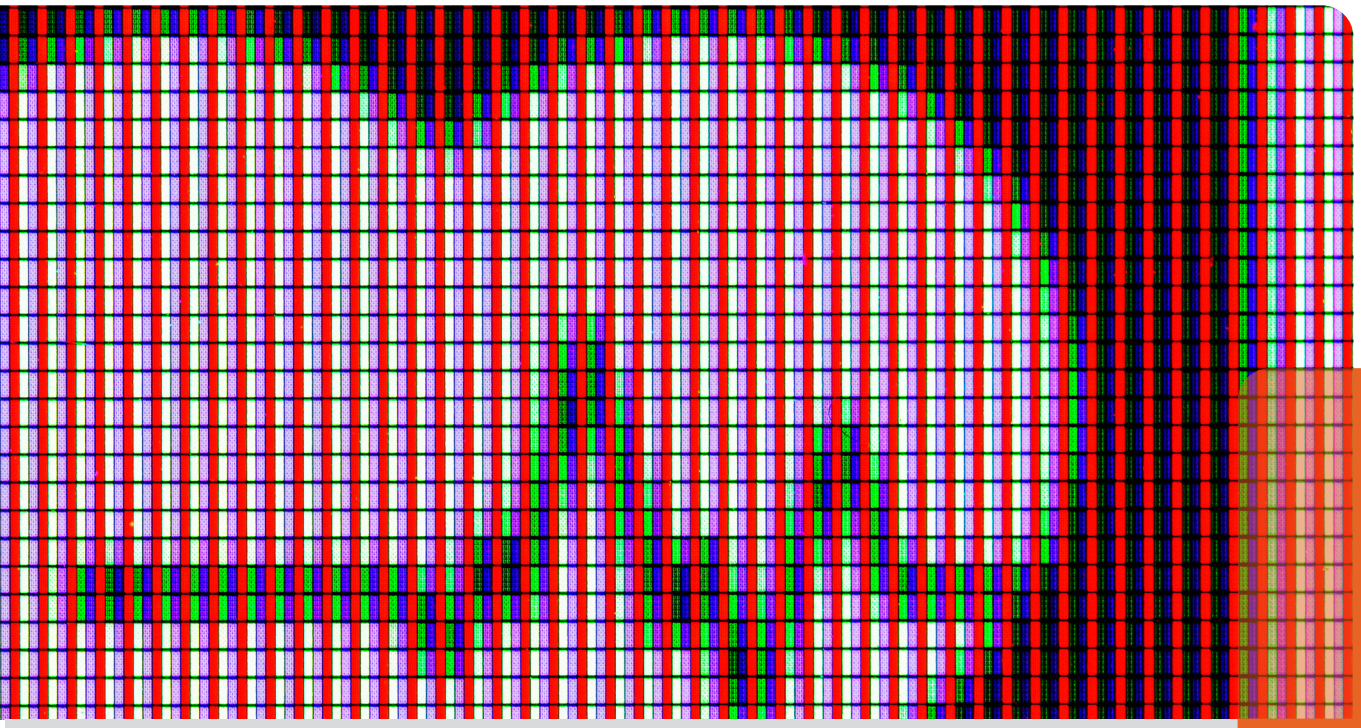
International
Comparative
Legal Guides



Digital Health

2024

Fifth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

glg Global Legal Group

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

Greece


Nefelie Charalabopoulou


Natalia Kapsi


Yolanda Antoniou-Rapti


Celia Karvouni

Zepos & Yannopoulos

1 Digital Health

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

Greek Law does not define "digital health" (nor "e-Health", which is also commonly used), yet the term is understood to encompass: (i) digital healthcare services, including telemedicine; (ii) software used as a medical device; (iii) medical devices used as diagnostic and/or monitoring tools; and (iv) other medical products that involve digital features. While digital health is not a defined legislative term, there is a single legislative reference to telemedicine to be found in Article 66 par. 16 of Law 3984/2011. Also, the Greek Ministry of Health (MoH) website refers to the definitions used by the World Health Organization: "[...] the efficient and safe use of information and communication technologies (ICTs) in support of health and health-related fields, including healthcare, monitoring and treatment, research and knowledge" and the European Commission "[...] tools and services that use ICTs to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health".

