Legal 500
Country Comparative Guides 2024

Greece
TMT

Contributor

Nikolinakos & Partners
Law Firm

Dr. Nikos Th. Nikolinakos

Managing Partner | nikolinakos@nllaw.gr

Dina Th. Kouvelou

Partner | kouvelou@nllaw.gr

Alexis N. Spyropoulos

Partner | spyropoulos@nllaw.gr

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Greece.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Greece: TMT

1. Is there a single regulatory regime that governs software?

No specific regulatory regime governing software exists. There are however provisions regulating software related matters, distributed over different sectors of law, as analyzed below.

2. How are proprietary rights in software and associated materials protected?

Software in Greece is considered literary work and protected under the provisions of intellectual property law, according to par. 3 of art. 2 of Law 2121/1993. A basic prerequisite for granting the protection of the intellectual property law to a software is that it is original, in the sense that it is the result of the personal intellectual work of its creator. In a few exceptional cases software can be protected by the Industrial Property Law as a patent (Law 1733/1987), if it qualifies as a patent, i.e. if it is a new invention, involving an inventive step and demonstrative of industrial application.

Supplementary protection is provided by the law of unfair competition, and specifically articles 16-18 of Law 146/1914 concerning the protection of commercial and industrial secrecy, as long as this software constitutes a commercial secret or a business secret, and as long as legal and technical measures have been taken to prevent any third party's access to the program. Furthermore, in case of outright copy or imitation of software by a competitor, the general clause of article 1 of Law 146/1914, prohibiting unfair behaviours, may apply.

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

The creator of a computer software will obtain the intellectual property rights, provided that the software is original, in the sense that it is the result of the personal intellectual work of its creator.

However, the Intellectual Property Law provides that that the economic right over a computer program that is created by an employee in the execution of their employment contract or following the instructions given by the employer, shall be *ipso jure* transferred to the latter, unless otherwise provided by contract (Article 40 of Law 2121/1993).

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There are no specific laws in the Greek legal framework governing the harm caused by software or computer systems. General provisions apply. Under Greek law the Consumer's law establishes a strict liability regime. Moreover, the producer is liable , in accordance with the provisions of Greek Civil Code on contractual liability and tort.

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Greek Criminal Code contains provisions on the misuse of software, such as the offenses of unlawfully copying, depicting, using or disclosing to a third party or violating data or computer programs that constitute state, scientific or professional secrets or secrets of a public or private sector company, copying or using computer software without a corresponding right, as well as the distribution (sale, supply, possession, delivery) of computer devices or programs, which could facilitate the disruption of IT systems, and the commission of fraud through the use of a computer.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

Several laws may apply to software contracts and the use of cloud technology such as the Greek Civil Code (GCC), as software concession contracts, software maintenance and software development contracts, the GDPR and its implementing Law 4624/2019, as well as the Greek

Consumer Protection Law. In addition, the rules around contracts for the supply of digital content (computer programs) regarding their compliance with the contract and the available remedies in case of failure to supply are defined by Directive 2019/770, which has been incorporated into Greek law by Law 4967/2022.

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

The software supplier, operating off-line or over the Internet, has the primary obligation to deliver the goods in the agreed condition and free of actual defects (534 GCC) and to transfer the software free of any legal defects. The seller/supplier of the software is liable for the actual defects and the lack of agreed characteristics under Article 537 GCC "regardless of fault" and is only exempted if the buyer was aware of them at the time of the conclusion of the contract or if the non-performance is due to materials provided by the buyer.

According to Article 332 of the GCC, any prior agreement excluding or limiting liability for wilful misconduct or gross negligence is null and void. The exemption of the supplier for slight negligence may be agreed in advance unless (a) the buyer is in the service of the seller, (b) the liability arises from the exercise of an undertaking for which the authority was previously delegated to the seller, (c) if the exemption clause has not been individually negotiated between the buyer and the supplier, which is also related to the Greek Consumer Protection Law.

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

IPR infringement claims under (d), and wilful or deliberate breaches under (g), are typically excluded from any financial cap on the software vendor's liability to the customer. The financial cap cannot be less than the actual damage. However, the parties are free to agree on a financial cap for their respective obligations under the contract in cases where liability arises from simple negligence.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

With the escrow agreement, if two or more have a dispute over a software, they may, in order to secure their disputed or uncertain rights over it or in the process of selling it, agree to deliver the software to a third party escrow holder for safekeeping, until their dispute is resolved, either by consensus or by court decision, in which case the escrow holder is obliged to return it. The escrow holder can be any natural or legal person, who will be selected by the depositors. However, escrow agreements are not very widely met in Greek jurisdiction.

10. Are there any export controls that apply to software transactions?

Export controls applicable to software transactions are those determined by the Customs Authorities and are subject to the application of EU Regulation 2021/821.

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

In Greece, there are no specific technology laws that exclusively govern IT outsourcing transactions. Generally, IT outsourcing transactions in Greece would be governed by various laws and regulations that cover contract law, data protection, intellectual property, labour regulations, and taxation.

