guideline BSI TR-03161, which describes security requirements for digital health applications, must be observed.

Without prejudice to the information security requirements for digital health apps, the health sector as such represents critical infrastructure according to section 6 of the BSI-KRITIS Regulation. This means that operators of critical infrastructure are obliged under section 8a(1) of the BSI-KRITIS Regulation to take appropriate organisational and technical precautions to avoid disruption to the availability, integrity, authenticity and confidentiality of the information technology systems, components or processes that are essential for the functionality of the critical infrastructure they operate.

Best practices and practical tips

16 What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

In practice, it is of great importance to be able to exploit the full potential of health data. This means that the data can be processed through the broadest possible means. This can be achieved, for example, by obtaining the broad consent of the data subject. Such consent can cover as yet unspecified research projects and future data processing, including, where possible, secondary use and transfer of data to third parties, such as other research partners.

In this context, the planned data processing must observe the 'principle of purpose limitation' (article 5(1)(b) of the GDPR). This principle stipulates that data may only be processed 'for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'. This means that the planned purposes of data processing must be already specified at the time of data collection. Until recently, it was controversial in Germany whether future data processing for secondary use could be based on broad consent, which only describes future planned data processing at a very high level. However, the German Data Protection Committee, in its Decision of April 2020, has now considered broad consent in the area of clinical studies to be permissible. It is possible that this view will also prevail in the context of digital health innovations to legitimise data processing for secondary use.

In order not to have to comply with the strict data protection regulations, it is recommended, whenever possible, to make personal data anonymous. In this case, the data protection regulations are no longer applicable. However, high demands are made on the true anonymisation of personal data, which always requires a separate legal basis to do so.

As regards the commercialisation of health data, it is not only necessary to ensure compliance with the above-mentioned data protection regulations if, for example, health data is transferred to third parties. In addition, effective contractual agreements between the data owner and the data recipient are also of crucial importance, since under German law there is no ownership of data. Rather, contractual arrangements are required that, in the context of the commercialisation of raw or anonymised health data, specify the extent to which the data recipient is to be granted rights of use of the data; in other words, which data may be used for which purpose (eg, for further research). In addition, the legal consequences of a violation of these data use rights (such as injunctive relief or contractual penalties) should also be governed in the respective contract. In short, only on a comprehensive contractual basis can an effective commercialisation of health data in Germany be guaranteed.

INTELLECTUAL PROPERTY

Patentability and inventorship

17 What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Patentability requires that an invention must pertain to a field of technology and be new, inventive and industrially applicable (article 52(1) of the European Patent Convention and section 1 of the German Patent Act). In the field of digital innovation, the technical character of an invention gains particular importance. Applying an invention by means of a computer alone does not make it eligible for patent protection. Therefore, software, algorithms and databases as such are not patentable (section 1(3) No. 1 and 2 of the German Patent Act). In contrast, computer-implemented inventions are patentable; if a programmable apparatus (computer, smartphone or the like) is used and some features of the inventions are realised by means of a computer program, for example, software monitoring the operation of technical equipment. The patentability of AI-generated content is currently a hot topic. The predominant opinion under the German Patent Act and the European Patent Convention is that an invention must be human-made. This was confirmed by the European Patent Office's refusal to grant two patents naming a machine as an inventor. Both decisions are currently under appeal. Under the current legislature, a patent can be granted if a human uses AI as a tool, recognises the results as an invention, determines its commercial usability and applies for protection.

Ownership of employee inventions is governed by the German Employee Inventions Act, according to which they generally belong to the employer. Simultaneously, the employee's right to remuneration arises.

Patent prosecution

18 What is the patent application and registration procedure for digital health technologies in your jurisdiction?

Patent prosecution for digital health technologies in Germany is subject to the same rules as inventions stemming from any other field. Patent prosecution starts with the filing of an application with the German Patent Office or for European patents with the European Patent Office. Applications are published 18 months after filing and examined after payment of mandatory fees. If a patent is granted, it is enforceable from the date of publication of its grant. Upon grant, third parties may file an opposition or, once the opposition period has expired, a nullity action. When examining patentability, the German Patent Office applies a three-step approach, assessing (i) (at least partial) technical character of the subject of the invention, (ii) that the patent claim contains instructions for solving a specific technical problem by technical means, and (iii) that the claimed subject matter is considered new and inventive over the state of the art. Digital health technologies often pertain to computer-implemented inventions. Therefore, the issues relating to the patentability of such types of inventions also apply. Thus, abstract ideas including mathematical methods are not patentable.