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

Key emerging technologies in digital health in Greece include various tools and platforms used by stakeholders that enable the monitoring, recording and health management, as well as digital tools for the remote provision of healthcare services, decision making, storing and sharing of data, managing clinical workflows, diagnostics and patient management and support. Examples include:

- Telemedicine.
- Wearable devices and biosensors.
- Mobile apps.
- Software as a medical device.
- AI digital health tools.
- Digital diagnostics.
- Health information exchange.
- e-Health records.
- Real-World Data and Real-World Evidence analytics.

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

The core legal issues in digital health in Greece are the applicability of and compliance with the regulatory framework, the categorisation of a digital tool or software as a medical device, liability issues regarding the interpretation of the data generated through the digital tools, and issues regarding data privacy and security and liability in general.

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

According to the Statista Market Forecast, Greece's revenue in the digital health market is projected to reach US$318.80 million in 2023. Revenue is expected to show an annual growth rate (CAGR 2023–2027) of 9.28%, resulting in a projected market volume of US$454.70 million by 2027.

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

Although no such data could be ascertained for Greece, there is an active innovation ecosystem in the field of digital health tools in Greece, with significant growth in recent years. Today, in "Elevate Greece" (which is the official platform and leading resource for in-depth information on the Greek Startup Ecosystem), there are 113 registered startups active in the field of life sciences (healthtech, medtech, biotech), constituting the most numerous category with 14.7%. More than half of them develop digital health applications and tools, mainly for disease management, telemedicine and wellness.

2 Regulatory

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

Some healthcare regulatory schemes related to digital health are the following:

1. Greek Law 4931/2022 "Doctor for All, Equal and Quality Access to the Services of the National Services Health Organization (EOPYY) and Primary Health Care and other emergency provisions"; in particular Article 28.
2. Greek Law 4961/2022 on emerging information and communication technologies, which has introduced rules and obligations about digital governance.
3. Greek Law 4715/2020 "Arrangements to ensure access to quality health services establishment and statute of the Organization for Quality Assurance in Health S.A. (ODIPY S.A.), other urgent provisions under the competence of the Ministry of Health and other provisions", namely Article 23.

4. Greek Law 4633/2019; in particular Article 33.
5. Greek Law 4213/2013 transposing Directive 2011/24/EU on the application of patients' rights in cross-border healthcare and other provisions, specifically Article 6.
6. Greek Law 3984/2011; in particular Article 66 par. 16 on Telemedicine.
7. As EU regulations, the MDR (Regulation 2017/745 on medical devices) and IVDR (Regulation 2017/746 on *in vitro* diagnostics) are directly applicable in Greece and do not have to be transposed into national law.
8. A number of legislative initiatives concerning the EU's digital strategy, such as the Digital Services Act (EU Regulation 2022/2065) and the EU proposal for an AI Act.

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

1. Law 4624/2019 "Protection of Personal Data and Measures for the Implementation of the GDPR", which enacts supplemental measures for the application of EU Regulation no. 2016/679 (GDPR).
2. Law 3471/2006 "Protection of Personal Data and Privacy in the Field of Electronic Communications".
3. Greek Law 1733/1987 on "Technology transfer, inventions and technological innovation" (Greek Patent Law).
4. Greek Law 1607/1986 on the "Ratification of the European Patent Convention".

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

As regards the consumer's protection, Law 2251/1994, which transposed into Greek law the Product Liability Directive 85/374/EC and Law 4933/2022, which transposed into Greek law Directive 2019/2161/EU (the omnibus directive of the "New Deal for Consumers" package) apply. On top of that, general provisions of the Greek Civil Code (Article 914 *et seq.* establishing tortious liability) are applicable in case they afford consumers more effective protection.