In 2020, the Bank of Greece issued Executive Board Act no. 178/5/2.10.2020 adopting the European Banking Authority's guidelines on outsourcing that also cover outsourcing to cloud service providers. The Act establishes a harmonised framework for outsourcing functions for all institutions supervised by the Bank of Greece, which includes a clear definition of outsourcing and of critical or important functions. In addition, it contains specific internal governance requirements and obligations for institutions, both at pre-contractual and contractual stages, aimed at effectively managing the risks posed by outsourcing agreements.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

Under Greek law, IT outsourcing is governed primarily by the contractual terms agreed on an *ad hoc* basis between the parties, as the decision to outsource any kind of services, including IT services, is subject to the freedom of contracts based on the provisions of article 361 of the Greek Civil Code.

In the event that IT services are outsourced to a third party, the individual employment contracts of the staff that previously performed the service are not automatically transferred to the outsourcing supplier, even in cases where the outsourcing of IT services takes place between associated companies.

However, under specific circumstances, an outsourcing contract could be regarded as a contract of legal transfer of part of the business, in the context of Council Directive 2001/23/EC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses and Greek Presidential Decree No. 178/2002 on measures relating to the protection of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, in compliance with Council Directive 98/50/EC, which was codified in the Greek Labour Code in 2022.

This applies only to contracts that, alongside the outsourced activity, provide for the transfer to the outsourcing supplier of third-party contracts, assets, employees etc. of the original business. In this context, outsourcing falls within the meaning of the "legal transfer" of business, whereby the transferred activity or operation constitutes an economic entity that retains its identity, meaning an organised grouping of resources which has the objective of pursuing in a stable manner, an economic activity, whether or not that activity is central or ancillary.

If an outsourcing contract meets the above conditions and constitutes a legal transfer of part of an undertaking, then the transferor's (original business-outsourcer) rights and obligations arising from a contract of employment or from an existing employment relationship, connected to the transferred part of the business, shall, by reason of such transfer, be automatically transferred to the transferee (outsourcing supplier). The transferor and the transferee are required in this case to comply with the provisions of Presidential Decree No. 178/2002, which aims to safeguard employees' rights and protect their interests when their employment is transferred to a new employer. According to Presidential Decree No. 178/2002, the transfer of an undertaking, business or part of an undertaking or business does not in itself constitute grounds for dismissing workers. However, this does not preclude, subject to compliance with the provisions relating to dismissals, employee dismissals which may take place for economic, technical or organisational reasons involving changes in the workforce.

It should be stressed that this automatic transfer of the employment contracts takes place only if the outsourcing contract provides for the transfer of an economic entity, an organised grouping of resources or part of the business, and not of the outsourced activity alone.

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The most important legislation applicable to telecoms comprises the following acts:

- Law No. 4961/2022 on the "Emerging Information and Communication Technologies, Strengthening of Digital Governance and other provisions".
- Law No. 4727/2020 on "Digital Governance (Transposition into Greek Legislation of Directive (EU) 2016/2102 and Directive (EU) 2019/1024) – Electronic Communications (Transposition into Greek Legislation of Directive (EU) 2018/1972) and other provisions".
- Law No. 4070/2012 on electronic communications.
- Law No. 4577/2018 transposing into Greek legislation Directive 2016/1148/EU of the European Parliament and of the Council on measures for a frequent level of security of network and information systems across the Union and other provisions (NIS1 Directive) and Ministerial Decision No. 1027/2019 of the Minister of Digital Governance, specifying the implementation and procedures provided in Law No. 4577/2018.
- Law No. 4411/2016 on the ratification of the Convention on Cybercrime and transposition of Directive 2013/40/EU on attacks against information systems, replacing Council Framework Decision 2005/222/JHA.
- Law No. 2251/1994 which applies to consumer

