Greece: Technology

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

For a full list of jurisdictional Q&As visit [here](#)
1. **What is the regulatory regime for technology?**

There is no specific regulatory regime for technology in Greece per se. The existing framework of several areas falling within the scope of the term (Internet of Things, AI and machine learning, IT service agreements, e-commerce and blockchain technology) is explained below, while the regulatory framework of the topics of telecommunications and data protection is referenced under the relevant questions that follow.

**Internet of Things Projects**

**IoT Devices**

With regard to the sale of IoT devices, in the absence of a tailor-made regime, the traditional national rules on the seller’s liability, guarantees and other relevant issues are applicable, while end-users as consumers are protected under the Consumer Protection Law 2251/1994. Also, of relevance are the legal provisions concerning the import and distribution of products (covering, for instance, the interference of a commercial agent or the conclusion of an exclusive distribution contract).

The main objective pursued under the IoT technology is to offer end-users enhanced control over differentiated devices by means of a connectivity network – ie, via the internet. As a result, the providers of the connectivity services (primarily, wireless networks) must comply with numerous rules provided by the EU and national law. In particular, electronic communications, networks and devices are covered by the European Electronic Communications Code (EECC), the transposition of which into Greek law is the purpose of a Ministry of Digital Governance draft law that was recently put to public consultation and which aims to replace in great part the existing legislation on electronic communications; the roam-like-at-home rules established in 2017 under the respective regulation; and the 2002 e-Privacy Directive which was implemented in Greece by Law 3471/2006, which introduced new rules for privacy in the digital age.

**Data Privacy and Cybersecurity**

Concerning the issue of data privacy, the principle of data protection by design and by default constitutes a crucial aspect. Moreover, the techniques promoted by the GDPR relevant to data anonymisation, pseudonymisation and encryption are thought to encourage the use of IoT in conjunction with the use of other, complementary tools such as data protection certifications and data protection impact assessments as provided by the law.

With respect to cybersecurity, the Ministerial Decision harmonising the Greek regulatory framework with Directive 2016/1148/EU (NIS Directive) was issued in October 2019, in execution of Law No 4577/2018 (implementing the NIS Directive into national law). According to the aforementioned instruments, new system security measures are required
from industries operating in e-commerce and information society services, providing also for a number of sanctions in case of non-compliance.

Product Liability

According to the European Commission, the provision of data through an IoT system shall be considered as a service. Therefore, the standard rules governing product safety and liability in cases of infringement shall not be applicable in this field. On the other hand, the rules governing the information service providers liability may be applicable in the case at issue, especially as regards electronic communications, protection of personal data and the confidentiality of information (covering, in addition, copyright infringement cases), as well as the traditional contract regime. At EU level, an amendment is currently being examined, aiming at the avoidance of fragmentation and at the fostering of interoperability.

Artificial Intelligence (AI) and Machine Learning (ML)

Data protection

Since AI systems analyse vast amounts of data in order to function and improve their performance, whenever personal data forms part of the large pools of data used in an AI system’s algorithmic decision-making process, this activity must be in compliance with Law 4624/2019 and the GDPR. Data subjects have the right to object to decision-making based solely on automated processing, including profiling and where such decision-making exists, meaningful information about the logic involved in the process, as well as its significance and its envisaged consequences ought to be provided to them.

Liability

The Greek Civil Code sets out five conditions that need to be fulfilled in order for tortious liability to be attributable to a party: (i) human behaviour, (ii) illegal action, (iii) fault, (iv) damage, (v) and causal link between the behaviour and the damage. It is apparent that where a system operating in the spectrum of autonomy causes damage, a number of these conditions are challenging, if not impossible, to substantiate.

In addition, all AI technologies in Greece ought to meet the essential health and safety requirements laid down in the EU safety legislation, as it has been transposed into Greek law, such as Directive (EC) 2006/42 on machinery (the safety legislation applicable to robots), Directive 2014/53/EU on radio equipment (which applies to all products that use the radio frequency spectrum, including embedded software), and Directive 2001/95/EC on general product safety (which aims to ensure that only safe consumer products are placed on the market).
The EU product liability regime is complementary to that of product safety. It was introduced by the Product Liability Directive (D 85/374/EEC) and was implemented by amendments of the Greek Consumer Protection Law No 2251/1994. The existing framework regulates all types of products and is also applicable to new digital technologies. The Greek Consumer Protection Law establishes a strict liability regime under which producers of defective products are held liable when such products cause damage to natural persons or their property, while the injured consumers are not required to prove the fault of the producer.

So far, the current legal framework of extra-contractual liability can be applied to damages caused by robots or AI.

Intellectual property

Greek Copyright Law (Law No 2121/1993) is human-centric, as it is traversed by the “principle of truth” according to which only a natural person shall be considered as the author of a work. Therefore, devices cannot be recognised as “authors”, and subsequently any work they produce cannot be qualified as a copyright-protected content. Computer-generated and AI works may only be protected if the prerequisite of “human intervention” is fulfilled (ie through the selection of the data to be entered into a machine or of the parameters determining the objective of the machine’s activity); inversely, works autonomously and exclusively produced by information technology systems, are not copyrightable. Accordingly, non-humans are excluded from the relevant rationae personae.

IT Service Agreements

Licensing Model

In Greece, IT service agreements are mainly ruled by the provisions set out in the Civil Code and Commercial Code, as those may be amended from time to time. Over and above the domestic legislation, Greece, as a member of the EU, follows closely the lines set out by EU legislation, whether this may be through the adoption of directives or the implementation of regulations.