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

According to Article 23 of Greek Law 4715/2020, as amended, the MoH is designated as the National Authority responsible for electronic health issues and in cooperation with the other involved agencies has the overall responsibility of coordinating the actions for the implementation of the national strategy for digital health. An important specialised agency is the MoH's National Council for eHealth Governance. Moreover, the Hellenic Data Protection Authority is concerned with ensuring the application of the GDPR regarding personal data protection. Last but not least, the Ministry of Digital Governance and its General Secretariat of Cybersecurity provide regulatory services for the security of informatic systems.

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

Privacy, data security and product liability of medical devices (including software) are important key areas of enforcement when it comes to digital health.

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

The MDR and the IVDR apply to Greece. As EU regulations, they apply automatically to Greece as soon as they entered into force, without needing to be transposed into national law.

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

Greek Law 4961/2022 on emerging information and communication technologies contains provisions about AI, Internet of Things, etc. It is worth noting that the European Commission tabled a proposal for an EU regulatory framework on AI in April 2021.

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:** Health data protection, liability and security issues are emerging.
- **Robotics:** Liability allocation and regime of product responsibility are key.
- **Wearables:** The collection of daily precise health data raises the issue of data protection.
- **Virtual Assistants (e.g. Alexa):** Their training and their function relates with AI issues and data protection compliance.
- **Mobile Apps:** Security and data protection in particular in the use of apps that collect health data are really important.
- **Software as a Medical Device:** Medical Device regulations (MDR/IVDR), data protection and security are key.
- **Clinical Decision Support Software:** Liability allocation, Medical Device regulation (MDR/IVDR) and data protection are key.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions:** Where the technology is provided to a public institution, providers have the obligation to disclose details that allow the public institution to study how the system works and the parameters which, in view of the intended purpose, are taken into account for taking or supporting decisions or adopting acts, to improve the system and to publish or make available in any way such improvements. Also, any public body using an AI system is required to carry out an algorithmic impact assessment before the system becomes operational.
- **IoT (Internet of Things) and Connected Devices:** Manufacturers, importers and distributors of such devices will have particular obligations, including from a data protection standpoint, once the relevant provisions of Greek Law 4961/2022 come into force, which is expected to happen in March 2024. Medical Device regulations may also apply depending on the features.
- **3D Printing/Bioprinting:** The use of the technology of 3D printing raises intellectual property and consumer protection issues and the Intellectual Property Law 2121/1193 and Law 2251/1994 on Consumer Protection shall apply. There is no specific regulatory framework on bioprinting; nevertheless, data protection and security regulations are likely to apply as well as the MDR/IVDR depending on the purpose of use.

- **Digital Therapeutics:** Liability allocation and data protection are emerging issues.
- **Digital Diagnostics:** The development and use of digital diagnostics technology may raise industrial property and data protection issues.
- **Electronic Medical Record Management Solutions:** The use of electronic management solutions for medical record keeping may raise data protection issues.
- **Big Data Analytics:** Big data analytics raise data protection issues.
- **Blockchain-based Healthcare Data Sharing Solutions:** The use of blockchain technology in the context of healthcare data solutions may raise issues concerning data protection and data security.
- **Natural Language Processing:** Proper and secure use of AI and data protection are important issues.

3.2 What are the key issues for digital platform providers?

Digital platform markets are rapidly maturing, raising issues about regulatory constraints, compliance with security standards, effective supervision and consumer protection.

4 Data Use

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

The use of personal data constitutes processing of personal data and therefore, compliance with the provisions of the GDPR and Law 4624/2019 should be complied with. The key issues to consider are ensuring compliance with the processing principles of the GDPR, processing personal data under an appropriate legal basis, ensuring that the data subjects are being informed about the processing of their personal data, implementing appropriate technical and organisational measures for the protection of personal data, maintaining records of processing activities and, if applicable, appoint a data protection officer (DPO). Also, health data are considered special categories of personal data as defined under Article 9 of the GDPR.