protection issues, as amended.
- Presidential Decree No. 131/2003 on e-commerce, as amended by Law No. 4403/2016, Article 24.
- Joint Ministerial Decision No. 70330/2015 on adjustments to the Greek legislation in line with Directive No. 2013/11/EU on Alternative Consumer Dispute Resolution, and the adoption of additional national measures for the implementation of Regulation 524/2013 on Online Dispute Resolution for Consumer Disputes.
- Presidential Decree No. 47/2005 on procedures as well as technical and organisational safeguards for the removal of communications confidentiality and its safeguarding.
- ADAE's Decision no. 28/2024, which is a Regulation on the Security of Electronic Communications Networks and Services, replacing the Regulation for the Assurance of Confidentiality in electronic communications (ADAE's Decision No. 165/2011) and the Regulation for the security and integrity of networks and electronic communication services (ADAE's Decision No. 205/2013).
- EETT Decision No. 991/4/31.05.2021 on the regulation of General Authorisations.
- EETT Decision No. 792/07/2016 on the fourth round of market analysis of wholesale fixed local access market, and the introduction of VDSL vectoring technology for the provision of NGA access in Greece.
- EETT Decision No. 874/2/2018 "Regulation on the determination of Rights of Way and Rights of Use of Rights of Way pursuant to Article 28 (9) of Law 4070/2012".
- EETT Decision No. 876/7B/17/12/2018 on a National Open Internet Regulation specifying issues of Regulation (EU) 2015/2120 on open internet access and amending Directive 2002/22/EC on Universal Service and rights of users in terms of electronic communications networks and services.
- EETT Decision No. 934/03/2020 on the third round of market analysis of wholesale and retail leased lines markets.
- EETT Decision No. 934/04/2020 on temporary measures on pricing methodology and pricing of wholesale leased lines products.
- EETT Decision No. 937/03/2020 on bottom-up LRIC+ models and pricing of wholesale access products.
- EETT Decision No. 968/01/2020 on the fourth round of market analysis of fixed origination and termination wholesale markets.
- EETT Decision No. 977/03/2021 on the definition of pricing methodology and pricing of wholesale leased lines products of wholesale leased line terminals, wholesale leased line trunk segments, which will apply until the implementation of the bottom-up LRIC+ wholesale leased lines pricing models according to EETT Decision No. 934/03/27.04.2020 following the temporary measures of EETT Decision No. 934/04/27.04.2020 and 938/01/25.05.2020 in accordance with Article 32 of Directive 2018/1972 and Article 140 of Law No. 4727/2020.
- EETT Decision No. 966/02/2020 regulation on numbering management and allocation.
- EETT Regulation No. 938/01/2020 on the approval of temporary prices of wholesale leased lines.
- EETT Decision No. 968/01/2020 on the analysis of termination market to individual fixed networks.
- EETT Decision No. 1016/06/2021, on the definition of temporary wholesale price for Ethernet circuits above 1 Mbps
- EETT Regulation No. 919/26/2019 on the licencing of antennas and base stations.
- Ministerial Decision No. 7435 ΕΞ 2022/28-2-2022 on the determination of the content of the Aggregate Service, the reasonable request, the selection criteria and the procedure for the designation of an undertaking subject to an Aggregate Service provision obligation.
- Ministerial Decision No. 20448 ΕΞ 2022/26-05-2022 on the procedure for apportioning the net cost of the Aggregate service, compensation of the Aggregate Service Provider.
- Ministerial Decision No. 12698 ΕΞ 2022/4-4-2022 on measures for the affordability of Aggregate Service services which are not provided in a set location.
- EETT Decision No. 1027/004/2022, "Regulation setting quality indicators and performance targets in the provision of the Aggregate Service".
- EETT Decision No. 1039/2/2022, "Regulation on the Aggregate Service pricing principles".
- EETT Decision No. 986/01/2021, on the results of the audit of the calculation of the Net Cost of Aggregate Service submitted by OTE S.A. for the years 2012, 2013, 2014, 2015 and 2016.
- EETT Decision No. 938/2/2020 "Provision of a calling line identification service"
- EETT Decision No. 732/4/11/9/2014 on access and interconnection.
- General Data Protection Regulation (GDPR) (EU) 2016/679, Law No. 4624/2019 on the protection of personal data.

With regard to pending legislation, it should be mentioned that by the end of the year NIS2 Directive is expected to be transposed into national legislation. NIS2 has included providers of public electronic communications networks and providers of publicly available electronic communications services within its scope, as subcategories of Sector 8 "Digital infrastructure". In light

of the above, if the national legislator maintains these sectors when adopting the Directive, telecommunications will fall within the scope of obligations that will be introduced.

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

In Greece, the development of technical standards for mobile communications and connected technologies is governed by the Hellenic Organization for Standardization (ELOT) and the Hellenic Telecommunications and Post Commission (EETT). The Hellenic Organization for Standardization (ELOT) is the national standards body of Greece and has been founded by the Greek Law 372/1976. ELOT's mission is the promotion and application of standardization in Greece. ELOT's main activities are: preparing and publishing standards, awarding marks of conformity and granting certificates of conformity, certifying quality systems for businesses and conducting laboratory tests. The Hellenic Telecommunications and Post Commission (EETT) is an independent authority with administrative and financial autonomy. It acts as the National Regulatory Authority (NRA) in matters of provision of services and networks for electronic communications, related facilities and services, and postal services.

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Technical standards that promote interoperability between connected devices significantly influence the development of connected technologies in the following ways:

1. Interoperability standards enable diverse IoT devices (such as sensors, actuators, and smart appliances) to work together harmoniously.
2. When devices follow common protocols and interfaces, they can seamlessly exchange data, commands, and status information. This seamless integration simplifies the development process and speeds up the time-to-market for new technologies.
3. When manufacturers comply with recognized standards, consumers and businesses gain confidence in the technology. They are assured that devices from different vendors will work together reliably, driving adoption and investment.
4. By leveraging existing standards, companies save resources. Additionally, interoperability reduces maintenance costs and ensures smoother upgrades.
5. Standards provide a foundation upon, which innovators can build. As a result, developers can focus on creating novel applications and services instead of reinventing basic communication mechanisms.
6. Standards help ensure compliance, leading to safer and more reliable products.

In Greece, as in other EU countries, the legal framework concerning these standards is influenced by both national and EU laws and especially in the field of Intellectual Property (IP), Competition Law and Data Protection.