Other IP rights

19 | Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Other IP rights relevant in the context of digital health products are copyright and design rights, as well as know-how and trade secret protection. For instance, aspects of a digital health product, such as the design of a user interface, can be subject to design protection under the German Design Act. Further, the program code itself can be protected by the German Copyright Act. With a view to digital health products developed by employees within the course of an employment contract, it is important to note that the developed computer programs are exclusively owned by the employer without requiring separate remuneration according to section 69a of the German Copyright Act. Simultaneously, if the program meets the requirements for patentability, it can also be subject to the German Employee Invention Act, thereby requiring remuneration. Registered IP rights provide for absolute legal protection. In addition, practical information resulting from experience and testing, which is secret, significant and useful and described in a sufficiently comprehensive manner, can be protected as a trade secret. It is primarily secured by practical measures taken to ensure secrecy. If the information qualifies as a trade secret under the German Trade Secret Protection Act, legal remedies are available in the event of misappropriation.

Licensing

20 | What practical considerations are relevant when licensing IP rights in digital health technologies?

Like any other field, the emerging market of digital health invites collaboration between medical and non-medical professionals, which may include licensing of relevant IP rights. This follows the same legal requirements as the licensing of IP rights in any other technical field. Ensuring that the granted licence covers all required IP, types of use and relevant territories is key. Where the digital health product involves a trade secret, third-party access to the licensed information should be restricted. Non-disclosure clauses and mandatory confidentiality measures should be included in any licence agreement. A particular practical consideration to keep in mind when opting to invest in digital health products is that the right to use the licensed IP alone does not necessarily suffice for successful market participation. Providing medical services is restricted to licensed healthcare professionals and companies. Market participants lacking the necessary licence are limited to providing non-medical supporting products, or to selling medical devices such as healthcare applications.

Enforcement

21 | What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

Most patents in this field are still at application stage or only recently granted. Supplementary and faster protection can be achieved by filing a split-off utility model for a product based on an earlier filed and published patent application. Specific enforcement issues concerning digital health technologies are likely to concern territoriality. Digital health products are frequently offered and performed across multiple jurisdictions, resulting in the issue whether (territorially limited) IP rights are enforceable. A recent noteworthy case concerned an online vision test that was performed on a user's computer in Germany, but the collected data stored and assessed on a server abroad for the calculation of a lens prescription. The court held that the German part of the patent was infringed because the vision test, the 'significant advantage' of the invention according to the court, was performed in Germany; and the patented teaching was commercially exploited in Germany (Dusseldorf District Court, judgment of 28 July 2020, file no. 4a O 53/19). This issue may well arise in future cases. It remains to be seen whether other courts will follow the Dusseldorf court's apparent aim to prevent market participants' circumvention of territorially limited IP rights.

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 | What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The legal framework for advertising digital health products is provided by the German Drug Advertisement Act and the German Unfair Competition Act. The most important rule in practice is the prohibition of misleading advertising as regulated in section 3 of the German Drug Advertisement Act and section 5 of the German Unfair Competition Act. According to the prohibition on misleading advertising, it is impermissible to give false impressions,such as that success can be expected with certainty. The prohibition also includes advertising with study results, if the study does not prove the results (or only with limitations, if they have not been mentioned in the advertising), or to advertise health-related claims without sufficient scientific evidence. In the interest of protecting the health of the public, health-related advertising claims are only permissible provided they are based on sound scientific evidence. Furthermore, according to section 7 of the German Drug Advertisement Act, it is generally impermissible to grant benefits with regard to product-related advertising, such as for medical devices, unless a legal exemption applies.

Furthermore, according to section 9 of the German Drug Advertisement Act, advertising for remote treatment is inadmissible, unless the advertising is for a remote treatment using communication media and according to generally accepted professional standards; personal medical contact with the person to be treated is not necessary. This exemption has just recently been regulated. Advertising for remote medical treatments is also subject to the applicable provisions of the Professional Codes for Physicians of the Federal States' Associations of Physicians. The premise of the resulting restriction of advertising is the avoidance of a commercialisation of the medical profession. Therefore, an advertisement and marketing of digital services may generally only take place in the form of factual and appropriate information.

Aside from that, with regard to any online marketing of digital health products (in particular, through AdTech solutions), the processing of personal health data and its subsequent use can result in issues if the processing is not based on consent of the individual. German data protection regulators have scrutinised companies that use health data on the legal basis of, for example, a legitimate interest.

e-Commerce

23 | What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

The general requirements under e-commerce laws with regard to consumer protection apply also for digital health offerings. This means that in relation to patients or other users, terms and conditions need to be balanced and fair, and clauses must be sufficiently transparent. Furthermore, a consumer must be informed about all relevant aspects of the digital health offering at the time the contract is concluded. For devices with limited screen size, exemptions to these information obligations apply. In the case of a premium service, the provider needs to implement a 'buy button' with unambiguous wording that indicates the obligation to pay or subscribe.