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

The data protection legislation applies regardless of the nature of the entities involved. Law 4624/2019 includes different provisions for controllers who are public and controllers who are private entities, for instance, when it comes to processing personal data for reasons different that the ones they were collected for, and in relation to processing activities on special categories of personal data.

4.3 Which key regulatory requirements apply?

1. As follows:
   a. Entities processing personal data shall be able to demonstrate compliance with the following processing principles: lawfulness; fairness; and transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
   b. Purpose limitation principle: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
   c. Data minimisation principle: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
   d. Accuracy principle: Personal data shall be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay.
   e. Storage limitation principle: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
   f. Principle of integrity and confidentiality: Personal data shall be processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisation measures.
2. The processing of personal data must be based on an appropriate legal basis. Different legal bases are provided for special categories of personal data, who are afforded greater protection, as opposed to non-special categories of personal data.
3. Data subjects must be informed about the processing of their personal data, including details about the controller's identity and contact details, the purposes of the processing and the legal basis, the recipients of their personal data, whether their personal data are being transferred outside the EU/EEA and under which safeguards, the retention period and their data protection rights. Where the personal data are not being collected directly from the data subject, the information provided should also include the source they originate from and the categories of personal data.
4. Controllers should respond to, and without prejudice to limitations provided by applicable legislation satisfy requests made by data subjects exercising their rights of access, rectification, restriction of processing, data portability, objection and the right not to be subject to automated decision making.
5. The roles of the parties involved in the personal data processing activities must be determined, i.e., controllers, processors and joint controllers. In a controller-to-processor relationship, an appropriate agreement in writing must be put in place in accordance with Article 28 of the GDPR. In case where two or more parties jointly determine the means and purposes of the processing activity, an agreement must be put in place pursuant to Article 26 of the GDPR.
6. The core processing activities must be evaluated in relation to determining whether there is an obligation to appoint a DPO. In case a DPO is appointed, either because it is required or as a best practice, said appointment must be announced to the data protection authority. The Hellenic Data Protection Authority expects that the DPO should be able to communicate using the Greek language; therefore, in case a DPO is appointed at Group level and does not speak Greek, a Greek-speaking local contact point should be also appointed and announced to the authority.
7. Processing activities, in particular those that involve the use of new technologies, that are likely to result in a high risk to the rights and freedoms of natural persons, require the carrying out of a Data Protection Impact Assessment (DPIA). Large-scale processing activities

on health data is an example that requires a DPIA and is specifically mentioned by the GDPR. The Hellenic Data Protection Authority has also issued a decision setting out an indicative list of processing activities that are subject to the requirement for a DPIA.

8. Appropriate technical and organisational measures should be put in place to ensure a level of security to the personal data that is appropriate to the relevant risk.
9. Controllers should ensure that appropriate arrangements are in place in order to be able to identify and assess personal data breach incidents and, where required, notify the Hellenic Data Protection Authority and communicate the breach to the affected data subjects.
10. In case personal data are transferred outside the EU/EEA, compliance with Chapter V of the GDPR should be ensured (e.g. standard contractual clauses).

4.4 Do the regulations define the scope of data use?

The scope of data use is defined, in the sense that data processing must comply with the above-mentioned principles (see question 4.3). The meaning of "processing" is the same as defined under the GDPR.

4.5 What are the key contractual considerations?

Where the controller engages a processor, their contractual relationship must determine the subject-matter, duration, nature and purpose of the processing, and the type of personal data and categories of data subjects, as well as the parties' rights and obligations. In particular, the contract should stipulate the obligations set out under Article 28 of the GDPR. The same contractual considerations apply when the processor engages a subprocessor, in the sense that the subprocessor should undertake the same obligations that the processor has undertaken against the controller. In case two or more controllers jointly determine the purposes and means of a processing activity, they should determine in a transparent manner their respective responsibilities for compliance with their data protection obligations, and in particular in relation to their obligation to inform the data subject about the processing of their personal data and their obligation to respond to requests by data subjects exercising their data protection rights.