16. When negotiating agreements which involve mobile communications or other connected technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

In Greece, the main legislative framework regarding the SEPs, includes the Greek Patent Law (Law No. 1733/1987) and its amendments, as well as the Competition Law No. 3959/2011, which align with the EU regulations, as there are no special provisions for SEPs.

When negotiating agreements related to mobile communications or other connected technologies, specific considerations regarding standard-essential patents (SEPs), should be taken under consideration, as the following:

Regarding the liabilities, when using SEPs, parties should consider potential infringement claims. In other words, if a product infringes a SEP, the licensee may face legal liabilities as in general, the liability of the licensee in Greek law is multidimensional and includes exploitation, protection against infringement, public disclosure, preservation of rights, compliance with regulatory obligations, civil liability and liability for insufficient or false statements. These duties and obligations ensure a balance between protecting inventions and promoting innovation and competition.

In addition, the parties must address indemnification clauses and allocate risks appropriately.

Moreover, as regards the warranties, SEP holders typically do not provide warranties regarding the validity

or enforceability of their patents. As a result, licensees should seek clarity on this and negotiate warranties accordingly.

The agreements shall also define the scope of the license and be clear about which patents are included.

Other than that, negotiating parties must agree on the price payable for the royalties e.g. the granting licenses and technology transfer agreements.

17. Which body(ies), if any, is/are responsible for data protection regulation?

The Hellenic Data Protection Authority (HDPA) is a constitutionally established independent public authority that serves as the supervisor for the application and enforcement of the data protection legislation. HDPA's structure and competences are regulated by Presidential Decree No. 30/2024 (Government Gazette 89/A/13-6-2024) entitled "Organisation of the Personal Data Protection Authority".

Moreover, the Hellenic Authority for Communication Security and Privacy (ADAE) is responsible for the protection of free correspondence and communication, including personal data issues in telecommunications.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR). The regulation focuses on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR repealed Directive 95/46/EC (Data Protection Directive) and has led to increased (though not total) harmonization of data protection law across the EU Member States.

Since 29 August 2019, the main data protection legislation in Greece has been Law 4624/2019, which has implemented Regulation (EU) 2016/679 (GDPR) and incorporated Directive (EU) 2016/680. Law 4624/2019 repealed Law 2472/1997, which incorporated Directive 95/46/EC. The main objectives of the Law are the protection of natural persons against the processing of personal data, the free movement of such data and the repeal of the Directive 95/46/EC.

Law 3471/2006, which incorporates Directive 2002/58/EC (E-Privacy Directive) – as amended by Directive 2006/13/EC – is complementary and specific to the institutional framework for the protection of personal data in the field of electronic communications.

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Based on the provisions of the GDPR, the HDPA may impose administrative fines up to €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, or, for serious violations related to data subjects' rights, fines up to €20,000,000 or 4% of the total worldwide annual turnover, whichever is higher. Pursuant to the provisions of the national law 4624/2019 on data protection, when the Controller is a public body, the fine can go up to €10,000,000.

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

According to the provisions of Law 4961/2022, the processing of personal data when using AI systems must be carried out in accordance with the principles and rules of the GDPR. Therefore, technology contracts in Greece typically refer to the GDPR.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Law 4961/2022 provides for the establishment of a Coordination Committee for artificial intelligence, which has the task of coordinating the implementation of the National Strategy for the development of artificial intelligence and is responsible for:

1. decision-making concerning the implementation and continuous improvement of the National Strategy for the development of AI,
2. the formulation of national priorities and guidelines for the optimal implementation of the National Strategy for the development of AI and
3. the design and promotion of proposals for policies and actions, as well as the submission of a proposal to public sector bodies for the adoption of corrective measures, if deviations in the implementation of the National Strategy or impacts on the fundamental

rights of natural persons are found.

In the same Law, a Committee for the Supervision of the National Strategy for the development of AI is established within the Ministry of Digital Governance, as an executive body of the Coordinating Committee for AI. The Supervisory Committee is responsible for:

1. mapping the progress of the implementation of the National Strategy for the development of AI and notifying the Coordinating Committee of derogations in the implementation,
2. overseeing the implementation of the decisions of the Coordinating Committee, and
3. coordinating the activities of the bodies involved in the National Strategy for the development of AI, based on the guidelines of the Coordinating Committee.

Finally, pursuant to Law 4961/2022, the Ministry of Digital Governance establishes an Artificial Intelligence Observatory, which is part of the General Secretariat for Digital Governance and Simplification of Procedures, with the mission of collecting data on the implementation of the National Strategy for the development of AI, drafting reports on activities related to AI and supporting the competent bodies in setting priorities and highlighting opportunities and value-added sectors. The Observatory will draw up and update Key Performance Indicators and provide information on:

- activities related to AI in Greece,
- public or private sector bodies active in the field of AI in Greece,
- the available educational activities on AI that take place in Greece at all levels of education,
- successful examples and best practices for the uptake of AI in the private and public sector, and
- the impact of AI activities on the fundamental rights of natural persons.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

At national level, the law that regulates issues related to artificial intelligence in Greece is Law 4961/2022. Its purpose is to create the appropriate institutional background to ensure the rights of natural and legal persons and to enhance accountability and transparency in the use of artificial intelligence systems as well as for the legitimate and safe use of AI technology by public and private sector entities.