Recipient of the IT service (B2B -B2C)

A significant factor that an organisation procuring IT solutions in Greece must take into consideration is whether this solution will be ultimately addressed to other businesses (B2B) or to consumers and individuals (B2C). In the first case, contracts between professionals are generally ruled by the parties’ freedom to agree on the content and the extent of their rights and obligations under the agreement. In the second case, however, and apart from the Greek applicable law, there is in place a rather elaborate body of consumer laws, primarily driven by EU initiatives and instruments, aiming for the protection of the weaker party, i.e. the
consumer, and prohibiting unfair terms, abusive clauses and clauses that have not been negotiated between the parties.

E-commerce

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (Directive on electronic commerce) relates to certain legal aspects of information society services, in particular the conduct of electronic commerce in the Internal Market. The Directive regulates an important part of the services provided online. The purpose of the Directive is to remove obstacles to cross-border online services in the EU and to provide legal certainty to business and consumers. The Directive sets out basic requirements on mandatory consumer information, determines certain steps to follow when establishing contracts online, as well as certain rules on commercial communications. Presidential Decree 131/2003 constitutes the –almost verbatim- adaptation of the above Directive into Greek legislation.

Some of the issues regulated in the Presidential Decree, are, among others, the following: the prohibition of any restriction on the free circulation of the services within the European market, due to national regulations, the obligation of information society service providers to provide their recipients and competent authorities with easy, direct and continuous access to basic information concerning their activities (name, geographical address, e-mail address, registration number register, etc.), the freedom of assumption and exercise of activity, the responsibility of service intermediaries, the extrajudicial settlement of disputes in cases of disagreement between a provider and a recipient of an information society service and the sanctions in case of violation of provisions of the Presidential Decree.

Telecommunications and Media sectors

The telecommunications and media sectors have developed quite separately in Greece. Telecommunications developed following the decision of the government in 1992 to proceed with the establishment of a competitive market for mobile telecommunications. That year, two licences for mobile networks were granted to two subsidiaries of foreign operators, Vodafone and Telecom Italia, which launched their services in 1993. The incumbent Greek operator, OTE, was then totally excluded from the tender. A licence for mobile networks was granted to OTE in 1995, which launched its services in 1998. At the same time, the government started the privatisation of the incumbent, a procedure that ended in 2008, 14 years later.

The key law for liberalisation of communications was enacted in 2000. The EU Framework on electronic communications networks and services was initially transposed into national legislation with a significant delay in 2006. The revised Electronic Communications Framework was transposed into national legislation through Law 4070/2012.

To prepare Europe’s digital future, a new European Electronic Communications Code
(Directive 2018/1972), was enacted by the European Commission. The Code which entered into force on 21 December 2018 modernises the current EU telecoms rules, inter alia by expanding the definition of “electronic communications service” to include any interpersonal communications services provided over the internet, including VoIP services, messaging apps and email services that do not use telephone numbers. It must be transposed to national legislation by the end of December 2020.

In the media sector, the liberalisation of the market in Greece and the transition from the state-controlled radio and television to the regime of radio and television operated by privately owned companies has been the result of a de facto development in the market that occurred before the appropriate legal framework. An immediate effect of this is that the market developed in a totally unregulated way. Few of the free-to-air television stations still operate with a temporary licence, and the majority of the free-to-air radio and television stations operate legally under certain temporary provisions, in a very muddy legal environment. In October 2015, Law No. 4339/2015 entered into force, introducing the provisions on the authorisation of digital terrestrial television broadcasting content providers. As issues to be evaluated it specifies the extent of the investment, financial reliability, experience and existing position in the market in order to avoid concentration, as well as the kind of programmes that will be transmitted.

According to the applicable legislation (Law No. 3592/2007), controlling more than one licence holder in the television or radio sector is prohibited. Everyone is allowed to participate in more than one licence holder in television or radio to the extent that he or she does not control more than one (a person has control over a licence holder if it can substantially influence the decision-making process or it has the power to appoint at least one member of the board of directors or an administrator in another operator). Foreign investors have the opportunity to participate in broadcasting activities in Greece, subject to the generally applicable restrictions. The concentration of media is prohibited. Concentration in media is considered to exist if an undertaking acquires a dominant position that is defined in Law No. 3592/2007, which provides also for complementary application of Competition Law No. 3959/2011. The Competition Commission is the competent authority to consider competition law issues in the media sector, including issues of concentration. Market share is calculated on the basis of income from advertising and exploitation of programmes or provision of other similar services during the previous year.

Nevertheless, Law No. 4339/2015 (as amended, by L N.4487/2017) sets the following restrictions on shareholders holding more than 1% board members and legal representatives of entities that participate in tenders for digital terrestrial TV content providers: non-convictions by irrevocable court decision for specific crimes; and non-participation in any manner in companies conducting research in the radio or TV market and in advertising companies, as well as in companies conducting telemarketing. The law also refers to the general prohibition from participating in companies that execute public contracts and require
licence applicants to submit evidence proving how the applicant acquired the financial means used or intended to be used for the operation of the content provider.

Finally, except for online gambling, e-commerce and the data protection legislation, there is no other internet-specific legislation. General provisions of law are applicable, along with certain guidelines or ad hoc decisions of the Greek DPA that are used as guidelines for the interpretation of such general provisions on specific electronic communications services.