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

As analysed under question 4.3 above, the data protection notice provided by controllers to the data subjects should include information about their rights and contact details of the controller and, where applicable, the DPO, where the data subjects can exercise their rights. Where the request is made by electronic means, the controller should respond by electronic means as well, unless the data subject requests otherwise. In other respects, as provided by the GDPR, the right to withdraw consent should be as easy as it was to give consent, and controllers have the obligation to respond to data subjects' requests within one month. That period may be extended by two more months if it is necessary considering the complexity and number of requests received. In any case, the data subject should be informed of any such extension and the reasons for the delay.

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

Data inaccuracy, bias and discrimination issues are addressed by the Hellenic Data Protection Authority under the power conferred to it to monitor compliance with Greek Law 4624/2019 and the GDPR, which amongst others as set out under question 4.3 above, establishes the principle of lawfulness, fairness and transparency, and the principle of accuracy. In general, violations of the data protection regulatory framework may lead to the imposition of administrative sanctions, as provided by the GDPR. Moreover, data subjects may also raise civil claims of the Greek Civil Code. Lastly, certain violations of the data protection regulatory framework may entail criminal sanctions.

Providers of AI systems to public bodies have the obligation to implement by design appropriate measures to safeguard the prohibition of any discrimination, the protection of equality between women and men, freedom of expression, access for individuals with disabilities and the rights of employees. Also, companies who use AI tools in the context of evaluating employees or candidates should ensure compliance with the principle of equal treatment and non-discrimination.

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?

There is no specific legislative framework for Generative AI companies. Compliance with all data protection requirements should be ensured. Also, Greek Law 4961/2022 includes specific provisions that impose obligations to entities who provide AI systems to public bodies.

5 Data Sharing

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

The same issues as set out under question 4.1 above should be considered in the context of sharing data as well. Sharing personal data across borders of the EU/EEA gives rise to the compliance obligations of Chapter V of the GDPR, in the sense that in principle they are prohibited unless there is an adequacy decision issued by the European Commission or other appropriate safeguards in place (e.g. standard contractual clauses).

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

Law 4624/2019 includes different provisions for controllers who are public and controllers who are private entities, for instance, when it comes to processing personal data for reasons different from the ones they were collected for, and in relation to processing activities on special categories of personal data.

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

The key regulatory requirements mentioned under question 4.3 are applicable in the context of sharing data.

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

As mentioned in question 2.1 above, many governmental initiatives have taken place in Greece in order to establish a legal framework regarding those issues.

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

There is no specific regulatory framework in relation to federated models of healthcare data sharing. The key issues to consider that apply are the issues mentioned under section 4.

6 Intellectual Property

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

According to the Greek Patent Law, as well as Greek Law 1607/1986 on the "Ratification of the European Patent Convention", inventions are patentable provided that they are new, they involve an inventive step and are susceptible of industrial application. According to par. 2I of Article 5 of the Greek Patent Law, computer programs are not patentable; however, the foregoing exclusion from patent protection applies to the extent that the patent application relates to a computer program as such. Inventions involving software are not excluded from patentability as long as they have a technical character. Additionally, the patentability of AI technology is also debatable. According to the European Patent Office's Guidelines for Examination, even though AI technology is based on computational models and algorithms and the latter as such are excluded from patentability, nevertheless, inventions using AI technologies can be patentable when they solve a technical problem in a field of technology. In terms of inventorship, it should be noted that under the European Patent Convention (EPC), the legal concept of inventorship requires a human being to be the inventor.

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

Greek Law 2121/1993 on Copyright (Greek Copyright Law) protects both literary and artistic works in a broad sense. The foregoing law confers protection to computer software as well. It should be mentioned, however, that copyright is an unregistered right and thus, protection achieved under the provisions of the Greek Copyright Law might be less efficient than the protection conferred under patents.