The law states that public sector bodies may, in the exercise of their functions, use artificial intelligence systems in the process of making or supporting the process of making a decision or adopting an act affecting the rights of a natural or legal person only if such use is expressly provided for in a specific provision of law containing appropriate safeguards for the protection of those rights. Any public sector body using an artificial intelligence system shall carry out an algorithmic impact assessment before the system starts operating. In addition, the law provides for certain transparency obligations such as the obligation for the public sector to keep a register of the artificial intelligence systems it uses.

In addition, it includes specific arrangements (information obligations, respect for the principle of equal treatment and non-discrimination in employment) regarding artificial intelligence systems that may be used by private sector companies and which affect any decision-making process concerning employees or potential employees and which has an impact on their working conditions, selection, recruitment or assessment. Any private sector undertaking which is a medium or large entity shall keep an electronic register of the artificial intelligence systems which it uses either in the context of consumer profiling or in the context of the evaluation of any of its employees or natural persons associated with it. Each company shall establish and maintain an ethical data use policy, which shall include information on the measures, actions and procedures it applies in relation to data ethics when using AI systems.

The AI Act published on 12 July 2024, adopts a risk-based assessment. Based on this approach, AI systems are divided into four levels according to the type and level of risk they pose: unacceptable risk, high risk, low risk, minimal risk. AI systems that fall into the unacceptable risk category are completely prohibited, high risk systems must comply with specific requirements, while low or minimal risk systems must comply with fewer or no requirements at all. Finally, it provides for specific requirements for general-purpose AI systems. This Regulation shall be binding and directly applicable in all Member States, including Greece. However, each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority for the purposes of this Regulation 12 months after the date of entry into force of this Regulation.

On 28 September 2022, the Commission delivered on the objectives of the White Paper and on the European Parliament's request with the Proposal for an Artificial Intelligence Liability Directive (AILD). The purpose of the

AI Liability Directive is to set uniform rules on access to information and to reduce the burden of proof in relation to damage caused by AI systems in order to establish broader protection for victims (whether individuals or businesses) and to strengthen the AI sector through increased safeguards. The Directive simplifies the legal procedure for victims when they have to prove that someone's fault has caused damage/loss. The Commission proposal has not yet been adopted by the European Parliament. Since this legislative act will be in the form of a directive, it will have to be incorporated into Greek law in order to have effect.

Finally, the GDPR also applies to the field of artificial intelligence. Some systems use personal data and/or make automated decisions concerning natural persons and in this case, issues of personal data breaches arise. Article 5 of the GDPR sets out the general principles governing data processing, which reflect the philosophy of the more specific provisions of the Regulation.

When an AI technology is applied for decision-making affecting natural persons, the user as controller must take into account the prohibition in Article 22(2)(a) of the GDPR. According to this provision, the data subject has the right not to be subject to a decision taken solely on the basis of automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar way. An exception to this prohibition is provided for in Article 22 par. 2 GDPR, according to which this prohibition does not apply where the decision is necessary for the conclusion or performance of a contract between the data subject and the controller or is permitted by EU or Member State law or is based on the explicit consent of the data subject. However, the controller should then take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, in accordance with par. 3 of the same Article. In particular, it should be ensured that there is a right of intervention by the controller and a right to challenge the decision. Another obligation of the controller is to carry out a data protection impact assessment (DPA), in accordance with Article 35 GDPR, which also applies to the AI systems in which personal data are processed.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

In the AI Act published in the Official Journal of the EU on 12 July 2024, there are special provisions regarding the deployment and use of Large Language Models and generative AI. According to article 3 par. 63 of the AI Act "general-purpose AI model" means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market. Furthermore, according to article 3 par. 66 "general-purpose AI system" means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems. In chapter V of the Regulation in the articles 51-55 special provisions are provided for the general-purpose AI models.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

In Greece, technology contracts are mainly regulated by the Civil Code and the Commercial Code; as an EU member state, Greece also adheres to EU legislation. At present, technology contracts do not typically contain mandatory provisions dealing with AI risk. However, Law 4961/2022 on "Emerging IT and communications technologies, strengthening digital governance and other provisions", contains provisions regarding the use of AI by public sector bodies. This national legal framework provides that in every public contract involving the design or development of an AI system, the tender must include the following obligations of the contractor:

a. to provide information to the public sector body to ensure the transparent operation of the system, without prejudice to the provisions on the protection of military, commercial and industrial secrecy, as well as the obligation to waive claims which may jeopardise the right of natural or legal persons to information;
b. to take appropriate measures in designing, developing, and operating an AI system, to ensure its compatibility with the legal framework, in particular with regard to the protection of human dignity, respect for privacy and protection of personal data, non-discrimination, gender equality, freedom of expression, universal access for persons with disabilities, employees' rights

and the principle of good governance.