These requirements are of high relevance since non-compliance can result in cease-and-desist claims by way of warning letters issued by consumer protection associations or competitors. Furthermore, any clauses within terms and conditions that do not comply with consumer protection law requirements are invalid and, as a result, if challenged in court, unenforceable.

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

On the basis of section 33a of the Fifth Social Security Code, which has just been introduced, physicians can prescribe 'digital healthcare applications', which are a certain type of 'Health App'. The costs are reimbursed by the Statutory Health Insurance (SHI). Digital healthcare applications are medical devices of low risk class (I or IIa), which mainly have a digital function and are intended to support the detection, monitoring, treatment or alleviation of diseases or the detection, treatment, alleviation or compensation of injuries or disabilities regarding the insured person or regarding the care of service providers (section 33a, paragraph 1, sentence 1 of the Fifth Social Security Code). However, if a Health App falls under this definition, this alone is not sufficient to participate in the reimbursement system. Rather, the insured person's right to receive the Health App and the reimbursement by the SHI system depend on certain conditions that are listed in section 33a, paragraph 1, sentence 2 of the Fifth Social Security Code. According to these conditions, the Health App must be included in the relevant directory pursuant to section 139e of the Fifth Social Security Code, which is maintained by the Federal Institute for Drugs and Medical Devices. In addition, a medical or psychotherapeutic prescription or an approval of the health insurance company must be available. Finally, no exclusion according to the third chapter of the Fifth Social Security Code or a negative decision of the Joint Federal Committee may have taken place. So far, very few Health Apps have been accredited. However, the number of accredited Health Apps is expected to increase significantly in the near future, increasing the variety of available and reimbursable services.

Furthermore, remote medical services provided by SHI-accredited physicians within the applicable regulations can generally be reimbursed by the SHI. Most private health insurances cover such remote medical services as well.

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The most significant recent development was the entry into force of the Digital Healthcare Act, along with the new Patient Data Protection Act, which gave many innovations in the digital health sector. As a result, physicians can now prescribe health apps, and sensitive health data is simultaneously protected in the best possible way. In addition, the telematics infrastructure of hospitals and pharmacies is being expanded, and patients, as insured persons, will have a right to have their data stored in an electronic patient file as of January 2021. Specialist referrals can be transmitted digitally. The electronic prescription will be introduced in 2022.

TaylorWessing

Anja Lunze
a.lunze@taylorwessing.com

Thanos Rammos
t.rammos@taylorwessing.com

Tim Jonathan Schwarz
t.schwarz@taylorwessing.com

Daniel Tietjen
d.tietjen@taylorwessing.com

Stephan Doom
s.doom@taylorwessing.com

Karolina Lange-Kulmann
k.lange@taylorwessing.com

Nora Wessendorf
N.Wessendorf@taylorwessing.com

Ebertstraße 15
10117 Berlin
Germany
Tel: +49 30 885636 0
Fax: +49 30 885636 100

Isartorplatz 8
80331 Munich
Germany
Tel: +49 89 21038-0
Fax: +49 89 21038-300

Benrather Str. 15
40213 Duesseldorf
Germany
Tel: +49 211 8387 0
Fax: +49 211 8387 100

www.taylorwessing.com

Telematic infrastructure has been and will be the main challenge in the recent past and in the future. The Hospital Future Act has established an important regulatory framework to promote and fund digitisation in the healthcare system in the upcoming years.

Furthermore, because of the change of law regarding the German Drug Advertisement Act, physicians can now provide information about their remote treatment and video consultation services on their websites in exceptional cases. The liberalisation of the prohibition of remote service provision has been a very significant development in the recent past. Previously, remote treatment in Germany had only been allowed in very limited cases and was therefore rarely practised.

Coronavirus

26 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programs, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Thanks to the Digital Healthcare Act, which came into force in 2019, numerous opportunities had already been created in the digital healthcare sector at the outbreak of the pandemic. Within a very short time, a data protection-compliant tracing app was developed and launched on the market by the Robert Koch Institut responsible for disease control and prevention, which serves as a central tool for combating the pandemic in Germany.

However, covid-19 has led to various temporary legislation in Germany with a financial or operative impact to ensure the continuous provision of safe patient care during the pandemic. Examples are the establishment of coronavirus test centres and numerous financial support systems, as well as the loosening of regulations on video consultations and remote certifications of incapacity for work.

The temporary legislation is constantly being adapted to the changing challenges of the pandemic. The legislator is working at record speed in these times. It is to be expected that the special regulations will continue to have an effect until 2021 in an adapted form.

* *Acknowledgements: Angela Knierim, and Nicolai Wiegand.*

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business