The general EU framework provisions on radio and television content applies to Greece, meaning that the programme must adhere to the general principles of the Constitution and there are further obligations concerning minors, rating of the programmes, advertising, pluralism and non-discrimination, etc. In fact, the Directives for Television without Frontiers are implemented in Greek law by Presidential Decree No. 109/2010, and apply to providers that are under the jurisdiction of Greece as defined therein. The EU’s current Audiovisual Media Services Directive 2010/13/EU (AMS Directive), as transposed in Greece by PD. 109/2010 governs EU-wide coordination of national legislation on all audiovisual media, both traditional TV broadcasts and on-demand services. The aforementioned framework has already been amended by Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 (Audiovisual Media Services Directive (AVMSD)) in view of changing market realities. The new directive that is in force should be transposed to all Member States, including Greece, by September 19th, 2020.

2. Are communications networks or services regulated?

Electronic communications networks and services providers in Greece are required to obtain a General Authorisation from the EETT. The main law that governs the provision of electronic communications is Law 4070/2012. Secondary regulation is issued by the EETT. The law defines the responsibilities of the competent Ministries (currently the Ministry of Digital Policy, Telecommunications and Information), which are mainly related to defining the national strategy in the sector and the responsibilities of the EETT, which is the key entity responsible for the design, implementation and enforcement of electronic communications regulation. The EETT has the power to issue regulatory decisions defining regulatory obligations or authorised operators, authorise operators, provide Rights of Use of numbers and spectrum, control the market and monitor compliance of authorised operators, enforce relevant obligations, impose sanctions and issue decisions on dispute resolution between authorised operators.

Currently, the only retail market that is still subject to ex-ante regulation is the market for retail leased lines with capacity up to 2Mbps, soon to be deregulated according to recent notification of EETT.

The incumbent OTE has also been designated an SMP operator in the following wholesale markets: fixed origination, termination to individual fixed networks, local loop unbundling (LLU), wholesale broadband access and terminating segments of leased lines.
All fixed network operators have been designated as having SMP in the markets for termination to individual fixed networks and all (three) mobile network operators have been designated as having SMP in the markets for termination to individual mobile networks.

The ex-ante regulatory obligations for transparency, price controls, cost accounting separation, access to and use of specific network facilities and non-discrimination have been imposed on SMP operators in the above markets (with a few exceptions in specific markets).

The EETT’s decisions on (deregulation of) the retail and (regulation of) wholesale access markets were issued on December 2016, whereas in June 2017 EETT issued a Decision on 4th Round of Analysis of wholesale market definition for termination of calls to Individual Mobile Networks, designation of operators with Significant Power and Regulatory Obligations thereof. Moreover, on December 2019, the updated Bottom up pure LRIC Techno-Economic Model for the aforementioned markets, as implemented by EETT Decision 815/002/22.06.2017, was adopted.

Additional issues regarding telecoms regulation (fixed infrastructure)

In practice there are no cable networks in Greece.

Access to the local loop or LLU is regulated. OTE is designated as an SMP operator and specific obligations are imposed upon OTE, namely access to the local loops and associated facilities (eg, collocation), transparency, non-discrimination, price control, cost accounting obligation and accounting separation.

The market analysis of the local access market, which designated OTE as an SMP operator, imposed an obligation to provide access for the deployment of NGA Networks based on VDSL Vectoring infrastructure and services by other operators (or based on other NGA technology) through a process managed by the EETT for the assignment of local sites to operators.

In Q2 2018, the EETT performed a public consultation on the third round of regulation of leased lines in the Greek Territory (market 4 of Commission Recommendation 2014/710/EU ‘Wholesale high-quality access provided at a fixed location’). The draft measure was finally notified following further national consultations in November 2019 and EETT’s final decision is expected shortly. According to the draft measure that was notified, the currently regulated retail leased lines market with capacity up to 2Mbps is proposed to be deregulated.

Additional issues regarding telecoms regulation (mobile)

With the exception of free spectrum bands, an individual right to use frequencies is required
for all wireless services and is granted by the competent authorities upon a relevant request. Only if the spectrum available is not enough to cater for existing demand from existing or new competitors will a limitation on the number of individual licences be effected. This will be the result of a public consultation that the EETT must prepare following a ministerial decision to that effect. If, as a result of that consultation, the number of individual rights has to be limited, the EETT must decide how this limited number of individual rights will be granted. Any kind of tender can be held in accordance with the principles of transparency, etc, that are set by Greek law in accordance with EU directives.

The aforementioned rules are also applicable in the assignment of unused radio spectrum. No change of permitted use is allowed.

The law allows for spectrum trading under specific conditions. To transfer, lease or make any change in the control of the rights holder, an application must be filed to the EETT, which assesses the relevant application and decides based on specific criteria defined by law.

A recent development is the new antenna construction licensing legal framework established by Law 4635/2019, according to which EETT’s issuance of antenna construction license is carried out through the Antenna Electronic Application System (SILYA), as in the previous legislative framework, but without requirement for planning permission to be granted. The planning approval is issued following EETT’s antenna construction permit, through the electronic system e-Licensing already used for buildings and intended to interoperate with SILYA, automatically at the request of an authorized engineer and followed by a building autopsy. The new law greatly simplifies the process of modifying antenna constructions, whereas recent joint ministerial decision exempts from the licensing process Low Electromagnetic Environmental Nuisance Antenna (ESCC) Facilities resulting in a significant number of antennas, mainly within the urban centers, now requiring a simple declaration procedure also implemented through SILYA.