Law 4961/2022 also provides that the supply or services contract for the design or development of an AI system must mandate that the AI system is delivered to the public sector body under conditions that allow the public sector body to study its functionality and its decision-making parameters; to make improvements to the system and publish or otherwise make available such improvements.

Although technology agreements usually take the form of software licences, some are much more complex. In many cases, the organisation procuring the technology services provides a solution that includes multiple components. This is important to bear in mind when drafting a technology agreement to avoid any ambiguity, to explicitly describe the parties' obligations, to include charges covering all the components and to foresee all possible risks that may lead to a breach of contract or exposure to liabilities. Depending on the technology agreement, various chapters of the Civil Code may be applicable (ie, sales contracts, work contracts, service contracts).

It is common for software and technology services or technology agreements to include clauses that limit the liability of the provider. As issues of civil and criminal claims from defective AI systems are already starting to arise, the tendency to cover risks and to limit liability up to certain amounts has also become noticeable in practice.

It is important to note that from a judicial point of view, clauses that extensively limit the liability of the professional against the consumer in B2C agreements – especially if they have not been negotiated – are usually considered as abusive and, thus, null and void. On the other hand, in B2B agreements under which the parties usually demonstrate similar bargaining powers, the freedom of the parties supersedes, unless one party has acted maliciously or in a grossly negligent manner or has acted without previous experience and knowledge in this type of agreement, thus demonstrating a disadvantage in bargaining.

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Internationally, the software is protected by intellectual property law through the Agreement on Trade Related Aspects of IPR, Including Trade in Counterfeit Goods, which was ratified in Greece by Law 2290/1995. Correspondingly, at European level, in art. 1 par. 1 of Directive 91/250, it is expressly stated that computer programs and the preparatory material for their design are considered works of speech, protected under the copyright provisions of the Berne Convention. Directive 91/250 was codified by Directive 2009/24 (Art. 1 par. 1) and transposed into Greek law by Law 2121/1993 (Art. 2).

Additional protection to software is provided by the law of unfair competition, as defined by Law 2121/1993 (Article 45 par. 1). Under this law the software can be protected by the provisions of Articles 16-18 of Law 146/1914 concerning the protection of commercial and industrial secrets. A prerequisite for this protection is that the computer program constitutes a trade secret or otherwise, a secret of the business, while at the same time, legal and technical measures are taken to exclude any third party from accessing the program.

Software contracts are also governed by the general provisions of the Civil Code, when and as long as they are not superseded by ad hoc provisions of Law 2121/1993 on intellectual property. In any case, their parallel application is not excluded, particularly in relation to sanctions for violation of the agreed terms of use. Regarding the exploitation of the author's work, copyright law regulates what applies in the event of a transfer of his economic rights, defines the concept of contracts and licenses and sets certain interpretative rules that ensure the most favourable protection of rightholders vis-à-vis their contractual partners. It should be emphasized that not only transfers, but also the conclusion of contracts or licenses require the existence of a constituent document (Art. 14, 8 and 16 of Law 2121/1993).

The specific nature of computer programs has triggered theoretical discussions on the inclusion of these contracts in regulated contractual forms. In practice, there is a diversity of conventional models, based on the combination of regulated contractual forms with non-legally established contractual forms, which makes it very difficult to distinguish between them. In Greece, there is a tendency to stipulate in contracts that the software is protected by applicable copyright law and that all rights not expressly granted in the contract are reserved. In addition to contractual commitments and confidentiality conditions, it is customary to provide for penalty clauses and indemnity provisions for consequential damages and lost profits.

26. What are the principal laws (present or

impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

In July 2022, Law 4961/2022 on "Emerging Information and Communication Technologies, reinforcement of Digital Transformation and other provisions" was published in the Government Gazette. This law provides a definition of Blockchain and Distributed Ledger Technologies and contains a dedicated chapter concerning the applications of Distributed Ledger Technologies (Chapter E). Chapter E contains provisions on the validity and the enforceability of a record on the Blockchain or on another DLT. Specifically, this Chapter:

- provides that data records or transactions may be conducted through a Blockchain or other DLT, thus rendering valid the exercise in this manner of declarations of will, and acknowledges that a Blockchain (or other DLT) record or transaction may form part of a main contract conducted by other means.
- references provisions of the Civil Code concerning the invalidity of declarations of will and of transactions, and defects of consent.
- provides that in case a Blockchain or other DLT record is declared invalid, courts may rule for *restitutio in integrum* by way of amendment of the record or transaction on the Blockchain or by way of compensation paid to the injured party.
- allocates the burden of proof, providing that the party invoking the existence of a record or transaction made on the Blockchain or other DLT is responsible for presenting all the relevant data or information to the court or other administrative body. It also defines that for the conversion of data or information from any programming language or code into a readable format, a cryptography expert report may be provided.

