



The Legal 500 Country Comparative Guides

Greece

TMT

Contributor

Nikolinakos & Partners Law Firm



Dr. Nikos Th. Nikolinakos

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.

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 behaviors, may apply.

Finally, if it is lawfully registered as such, the title of a software can be protected as a trademark, under the relevant legislation (articles 121 et seq. of Law 4072/2012), when it appears in manuals, accompanying material or packaging. Trademark protection may be extended to the software itself if the title is embedded in such a way that it appears on the screen when the software runs. This is because, according to the law, the proprietor can use the trademark in electronic media as well, such as the software (Article 125 § 1 of Law 4072/2012). However, according to article 126 § 1 of Law 4072/2012, the right granted by the trademark to its

proprietor does not prevent third parties from using their name and address in transactions, as well as indications related to the type, quality, purpose, value, geographical origin and the time of production of the product or service. Therefore, the use of the trademark by distributors would not be unlawful. If it is used in transactions as a distinctive feature, the title of the software may also be protected in accordance with the provisions of Law 146/1914 on unfair competition, and also according to Law 2121/1993 on intellectual property, provided that it is original.

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.

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?

No. However, 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.

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?

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. Special provisions for the management of outsourcing transactions, including IT outsourcing (e.g. outsourcing of cloud services), are included in the relevant act of the Bank of Greece and concern all of the institutions supervised by it (e.g. credit and financial institutions).

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.

In the event of an outsourcing of IT services, any individual staff that perform the service, which is transferred, is not transferred automatically to the outsourcing supplier. In specific, the content of an outsourcing contract is always determined on an ad hoc basis by the two counterparties, the outsourcer and the outsourcing supplier. Without special contractual clauses dictating the transfer of employees, no such transfer can take place automatically, especially when the outsourcing agreement relates only to the outsourced activity. As far as the employees are concerned, even in cases where the outsourcing of IT services takes place between associated companies, the employee cannot be transferred to the outsourcing supplier automatically. Therefore, under Greek law, outsourcing is governed primarily by the contractual terms agreed on an ad hoc basis between the counterparties and no transfer of employees takes place automatically since 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.

Moreover, it should be noted that after the drafting of the above-mentioned outsourcing contract and depending on its specific terms, 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 and Greek Presidential Decree No. 178/2002.

This applies only to contracts that provide alongside the outsourced activity, 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” of Directive 2001/23/EC and the relevant PD 178/2002, as long as, the transferred (outsourced) 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 and not time-limited manner, an economic activity, whether or not that activity is central or ancillary.

Should an outsourcing contract be deemed to meet the above conditions and constitutes, in fact, a legal transfer of part of an undertaking, as required by the Directive 2001/23/EC and the Presidential Decree No. 178/2002, 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. The transferee (outsourcing supplier) will in this case have to comply with the provisions of Presidential Decree No. 178/2002. This ipso jure transfer, relating to the employment contracts, takes place only in the event that, as we explained above, that the outsourcing contract already provides for the transfer of an economic entity/organised grouping of resources/part of the business and not only the outsourced activity.

The above Presidential Decree aims to safeguard employees' rights and protect their interests when their employment is transferred to a new employer, such as a third-party IT outsource provider.

13. Which body(ies), if any, is/are responsible for the regulation of telecommunications networks and/or services?

The Ministry of Digital Governance has the most direct involvement and plays a key role in the telecoms and media sectors.

However, major responsibilities in these sectors are undertaken by regulatory agencies which are independent administrative authorities, with full independence from network operators and service providers. These agencies are the following:

- the Hellenic Telecommunications and Post Commission (EETT): the national regulatory authority that supervises and regulates the electronic communications and postal services market. It is also responsible for the application of competition law in the electronic communications sector and in the postal services sector;
- the National Council for Radio and Television (ESR): an independent administrative authority that supervises and regulates the radio and television market;
- the Hellenic Competition Commission: responsible for the application of competition law in all sectors, excluding the telecoms sector which falls under the EETT's field of competence;
- the Independent Authority for Public Revenue (ADAE): an independent authority responsible for the protection of security and privacy of communications; and
- the Hellenic Data Protection Authority (HDP): an independent authority responsible for the protection of personal data in all sectors.