A general obligation to provide access to MVNO operators is imposed on mobile network operators (MNOs) through a relevant provision included in the rights of use of frequencies. However, this obligation does not specify the pricing or non-pricing terms of access provision. In Q4 of 2018, the EETT issued a decision, following a dispute resolution petition by fixed operator Forthnet requesting MVNO access by mobile operators Vodafone and Cosmote, ruling on both the obligation but also the pricing terms thereof.

The provisions of the EU Roaming Regulation have been fully implemented as of 15 June 2017.

Additional issues regarding internet services (including voice over the internet)

With the exception of radio and TV legislation, online gambling legislation, the provisions of
the Greek presidential decree implementing e-commerce and the data protection legislation, which includes specific provisions on internet services, there is no specific national regulation. The general provisions of law and relevant EU framework, recommendations, opinions and self-regulation instruments also affect the provision of internet services. In June 2019 the ECJ made a preliminary ruling in Case C-142/18, Skype Communications Sàrl, on whether VoIP calling apps fit within the definition of an ECS under EU law. In its decision, the ECJ found that SkypeOut was a regulated communications service because Skype assumes responsibility for transmitting calls to telephone numbers: it charges customers for making calls and enters into agreements with telecom service providers to terminate calls. Telephone calling apps, such as Skype, Viber and Google Hangouts, are therefore subject to European telecom regulation and may now be required to comply with EU obligations that apply to traditional telephone services, such as registration, privacy, consumer protection and law enforcement access to user communications. Nevertheless, in the EU’s new telecom code (Directive 2018/1972), the definition of “electronic communications service” has been expanded to include any interpersonal communications services provided over the internet, including VoIP services, messaging apps and email services that do not use telephone numbers.

There are no specific limits on an internet service provider’s freedom to control or prioritise the type or source of data that it delivers. The EU legislation on Open Internet Access, namely Regulation 2015/2120 is fully implemented. The Regulation prohibits operators from blocking, slowing down or prioritising traffic. Traffic management measures are authorised if they are reasonable, meaning that the measures shall be transparent, non-discriminatory and proportionate and based on objectively technical differences of traffic (Article 3(3)). Such measures cannot monitor specific content and cannot be maintained longer than necessary. The EETT has issued Decision on National Open Regulation Issues – implementing of Regulation (EU) 2015/2120 on 2018.

Additional issues regarding access and/or securing or enforcing rights to public and private land to install telecommunications infrastructure

Law 4463/2017 implemented EU cost reduction Directive 2014/61/EU. Until the operation of the Information System, which will support the one-stop procedure for the granting of the rights of way, the procedure of article 11 of Annex X of Law 4070/2012, as amended by Law 4463/2017, applies.

In July 2018 the EETT conducted a public consultation on the modification of EETT regulation (528/075/2009) for the determination of fees for rights of way, rights of use of rights of ways and the amount of guarantees of good performance of rights of ways operations for Greece with the aim of simplifying the relevant procedures. Additionally, the EETT issued in August 2018 its new Regulation on Collocation and common use of facilities.
3. **If so, what activities are covered and what licences or authorisations are required?**

Any natural or legal person can apply to acquire a general authorisation to provide electronic communications services or networks, which is processed at once. To obtain a general authorisation, the requesting entity needs to submit a Registration Declaration to the EETT, using the standard form provided by the EETT, along with the relevant supporting documents. This Registration Declaration must be submitted solely through the Online Application System for Electronic Communications Services Providers. When submitting the application, the person concerned must electronically send to the EETT all required supporting documents attached to the Statement. To access the Online Application System for Electronic Communication Providers, the applicant must submit an ‘Administrator’s Statement’, according to the provisions of the EETT decision 586/006/2010 as in force. The person providing this Statement may perform the specific electronic communications activity described in the Registration Declaration, immediately upon filing a complete Registration Declaration. For the Declaration to be deemed complete, relevant administrative fees must be paid. The requesting operator is included in the Registry of Authorised Operators and may obtain a relevant certificate by the EETT upon request within seven days of receipt of such request.

Any natural or legal person can apply for rights of use, which will be processed within three weeks from the application for a right of use of numbers or six weeks for numbers with significant economic importance; applications for rights of use of frequencies will be processed within six weeks if there is no limitation of the number thereof or up to six months from the application if such a limitation is imposed.

With the exception of free spectrum bands, for all wireless services an individual right to use frequencies is required and is granted by the competent authorities upon a relevant request. Only if the spectrum available is not enough to cater for existing demand from existing or new competitors will a limitation on the number of individual licences be effected. This will be the result of a public consultation that the EETT must prepare following a ministerial decision to that effect. If, as a result of that consultation, the number of individual rights has to be limited, the EETT must decide how this limited number of individual rights will be granted. Any kind of tender can be held in accordance with the principles of transparency, etc, that are set by Greek law in accordance with EU directives. In practice, in cases of limited number of rights of use of frequencies, the EETT usually awards them through auctions.

As far as licences for antennas and base stations are concerned, the relevant framework has been reviewed to deal with the bureaucracy and the incomplete framework that led to severe delays in the issuance of licences. The main target of the new process is to accelerate the process by establishing a one-stop shop for applications.