Law 5113/2024 was published in June 2024, which, among other issues, adopts measures to implement Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU. Crucially, Law 5113/2024 recognises that Greek SAs can issue digital securities through the use of blockchain technology, which can be listed on a stock exchange or relevant market infrastructures

In particular, Law 5113/2024:

- broadens the definition of financial instruments to include financial instruments (shares, bonds, etc.) issued, registered, transmitted and stored using blockchain technology (DLT.
- appoints the Hellenic Capital Market Commission as the competent authority for the application of Regulation (EU) 2022/858 and the acts adopted pursuant thereto.
- provides that a DLT is a valid dematerialisation method for the securities issued by Greek S.A.s, such as shares, bonds and bond loan notes.
- enables the admission and initial recording of DLT financial instruments in a DLT market infrastructure or a Central Securities Depository.
- establishes rules on how DLT financial instruments are transferred, on their beneficiaries and on the establishment and exercise of rights in rem attached to them.
- confirms that provisions of laws and regulations relating to transferable securities also apply to DLT transferable securities

Also, Law 4557/2018 on the "Prevention and suppression of the legalisation of proceeds of crime and terrorist financing (Incorporation of Directive 2015/849/EU) and other provisions" contains a definition of virtual currencies and defines the obligations of digital wallet providers and providers of exchange services between virtual currencies and fiat currencies that provide their services in Greece or from Greece to other countries. These categories of providers are also obliged to register their activities in a special register which is maintained by the HCMC, pursuant to article 6 of the same law. By virtue of decision No 5/898/3.12.2020 (as amended by decision No 7/960/04.08.2022) of its BoD, the HCMC determined the formalities for providers' registration (the digital submission of the application, the type of information and documents required for the registration and the relevant costs) as well as the criteria and the process for the removal of providers from the registers. If a provider's request for registration is not approved, the HCMC prohibits them from providing services.

In addition, an assessment of the characteristics of each blockchain application is advisable prior to entering the Greek market, to assess whether a particular blockchain application might fall within the scope of Law 4514/2018 which transposed Directive 2014/65/EU on markets in financial instruments (MiFID II).

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation

of the general purpose of those laws.

Regulation 2019/1150 applies to online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website users, respectively, that have their place of establishment or residence in the Union and that, through those online intermediation services or online search engines, offer goods or services to consumers located in the Union, irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable. The purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down rules to ensure that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities. Following the above, all the obligations arising from Regulation 2019/1150 govern search engines and marketplaces.

Online marketplaces and search engines are also impacted by the Digital Services Act (DSA) and the Digital Markets Act (DMA). The Digital Services Act and the Digital Market Act form a single set of rules that apply across the whole EU and have two main goals:

1. to create a safer digital space in which the fundamental rights of all users of digital services are protected;
2. to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally.

Similar to Q. 13 and the imminent transposition of the NIS2 Directive by the end of the year, it is noted that digital providers are included among the sectors the NIS2 Directive covers and two of its subcategories are "Providers of online marketplaces" and "Providers of online search engines". In light of the above, if the national legislator maintains these sectors when adopting the Directive, Search Engines and Marketplaces will fall within the scope of obligations that will be introduced.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

The conduct of platform providers, otherwise of any natural or legal person providing information society services, is primarily regulated under Presidential Decree 131/2003 that has transposed Directive 2000/31/EC (E-Commerce Directive) into the national legal order. As regards the platform liability regime, the Decree exempts intermediaries from liability for the content they transmit or store provided that their services have a neutral, merely technical and passive role towards the hosted content, which implies that the service provider has neither knowledge of nor control over the information which is transmitted or stored. (namely "caching", "mere conduit" and "hosting" services). To benefit from the liability exemption, the information society service provider, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned.

Law 4779/2021 which transposed the amended Directive 2018/1808/EU (AVMSD) into the Greek legal order and updated the legal framework for audiovisual content, in all its forms of promotion and reproduction – i.e., traditional television, custom-made audio-visual services, and also for the first time, both video-sharing platforms and social media services exclusively with regard to their audio-visual content. The obligations imposed on VSPS under Greek jurisdiction, including social media and platforms where user-generated content is shared, mainly include the protection of minors, the protection of general public from content bearing incitement to violence or hatred directed against group(s) of persons and obligations regarding audiovisual commercial communications that are marketed, sold or arranged by those providers. While VSPS which do not fall under Greek jurisdiction, are not caught by the obligations set by the national regime, it is nonetheless recommended by the Law that these services be encouraged to develop codes of conduct with the aim of further protection of consumers, of minors, as well as of public health and of fair competition.

Furthermore, platform providers are subject to the rules governing the confidentiality of communications (namely Law 2225/1994, Law 3917/2011 regarding data retention, which transposed Directive 2006/24/EC, and relevant ADAE Decisions and Regulations), as well as to the obligations set by the Personal Data protection framework namely Law 4624/2019 which implemented Regulation EU 2016/679 (GDPR), and Law 3471/2006, which transposed Directive 2002/58/EC (E-Privacy Directive). If the providers offer services to regulated entities (such as in financial services, or gaming etc.) they may also be subject to monitoring and supervision by the competent supervision authorities of the said industries.