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

Greek Law 4605/2019 on the harmonisation of Greek legislation to Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure may be invoked for the protection of AI systems from illegal possession or usage from third parties.

A trade secret means information that fulfils all of the following conditions: (a) it is secret; (b) has commercial value resulting from its secret nature; and (c) the person lawfully in control of that information has made reasonable efforts, taking into account the circumstances, to protect its confidentiality.

Trade secrets are unregistered rights and thus, provided that the foregoing conditions are met, wrongful acquisition or disclosure of such information is prohibited.

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

Under the technology transfer contract, the technology donor is obliged to provide the receiver with the technology and the receiver is obliged to pay the agreed price. The contract shall be registered in the Technology Transfer Register. Academic technology transfer in Greece is regulated under the provisions of Articles 21 and 22 of the Greek Patent Law, Article 23 of the Greek Law 2741/1999 and Law 4310/2014. The aforementioned laws apply, *inter alia*, to technology transfer contracts, filing of technology transfer contracts with the National Industrial Property Organization, licensing and institutional matters.

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

Under the provisions of the MDR, software may be considered as a medical device under certain conditions defined in Annex VIII to the MDR and can be classified in all four risk classes, according to their intended purpose and their inherent risks. As to the protection of software *per se* either under the patent or the copyright legislative framework, the analysis under questions 6.1 and 6.2 applies *mutatis mutandis*.

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

Whether an AI device can be recognised as inventor of a patent is a much-discussed issue. In the context of the Greek Copyright Law and Greek Patent Law, which follow an anthropocentric approach, the creator/inventor of a work always corresponds to natural persons. Therefore, for the time being, as analysed hereinabove, in compliance with the EPC, only humans can be considered inventors and thus, can be granted patents in Greece.

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

The provisions on service or dependent inventions, as per Article 6 of the Greek Patent Law, apply *mutatis mutandis* to the IP rights on government-funded inventions.

7 Commercial Agreements

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

Collaborating parties shall clarify the applicable legal and regulatory framework. In their contract they shall agree on the results of their partnership, the allocation of IP rights, liability-related matters, including, *inter alia*, product liability issues.

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

Agreements between healthcare and non-healthcare companies shall ensure that the non-healthcare companies comply with the specific rules and regulations applicable to healthcare companies, in particular on a regulatory level, including, indicative compliance with the provisions of the overseeing authorities' circulars, announcements, guidelines and the applicable code(s) of ethics.

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

Federated learning allows multiple healthcare institutions to collaborate and train machine learning models based on decentralised data without the need for sharing sensitive patient information. Parties shall consider the importance of patients' security and data protection.

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

Parties should take into consideration the strict regulatory and legal requirements that apply and guarantee the protection of patients' personal data and rights through their transparent activity.

8 Artificial Intelligence and Machine Learning

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

Machine learning has an assistive role in digital health. It provides physicians with accurate information, helping them in their research, their practice and their decision making. It also contributes, among others, to automating hospital processes and even diagnosing diseases.

8.2 How is training data licensed?

Currently, in Greek Law there are no provisions specifically regulating the licensing of training data; said are subject to the general provisions on licensing.

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

Currently, in the context of the Greek Copyright Law, which follows an anthropocentric approach, IP rights are owned only by natural persons who were involved in the development of the algorithms.

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

Security, data protection and transparency are key.

9 Liability

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

1. Civil Liability: Healthcare service providers may bear contractual and non-contractual liability towards patients if they act illegally and cause damage to patients by fault or negligence. Provisions of Greek Civil Code, in particular Articles 914 and 330, and provisions of Greek Law 2251/1994 on Consumer Protection, namely Article 8, are applicable.
2. Criminal Liability: Healthcare service providers may bear criminal liability in accordance with the provisions of the Greek Criminal Code.
3. Regulatory liability: Competent authorities may impose administrative functions in case of non-compliance with the regulatory framework.