The duration of general authorisations is indefinite. The duration of rights of use of frequencies is defined in the relevant EETT Decisions, awarding the rights of use.
Fees imposed on operators with a general authorisation are paid on an annual basis and correspond to the costs of management, monitoring and compliance with the General Authorisation Regime and to the rights to use radio frequencies or numbers it derives from a formula included in the EETT Decision on General Authorisations. The main factors taken into account for the calculation of the fees are the total turnover from electronic communications networks or services minus the wholesale interconnection and roaming costs paid to other operators. The fees are equal to a percentage that varies depending on the net revenues, calculated as described above.

Fees for use of numbers are defined for each series of numbers in a decision of the EETT on allocation of numbering resources.

Fees for rights of use of spectrum are imposed by decision of the EETT and are usually paid on an annual basis, except for rights of use of frequencies that are granted through competitive procedures, such as auctions, in which case the EETT only defines the minimum bid, and the final fees result from the auction procedure.

All the telecoms operators are obliged to have registered themselves under the general authorisation regime and be granted individual rights to use frequencies or numbers and the appropriate licences for every antenna they use. Apart from that there is no other substantial difference in relation to the regulation of fixed, mobile and satellite services.

There is no exclusivity granted to any operator in any sector. However, there is a limited number of licences with regard to mobile and fixed wireless access and digital television networks. According to the relevant legislation, the EETT proceeds to a public consultation that leads to a proposal by the EETT to the Minister of Transport concerning the way in which licences will be granted, the cost, the duration of the entitlement, etc.

4. **Is there any specific regulator for the provisions of communications-related services?**

The intendent regulatory authority responsible for defining and implementing any sector-specific regulation in the electronic communications sector is the EETT. The EETT is also responsible for the application of competition law in the electronic communications sector. Issues related to data protection and privacy of communications are regulated by the DPA and the ADAE respectively, both established by the Greek Constitution. The Competition Commission is also an independent authority, but as with the EETT, it is not established by the Greek Constitution.

The EETT is also (under Article 9 of Law 4463/2017 on the transposition of the cost reduction Directive 2014/61/EU), the National Dispute Settling Body for any dispute regarding:

- Access to existing physical infrastructure.
· Transparency of existing physical infrastructure.

· Negotiation of an agreement to coordinate civil work.

· Access to information regarding civil coordination.

· Access to in-building physical infrastructure or to the building access point.

· Refusal of rights of way.

5. Are they independent of the government control?

EETT is an independent authority of the government control but it is not established as such by the Greek Constitution.

6. Are platform providers (social media, content sharing, information search engines) regulated?

Although they are not specifically regulated, they are bound to abide by all legislation set in protection of personal data, systems and network security as well as in protection of the consumers using the said services. However, if the platform providers offer services to regulated entities (such as in financial services, or gaming etc) then they may also be subject to monitoring and supervision by the competent supervision authorities of the said industries.

The conduct of platform providers, otherwise of any natural or legal person providing information society services (service providers)1 is primarily regulated under the Presidential Decree No. 131/2003 that introduced into the national legal order the E – Commerce Directive. Under this legal instrument, the information society services provided by a service provider established in Greece or in another Member – State shall comply with the national provisions applicable within the coordinated field without restricting though the freedom to provide information society services from another Member State.2 In addition, Article 3 provides that the taking up and pursuit of the activity of an information society service provider is free, meaning that it is not subject to any prior authorisation or any other requirement having equivalent effect with the exception of authorization schemes which are not specifically and exclusively targeted at information society services or those related to telecommunication services in accordance with the Law No. 2867/2000 (Official Government Gazette A’ 273) and the Presidential Decree No. 157/1999 (Α’ 153), as applicable. Moreover, the Decree provides, in accordance with Union law, for a number of tailor – made and specific obligations for service providers as related to the provision of general information -on a de minimis basis- to the recipients of the service and competent authorities (Article 4), of additional information when commercial communications are implicated (Article 5), as well as to their duty to consult on a regular basis and respect the opt-out registers in which natural persons not wishing to receive unsolicited commercial communications by electronic mail can
register themselves (Article 6).

Furthermore, it had been stated that the issue of service providers’ liability may not be divorced on the grounds of the type of content provided, however specific rules may be applicable at each case at issue. Although the E-Commerce Directive provided for an “immunity regime” in the case of unlawful or harmful content, special subsequent regimes had increased their obligations and enhanced their respective liability. For example, in the case where infringing -to-copyright-content is provided, the relevant theory dictates that providers’ -operating and being accordingly identified as intermediaries- liability shall be distinguished to the primary and the secondary one; in the first case, the provider is liable if performing himself an infringing act. On the other hand, secondary liability is founded in the case where the intermediary enables or facilitates a restricted act.

In this regard, it is noteworthy that the conduct of internet service providers with regard to copyright and related - rights infringements on the Internet may also addressed to the Greek Committee for the

Notification of Copyright and Related Rights Infringement on the Internet (EDPPI)3 as established under the Law No. 4481/2017 under which Article 66E was added to the Greek Copyright Act, Law No. 2121/1993, as it had been recently amended by Article 25, Law No. 4708/2020. Provided that both the typical and substantial prerequisites set - out by the law are fulfilled, the Committee may at first notify internet service providers to remove -within a specific time - the infringing content and subsequently -in the case of non-compliance- order the blocking of access to such a content or undertake any other measure deemed as appropriate by the Committee, aiming at the cease, deterrence of recurrence and/or prevention of the infringement.