The Regulation (EU) 2019/1150 "on promoting fairness and transparency for business users of online

intermediation services", which has been implemented by Greece since November 2020 by Law 4753/2020, addresses the imbalance in bargaining power between online platforms and small businesses conducting their business on the platforms. Starting from that date, the terms and conditions of online platforms should: i) be drafted in plain and intelligible language; ii) cannot be changed without an advance notice of at least 15 days; iii) need to exhaustively spell out any reasons that could lead to the delisting of a business user; iv) list the main parameters that determine the ranking of search results (this also applies to search engines like Google); v) include information about any ways in which a platform that sells on its own marketplace might give preferential treatment to its own goods or services; vi) be clear about the data policy of the platform – what data it collects, whether and how it shares the data, and with whom. In addition, the Regulation makes it easier for business users to seek redress in case of problems.

In July 2022 the European Parliament adopted a package of legislation consisting of two pieces, the Digital Services Act (DSA) and the Digital Markets Act (DMA). DSA updates the framework for handling illegal or potentially harmful content online, the liability of online providers for third party content and the protection of users' fundamental rights online and entered into force on 16 November 2022. The Digital Markets Act (the DMA) addresses market imbalances, arising from the gatekeeper role of large online platforms (such as search engines, social networking services, certain messaging services, operating systems and online intermediation services). The DMA aims to set out harmonized rules to combat certain unfair practices by gatekeeper platforms and to provide relevant enforcement mechanisms.

Exactly what was stated in Q. 27 in terms with the NIS2 Directive applies to social media as well, since "Providers of social networking services platform" are a subcategory of the sector of "Digital Providers" of the Directive.

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

It should be noted that the revised Product Liability Directive is expected to be published soon, bringing significant and impactful changes to this field. These changes are likely to modernize the existing legal framework, addressing new technological advancements and challenges, particularly those related to artificial intelligence and digital products. The revised Product Liability Directive (PLD) introduces provisions to address liability for products such as software (including AI systems) and digital services that affect the functioning of the product (e.g. navigation services in autonomous vehicles). Additionally, it clarifies the liability rules for companies that substantially modify products before reselling them. It also ensures that consumers are compensated for defective products manufactured outside the EU. The revised PLD broadens the notion of "defect" and allows compensation for damage when products like robots, drones or IoT smart-home systems become unsafe by software updates, AI or digital services that are needed to operate the product, as well as in cases where manufacturers fail to address connectivity risks and cybersecurity vulnerabilities. Under certain circumstances, the new Directive requires manufacturers to disclose information in cases where plausible claims for compensation are made, and alleviates the burden of proof for victims (consumers) seeking compensation for damages resulting from defective products. The final text of the revised PLD was formally endorsed by the European Parliament at the Plenary of 12 March 2024, which adopted its position at first reading.[1]The revised PLD will enter into force on the twentieth day following its publication in the EU Official Journal.

The European Commission published a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (the 'AI liability directive') in September 2022. The Commission proposes to complement and modernise the EU liability framework to introduce new rules specific to damages caused by AI systems. The new rules intend to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies in the EU. Therefore, after the entry into force of the AI Act, it is expected that discussions regarding the adoption of the AI liability directive.

Furthermore, as the metaverse concept expands, European regulators will likely develop frameworks to address the unique challenges it presents. Key regulatory areas might include:

- Digital Identity and Privacy: Laws could be enacted to protect users' digital identities and ensure privacy within the metaverse. This might involve regulations on how personal data is collected, used, and shared in virtual environments.
- Content and Conduct: Regulations may address acceptable behavior and content within the metaverse, aiming to prevent illegal activities, harassment, and other harmful behaviors. This could involve robust moderation and reporting mechanisms.
- Intellectual Property: New legal frameworks

might be needed to address intellectual property rights in virtual spaces, ensuring that creators' rights are protected while promoting innovation and creativity.

Finally, Web 3.0, characterized by decentralized applications and blockchain technology, will likely see significant legal developments in Europe. Key aspects could include:

- Smart Contracts and Legal Recognition: There could be a push to formally recognize smart contracts and ensure they are enforceable under European law, providing clarity on their legal status and the mechanisms for dispute resolution.
- Cryptocurrency and Digital Assets: As part of Web 3.0, regulations on cryptocurrencies and digital assets might be expanded, focusing on anti-money laundering (AML), combating the financing of terrorism (CFT), and consumer protection.

Footnote(s):

[1] European Parliament legislative resolution of 12 March 2024 on the proposal for a Directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)), (Ordinary legislative procedure: first reading) – P9_TC1-COD(2022)0302, Position of the European Parliament adopted at first reading on 12 March 2024 with a view to the adoption of Directive (EU) 2024/... of the European Parliament and of the Council on liability for defective products and repealing Council Directive 85/374/EEC ["Position of the European Parliament of 12 March 2024 for the adoption of a Directive on liability for defective products (revised PLD)"].

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Not in general.

Contributors

Dr. Nikos Th. Nikolinakos
Managing Partner
nikolinakos@nllaw.gr

Dina Th. Kouvelou
Partner
kouvelou@nllaw.gr

Alexis N. Spyropoulos
Partner
spyropoulos@nllaw.gr