14. 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, including to the internet and to the audio-visual media distribution sectors, comprises the following acts:

- Law No. 4961/2022 on the "Emerging Information and Communication Technologies, Strengthening of Digital Governance and other provisions".
- Law No. 4070/2012 on electronic communications.
- 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. 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.
- 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. 991/4/31.05.2021 on the regulation of General Authorisations.
- Law No. 3115/2003 on issues related to the protection of communications privacy.
- General Data Protection Regulation (GDPR) (EU) 2016/679, Law No. 4624/2019 on the protection of personal data.
- Law No. 121/1993 on the protection of intellectual property.
- 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.
- 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.
- Presidential Decree No. 47/2005 on procedures as well as technical and organisational safeguards for the removal of communications confidentiality and its safeguarding.
- Decision No. 99/2017, amending ADAE Decision No. 205/2013 titled "Regulation on the Security and Integrity of Electronic Communications Networks and Services".
- 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 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. 2251/1994 which applies to consumer protection issues, as amended.
- EETT Decision No. 843/2/2018 on the regulation of management and assignment of

[.gr] or [.ελ] domain names, which amends and codifies EETT Decision No. 750/2/2015, as amended by the EETT Decisions Nos 760/3/2015 and 757/2/2015.

- Law No. 3592/2007 on the licensing of media and other provisions.
- Law No. 4339/2015 on the licensing of digital terrestrial TV content providers, as amended.
- Ministerial Decision No. 1830/2017 on the determination of the number of tendered licences to providers of free, nationwide, general information, terrestrial digital television broadcasting content.
- Joint Ministerial Decision No. 2178/2017 on the determination of the first bid price of each one of the seven tendered licences to providers of free, nationwide, general information, terrestrial digital television broadcasting content.
- ESR Decisions Nos 61, 63/2018 and 65/2018, as well as 1/2019, 115 and 117/2019.
- Ministerial Decision No. 169/2018 on the Terrestrial Digital Broadcast Frequency Map.
- Ministerial Decision No. 170/2018 on the assignment of a terrestrial digital radio broadcast spectrum to "Hellenic Radio, Television Company Limited" (ETR S.A.).
- Ministerial Decision No. 171/2018 on the limitation of the number of rights to use radio frequencies of terrestrial digital radio broadcasting, national and regional coverage, and determination of the type of competition.
- Law No. 4463/2017 as amended by Law No. 4487/2017, Article 49 on the transposition of the cost reduction Directive 2014/61/EU.
- 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
- Law No. 4635/2019 on investments in Greece.
- EETT Regulation No. 919/26/2019 on the licencing of antennas and base stations.
- Law No. 4886/2022 on the modernization of competition law for the digital age, the amendment of Law No. 3959/2011 and the transposition of Directive (EU) 2019/1.
- 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.

15. 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.

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.

16. Please summarise the principal laws (present or impending), if any, 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.

17. 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.

18. 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?

Technology contracts in Greece typically refer to the GDPR.

19. 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:

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

20. Please summarise the principal laws (present or impending), if any, 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.

At European Union level, in April 2021, the European Commission proposed the first EU regulatory framework for AI (Artificial Intelligence act). On 6 December 2022 the European Council adopted the AI Act's general approach. On 14 June 2023, the Members of the European Parliament adopted Parliaments negotiating position on the AI Act. The aim is to reach an agreement by the end of this year. The proposal for a Regulation 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 to health, safety and security and adverse effects on fundamental rights (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.

In order to ensure effective cooperation and coordination between national supervisory authorities and the Commission and to ensure consistent application of the Regulation, a European AI Council is foreseen. In addition, competent authorities for the implementation

and enforcement of the Regulation shall be established or designated in each Member State.

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.

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.

21. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language

Models and/or generative AI?

There are no specific legislative provisions in respect of the deployment and use of Large Language Models and/or generative AI. See above what was mentioned in question 20.

22. Which body(ies), if any, is/are responsible for the regulation of blockchain and / or digital assets generally?

A specific body tasked with the regulation of blockchain and digital assets in general has not yet been created in Greece.

The Hellenic Capital Market Commission (HCMC) monitors the proper operation, transparency and integrity of financial markets in Greece. It is also responsible for the supervision, for AML purposes specifically, 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. However, the HCMC clarifies that it is not responsible for monitoring cryptoasset markets nor the provision of services in cryptoasset investments.

The Bank of Greece is Greece's central bank and is responsible for ensuring the stability and the sound operation of the financial system (credit institutions, credit companies, etc).

23. 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.