With regard to copyright infringements, platforms providers may be subject to administrative, civil and criminal sanctions as provided under Chapter 11 of Law No. 2121/1993.

Focusing on information search engines and online content-sharing service providers in general, it should be stated that they will be subject to the new liability regime as provided under Article of the Directive 2019/790/EU4, the transposition period of which into the national legal order expires (as in all Member States) at June 7, 2021.

Furthermore, providers are subject to the rules governing the confidentiality of communications being such as respectively liable for the public telecommunications network, routers and servers via which access to the Internet, as well as to various services, is provided (inspected by the Hellenic Data Protection Authority), as well as to the obligations deriving from the Personal Data legislation, meaning the Law No. 4624/2019 under which the Regulation (EU) 2016/679 was transposed into the Greek legal system.
In addition, the Hellenic Telecommunications and Post Commission (EETT) requires for General Authorizations for the engagement in all kinds of electronic communication activities pertaining to the provision of electronic communication networks and/or services. More precisely, a Registration Declaration for Engaging in Electronic Communication Activities under a General Authorization Regime is (exclusively) required by persons providing public communication networks or publicly available electronic communication services, as well as by persons operating special radio networks. In addition, a General Authorization is required for the provision of electronic communication services by third parties which, notwithstanding the fact that they do not have their electronic communication infrastructure, they provide electronic communication services on the basis of the infrastructure of other counterparties (providing likewise for electronic communication networks and/or services).

Platforms providers may be also subject to the sanctions provided under other legal instruments, such as the law governing the fighting of certain forms and manifestations of racism and xenophobia by the means of penal law -Law No. 4825/2014 under which once notified, providers shall promptly remove such a content otherwise they are subject to the punitive sanctions provided therein.

Currently, a Public Consultation on the Draft Law of the Electronic Communication Code of the Ministry of Digital Governance, which is a transposition of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018, has been completed. As far as Over-The-Top services are concerned, the definition of “electronic communications services” is expanded in such a way that consumer protection rules will also apply to services provided via them, as well as to services provided in return for provision of data, in return for financial payment, in return for display of advertising messages or in cases where the service provider financially exploits the collected data. However, since this is the draft law, as mentioned above, the final text might include differentiations.

Under a tax perspective, Article 29 of Law 4646/2019 establishes new obligations for digital platform administrators, amending Article 15 and introducing Article 54D to the Greek Tax Procedure Code (Law 4174/2013). In particular, Article 15 establishes the obligation for any digital platform administrator active on the sharing economy field, to provide information to the Independent Authority for Public Revenue (ADAE), when required to do so by a tax authority, regarding persons using its platform as business users/sellers, for which tax obligations under Greek territory arise. The added Article 54D refers to the sanctions, in case of non-compliance to the above obligation, such as blocking of access to the Platform or imposition of a fine up to €100,000.

The Regulation (EU) 2019/1150 (EU) “on promoting fairness and transparency for business users of online intermediation services”, which is applicable as from 12 July 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.

Finally, the Hellenic Competition Commission, taking into account the increasing important role of e-commerce in Greek consumers’ habits as a reliable channel for the distribution of goods and services, as well as the ability of modern technology tools to facilitate restrictions of competition in the digital environment, initiated a sector inquiry into e-commerce. The sector inquiry primarily focuses on the markets of clothing and footwear, electronic and electric devices, books, mediation services to provide travel tickets, mediation services for the provision of tickets for events, mediation services to provide catering services, accommodation and rental – AIRBNB, e-pharmacies (with emphasis on dietary supplements and parapharmaceuticals), without prejudice to the ability of the Hellenic Competition Commission to further specify and / or limit and / or expand the scope of the inquiry depending on its case-by-case findings, as it evolves. The final report is expected to be published on 30.04.2021.

7. **If so, does the reach of the regulator extend outside your jurisdiction?**

In principle, there is no such an extension outside Greek jurisdiction with the exception of specific rules on special regimes; this is the case, for instance, under copyright law where tailor - made provisions are provided with regard to applicable law in various cases.6 In the case where foreign elements are implicated, the rules of private international law are applicable. When it comes to consumer protection and personal data protection, if the services are offered to residents of our jurisdiction, then the supervision authorities’ reach may extend to service providers outside our jurisdiction.

8. **Does a telecoms operator need to be domiciled in the country?**

No, the purpose of European rules is to complete the internal market and the abolition of all obstacles to its completion, the corollaries of which are freedom of establishment and freedom to provide services.

Indeed, Directive 2002/77 of 16 September 2002 lays down the principle of the abolition of exclusive and special rights for the establishment and/or operation of electronic communications networks and the provision of electronic communications services.
Article 3 of the new Directive 2018/1972 establishing the European Code for Electronic Communications states that « the national regulatory authority, (...), the Member States shall pursue each of the following general objectives : (...) contribute to the development of the internal market by removing remaining obstacles to, and facilitating convergent conditions for, investment in, and the provision of, electronic communications networks, electronic communications services, associated facilities and associated services, throughout the Union ».