9.2 What cross-border considerations are there?

From a data protection standpoint, see the answer to question 5.1.

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

Compliance with the protection legislation and the AI-related provisions under Law 4961/2022 are key to minimise risks posed by the use of generative AI in the provisioning of digital health solutions.

10 General

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

From a data protection legislation standpoint, compliance with applicable legislation is a key issue and in particular the personal data transfer provisions where Cloud-based services are not hosted within the EEA.

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

Companies that wish to engage in the digital healthcare market must be particularly mindful of the deficient regulatory framework and institutional gaps which create considerable market ambiguities.

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

Investing in digital healthcare ventures in Greece presupposes a thorough understanding of the regulatory landscape and the local market. Venture capital and private equity firms should consider, *inter alia*, the following key issues before making an investment in digital healthcare in Greece:

1. Regulatory environment: Understand the regulatory framework (or lack thereof) and institutional gaps.

2. Market landscape: Assess the level of adoption of digital health technologies locally. Identify key players, competitors and potential areas for disruption.
3. Healthcare infrastructure: Evaluate the existing infrastructure and assess how well digital solutions can integrate within the current healthcare system.
4. Patient data privacy and security: Assess how patient data shall be handled in compliance with data privacy and date security rules.
5. Reimbursement policies: Understand the potential for reimbursement and assess whether the existing landscape supports or hinders a particular digital health solution.

By thoroughly examining these factors, venture capital and private equity firms can make more informed decisions when investing in digital healthcare ventures in Greece.

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

Lack of existing legislative and regulatory provisions, as well as reimbursement-related matters, could be considered as some of the key barriers for adopting digital health solutions in Greece, on a wide scale.

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?

The MoH is primarily the competent body for any health-related decisions, policies and solutions; depending on the matter at hand, the Ministry of Digital Governance may also be competent.

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?

Digital health tools are not, in general, reimbursed in Greece and no operational framework exists for digital health providers in particular.

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.

In the context of its strategic planning for its digital transition, Greece has prioritised the digital transformation of the healthcare sector, through the Digital Bible of Transformation, and the Recovery and Resilience Plan Greece 2.0. The Bible includes 22 digitisation projects, 10 of which are ongoing. These include the completion of the electronic patient file, the upgrade of digital infrastructures in the public sector hospitals (with an emphasis on the development of clinical information systems and the input of data available in the electronic health record), the expansion of telemedicine solutions and the digitisation of cancer management. So far, they have been included in two pillars, with a total budget of over €780 million and should be completed by the end of 2025. Indicatively, the most important are:

- The projects for the digitisation of the Public archives, the provision of Cloud infrastructure and the national payer's (EOPYY) digital transformation.
- The digitisation project of the NHS archives (€235.6 million), which concerns the digitisation of approximately 200 million pages and imaging examinations that shall be available through the electronic health record.
- The extension of the National Telemedicine Network.
- The projects of improving the digital readiness of hospitals (€173.1 million) and the National Electronic Health File (€55.9 million).
- The project of installing RIS PACS systems in public hospitals (€36.3 million).

Bearing the above in mind, it can be said that so far, emphasis has been given by the State to the digitisation of systems and processes, as well as promoting interoperability. Next steps should also include the establishment and/or updating of the corresponding regulatory frameworks and providing strategic incentives to investors to invest in digital health solutions.