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” as amended by Law 4734/2020, 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).

Finally, on an EU level, there is a Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937.

24. Are blockchain based assets such as cryptocurrency or NFTs considered “property” capable of recovery (and other remedies) if misappropriated?

There is no consensus in Greek legal theory about the legal nature of such assets, however Article 210 of the Greek Criminal Code on the unlawful acquisition of non-corporeal payment instruments provides that unlawfully obtaining non-corporeal payment instruments through unlawful access to information systems, illegal interference to systems or data and unlawful interception carries a sentence of imprisonment of at least three months and a fine.

25. Which body(ies), if any, is/are responsible for the regulation of search engines and marketplaces?

Greek Law 4753/2020 provides certain implementation measures for the adoption of Regulation (EU) 2019/1150 (“P2B”) on providers of online intermediation services or online search engines. It is noted that Regulation 2019/1150 applies when the above services are provided to business users and corporate website users. Pursuant to Art. 4 of Law 4753/2020, the Interdepartmental Unit for Market Surveillance (hereinafter “IUMS”), a body subject to the Ministry of Development and Investments, is responsible to supervise the compliance of providers of online intermediation services or online search engines with the provisions of Regulation (EU) 2019/1150, as well as to investigate any relevant case, acting upon a complaint or ex officio.

According to Art. 5, IUMC has the authority to gain access to any information, data and document coming from any source and to carry out dawn raids. If an infringement of Regulation 2019/1150 is detected, IUMS may issue a recommendation for compliance or impose an administrative fine of 1.500€ to 2.000.000€.

26. 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.

As mentioned above, 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.

27. Which body(ies), if any, is/are responsible for the regulation of social media?

The Ministry of Digital Governance has the most direct involvement and plays a key role in media sectors. However, major responsibilities in these sectors are undertaken by regulatory agencies which are independent administrative authorities, with full independence from network operators and service providers.

EETT is the competent regulatory authority responsible for defining and implementing any sector-specific regulation in the electronic communications sector. It is also the competent authority for the application of competition law in the electronic communications sector, and it is granted all the powers of the Competition Commission to this end and to the extent required for the sector of electronic communications. EETT is an authority independent of governmental control, but it is not established as such in the Greek Constitution.

Issues related to data protection and privacy of communications in social media are regulated by the HDPA and ADAE respectively, both established by the Greek Constitution.

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. In relation to liability for copyright infringement, it should be noted that intermediaries will be subject to the new liability regime as provided under Directive 2019/790/EU (new Copyright Directive), which is due to be transposed into the national legal order.

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). Platform providers also abide by the legislation set for the protection of systems and network security as well as for the protection of consumers. However, 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.

29. What are your top 3 predictions for

significant developments in technology law in the next 3 years?

The Digital Services Act, which entered into force on 16 November 2022, will be enforced through a pan-European supervisory architecture. According to the Regulation, Member States shall designate one or more competent authorities as responsible for the supervision of intermediary service providers and the enforcement of this Regulation (“competent authorities”). Member States shall designate one of the competent authorities as their digital services coordinator. The digital service coordinator shall be responsible for all matters relating to the supervision and enforcement of this Regulation in that Member State, unless the Member State concerned has delegated certain specific tasks or areas to other competent authorities. The digital services coordinator shall in any case be responsible for ensuring coordination at national level in relation to those issues and for contributing to the effective and consistent supervision and enforcement of this Regulation throughout the Union. Member States shall designate the digital service coordinators by 17 February 2024

It is therefore expected that a legislative act will be adopted empowering the competent authority responsible for the supervision of intermediary service providers and the enforcement of this Regulation.

The Digital Markets Act (DMA) establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called “gatekeeper”. This allows the DMA to remain well targeted to the problem that it aims to tackle as regards large, systemic online platforms. As of 12 October 2022, the DMA was published in the Official Journal and entered into force on 1 November 2022. Before 3 July 2023, companies have to provide the Commission with information about their number of users so that the Commission can designate “gatekeepers” before 6 September. Gatekeepers will then have until March 2024 to ensure that they follow the obligations of the DMA.

Finally, it must also be noted the use of generative AI and blockchain is expected to develop, which appears to be the trend globally.

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
Partner

nikolinakos@nllaw.gr



Dina Th. Kouvelou
Partner

kouvelou@nllaw.gr



Alexis N. Spyropoulos
Partner

spyropoulos@nllaw.gr