9. Are there any restrictions on foreign ownership of telecoms operators?

Electronic communications sector is open to foreign investment, subject to generally applicable restrictions. Besides, one of the objectives set out by Directive 2018/1972 establishing the European Code for Electronic Communications is to promote efficient investment and innovation in new and enhanced infrastructures, including by ensuring that any access obligation takes appropriate account of the risk incurred by the investing undertakings and by permitting various cooperative arrangements between investors and parties seeking access to diversify the risk of investment, while ensuring that competition in the market and the principle of non-discrimination are preserved.

10. Are there any regulations covering interconnection between operators?

The EETT’s regulation 732/4/11-9-2014 sets the framework for access and interconnection between operators.

In cases of interconnection disputes, the EETT can intervene through the standard dispute resolution procedure, provided for by the Law on Electronic Communications.

If so, are these different for operators with market power?

The interconnection market is regulated. Concerning the fixed market, OTE is designated as having an SMP in the fixed origination and termination markets. All other fixed network operators have been designated as having an SMP in the markets for termination to their individual networks. Interconnection rates in these markets are regulated on the basis of cost-orientation. Additional obligations for transparency, price control, cost accounting separation, access to and use of specific network facilities and non-discrimination have been imposed.

In the mobile market, all MNOs have been found to hold an SMP in the markets for termination to their individual networks. Mobile termination rates are regulated on the basis of the cost-orientation principle on a pure LRIC model basis and further obligations on access, transparency, non-discrimination, and accounting separation have been imposed on SMP operators.
The fixed incumbent OTE and the three (3) MNOs (Cosmote, Vodafone, Wind) are required to publish their standard interconnection contracts and prices.

11. **What are the principal consumer protection regulations that apply specifically to telecoms services?**

Customer terms and conditions for the provision of electronic communications networks and services are subject both to general consumer protection legislation and to sector-specific regulation and particularly to the General Authorisation Regulation of EETT, which defines the minimum content of such terms and conditions.

As of January 2019, the EETT’s General Authorisation Regulation introduces obligations for:

- automatic service interruption to avoid overcharging;
- maximum termination rate for early termination of a fixed-term contract; and
- seamless access of customers to conventional terms and pricelists.

12. **What legal protections are offered in relation to the creators of computer software?**

Under the Greek Copyright Act, namely Law No. 2121/1993 (Official Government Gazette A’ 25/1993), computer programs, as well as their preparatory design material, shall be deemed as literary works within the meaning of the law, meaning that they are copyright protected insofar as they constitute original intellectual creations. Accordingly, the protection applicable under national copyright law covers the expression (emphasis added) of a computer program in any form. However, it is explicitly stated that the ideas and principles which underlie any element of a computer program, including those underlying its interfaces, are not copyrightable. With regard to the identification of the notion of originality -as the sole prerequisite for copyright protection under the CJEU case - law-, the national legislator had adopted the relevant interpretation providing that a computer program shall be protected if it is original in the sense that it constitutes the author’s own intellectual creation.

Accordingly, creators of computer software are vested with the absolute and exclusive rights provided under Articles 3 and 4 of the Greek Copyright Act, being further analyzed to the bundle of rights deriving from the author’s economic and moral right respectively over his/her work. More precisely, the economic rights shall confer upon authors notably the right to authorize or prohibit: a) the fixation and direct or indirect, temporary or permanent reproduction of their works by any means and in any form, either in whole or in part; b) the translation of their works; c) the arrangement, adaptation or any other alteration of their works; d) the distribution to the public in any form by sale or otherwise of either the original or copies of their works. It shall be noted that the law provides that the distribution right shall be exhausted within the Union only in the case where the first sale or any other transfer
of ownership within the Union of either the original or copies is made by the rightholder or with his/her consent. Moreover, author’s economic right covers also: e) the rental or public lending of the original or copies of works; f) the public performance; g) the broadcasting or rebroadcasting of works to the public by radio, television, wireless means or by cable or any kind of wire or any other means in parallel to the surface of earth or by satellite; h) the communication to the public by wire or wireless or any other means, entailing the making available to the public of works in such a way that the public may access these works from a place and at a time individually chosen by them and; i) the import of copies of the works produced abroad without the creator’s consent or the import of copies from a country outside the European Union, when the right over such an import in Greece had been retained by the author through contract.

In parallel, authors -of any type of works, profoundly including software- are vested with moral rights under the scope of safeguarding the personal bond that connects them with their works. Respectively, authors have notably the right: a) to decide on the time, place and manner in which a work shall be made accessible to the public (right of publication); b) to demand that his/her status as the author of the work will be acknowledged and, in particular and to the extent possible that his/her name will be indicated on the copies of the work and noted whenever his work is used publicly. Under this right, an author may on the contrary decide that his/her work will be presented anonymously or under a pseudonym. In addition, copyright holders have the right to: c) prohibit any distortion, mutilation or other modification of his/her work and any offence caused by the circumstances in which a work is publicly presented; d) to have access to his/her work, even in the case where the economic right over work or the physical embodiment belongs to another person and; e) in the cases of literary or scientific works, the author has also the right to rescind a contract transferring the economic right or a contract concerning its exploitation or a relevant license insofar as this is necessary for the protection of his/her personality on the grounds of a change either in his beliefs or in circumstances. This rights though is aligned with the author’s obligation to the payment of material damages to his/her counterparty.

Moreover, Greek law provides for further tailor-made provisions with regard to computer programs (and databases - meaning the sui generis right granted to the maker of a database). Focusing on software, the national legislator had determined that the economic right over a computer program that is created by an employee in the execution of his/her 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). In addition, Article 41 provides that the first sale within the Union of a copy of a program either by the author him/herself or with his/her consent, shall exhaust the distribution right of that copy within the Union exempt from the right to control the further rental of the program or of a copy thereof.