Nefelie Charalabopoulou is head of the Zepos & Yannopoulos healthcare, pharma & life sciences practice. Nefelie practises corporate, commercial and healthcare law. She focuses on advising clients in highly-regulated industries on all inherent legal and compliance issues, with an emphasis on pharmaceuticals, medtech products, biotech and cosmetics. She also advises them on their corporate law matters. Her extensive experience in the life sciences sector is particularly valuable; it allows her to thoroughly understand and analyse the complex environment in which her clients operate and helps them to achieve breakthrough results. She supports domestic and multinational stakeholders on a wide range of regulatory and compliance issues, such as marketing authorisations and registrations, pricing and reimbursement, licensing and distribution, interactions with HCPs/HCOs, clinical trials, promotional activities, etc.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: n.charalabopoulou@zeya.com
LinkedIn: www.linkedin.com/in/nefelie-charalabopoulou

Natalia Kapsi is a member of the Zepos & Yannopoulos healthcare, pharma & life sciences practice. She focuses on corporate, commercial, pharmaceutical and IP law. She has experience in advising multinational healthcare companies on regulatory, commercial and compliance issues, with an emphasis on regulations, standards and codes of practice related to the marketing and promotion of pharmaceutical products, medical devices and cosmetics. Natalia also provides advice to multinational tobacco companies on a wide variety of regulatory and commercial matters, particularly the marketing, promotion and advertising of Next Generation Products. In addition, she focuses on all areas of IP – such as trademarks, copyrights and patents – advising clients on both contentious and non-contentious IP issues and representing them before the Administrative Committees, as well as Civil and Administrative Courts.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: n.kapsi@zeya.com
LinkedIn: www.linkedin.com/in/natalia-kapsi

Yolanda Antoniou-Rapti focuses on Greek and EU data protection, privacy, cybersecurity, competition & antitrust, corporate and commercial law. She advises on all aspects of EU and Greek data protection compliance issues, including assisting clients in identifying compliance gaps, both in the context of GDPR compliance audits and M&A due diligence reviews, assessing and managing relevant risks, and in taking steps to ensure overall compliance, including conducting trainings and workshops. Yolanda's practice also covers data protection litigation, as well as advisory and assistance tasks on day-to-day matters, including drafting and negotiating privacy terms in contracts, drafting privacy policies and notices, data processing agreements, consent forms, the use of new technologies, ePrivacy issues, data breach management and notification, international data transfers and carrying out data protection impact assessments.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: y.antoniou@zeya.com
LinkedIn: www.linkedin.com/in/yolanda-antoniou-rapti

Celia Karvouni is a member of the Zepos & Yannopoulos M&A and project development practice, as well as the healthcare, pharma & life sciences practice. She joined our team as a trainee lawyer with great interest in corporate, pharmaceutical and civil law. Celia regularly focuses on corporate and commercial matters on the day-to-day operations of international and domestic clients, including the drafting and review of commercial contracts and corporate resolutions. She joined the firm in September 2023.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: c.karvouni@zeya.com
LinkedIn: www.linkedin.com/in/vasiliki-celia-karvouni-629a18208

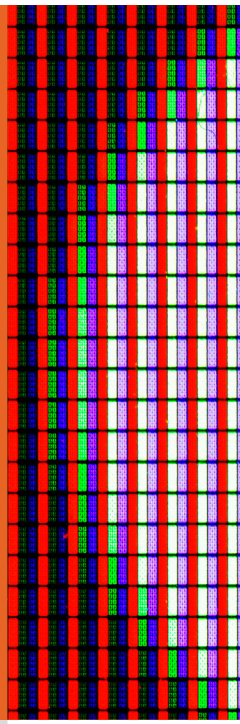
Zepos & Yannopoulos is a leading Greek law firm known for its long heritage, legal acumen and integrity. As a full-service business law firm, we take pride in our distinctive mindset and offering. This shows not only in responsiveness, but also our ability to field versatile, approachable, easy-to-work with teams of practitioners who truly understand our clients' interests. Our strong international orientation is echoed in our structure, standards and approach, and ultimately attested in the profile of our client base, our rankings and the network of our affiliations and best-friend law firms around the world. Established in 1893, we know that change, whether in the legal or economic environment, is inherent to our jurisdiction; we are accustomed to implementing untested legislation, structuring innovative solutions and putting our bold legal argumentation to the service of our clients. For more details on our firm and practice please visit our website.

www.zeya.com

ZEPOS & YANNOPOULOS

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