Article 42 provides for a number of limitations to the rights conferred to authors of protected computer programs. It shall be noted that these special limitations are exclusively applicable to this type of works; consequently, the cumulative application of the exceptions and
limitations provided under Chapter 4 of the Greek Copyright Act, shall be excluded. With regard to the wording of this provision, paragraph 1 provides that in the absence of an agreement to the contrary, the reproduction, translation, adaptation, arrangement or any other alteration of a computer program shall not require the author’s (prior) authorization by the author or necessitate the payment of a fee, where the aforementioned acts are necessary for the use of the program by the person who had legitimately acquired the right to use such a program. The correction of errors is also explicitly covered under the term “use”, while the law provides that the latter shall always take place in compliance with the program’s “intended purpose”. On the contrary, reproduction that is necessary for the purposes of loading, displaying, running or storage of a computer program shall be subject to the author’s authorization (paragraph 2). The next paragraph refers to the making of a backup copy by a person having the right to use the computer program thus dictating that this act may not be prevented by contract insofar as it is necessary for the use of the program. In addition, the author’s consent is not required neither the payment of a fee (paragraph 3). The same applies with regard to the right of a person who is legitimately able to use a copy of a computer program to observe, study or test its functioning in order to determine the ideas and principles that underlie any of its element. However the scope of application of this limitation had been determined as to entail the aforementioned uses insofar as they take place during an act that falls within the concept of the program’s legitimate use. Lastly, paragraph 4 clearly states that any agreement to the contrary shall be prohibited excluding as such any contractual deviation. According to the next paragraph of this provision, the aforementioned circumstances (i.e. the circumstances provided under paragraphs (3) and (4)) consist of the sole reproducti

implementation into the Greek legal order of the Directive 2017/1564 (EU)12, an addendum to this provision had been introduced13 dictating that the limitations to the economic right provided for the purpose of permitting certain uses for the benefit of print – disabled persons and persons with other disabilities14, shall be also applicable to the rights of the holder of rights over a computer program.

Concluding, it should be noted that the national legislator had also regulated the issue of decompilation providing for a tailor – made provision15 according to which the person having the right to use a copy of a computer program shall be entitled to carry out reproduction, translation, adaptation, arrangement or any other alteration, as well as reproduction that is necessary for the purposes of loading, displaying, running or storage of a computer program16 with no need to obtain the author’s permission and without the payment of a fee. This exception though applies to the case where such acts are indispensable in order to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs insofar as the following prerequisites are cumulatively fulfilled; i) that this information has not previously been easily and readily available to the legitimate user and ii) that these acts are confined to the parts of the original program which are necessary to achieve the aforementioned interoperability17.

However, it is clearly provided that the application of the first paragraph of this provision –as
stated above- shall not permit this information –meaning the information received within the scope of its application: a) to be used for objectives other than to achieve the interoperability of the independently created computer program; b) to be announced to other persons except when necessary for the said interoperability or c) to be used for the development, production or marketing of a computer program, the expression of which is substantially similar to the initial program or for any other act that infringes the author’s copyright.

Last, paragraph 3 of Article 43 makes an explicit reference to the three - step test thus concerning (as in all cases) an exception and limitation to the author’s economic right. As a result, it is (also in this case) explicitly provided that the provisions established under Article 43 shall not be interpreted in such a way as to allow its application to be used in a manner that would conflict with the normal exploitation of the computer program or would unreasonably prejudice the author’s legitimate interests.

13. Do you recognise specific intellectual property rights in respect of data/databases?

Databases fall explicitly within copyright’s rationae materiae under the Greek Copyright Act thus being identified as deriving from the original selection or arrangement of their contents; on these grounds, databases constitute the author’s intellectual creation and shall be profoundly protected as such by copyright. However, the law provides that copyright protection shall not extend to the contents of a database and shall not prejudice any right subsisting in those contents per se. According to the relevant definition, a “database” is a collection of independent works, data or other material arranged in a systematic or methodical way that is also individually accessible by electronic or other means.

Consequently, the author of a database is the (initial –as in all cases following the relevant presumption (Article 6(1), Law No. 2121/1993) holder of copyright over this type of work on the grounds of the original selection or arrangement of its contents.

Focusing on the contents of a database, national law provides for the sui generis right of the maker of a database. More precisely, the maker of a database has the right to prevent extraction and/or re-utilization of the whole or of a substantial part of the content of a database, being evaluated qualitatively and/or quantitatively, provided that the acquisition, control or presentation of such a content demonstrate substantial qualitative or quantitative investment. The notion of the “maker of a database” had been determined as either the natural or legal person who takes the initiative and bears the risk of investment with the exception of the contractor of a database who shall not be considered as “maker” within the meaning of law.

Moreover, a number of critical definitions are provided under paragraph 2 of Article 45A of the Greek Copyright Act, being analyzed –for the purposes of this provision- as follows: a) “extraction” shall mean the permanent or temporary transfer of all or of a substantial part of the content of a database to another medium by any means or in any form, and b) “re-utilization” shall mean any form of making
available to the public all or a substantial part of a database’s content by the means of distributing copies, by renting, by transmitting either online or through other forms. With regard to exhaustion, the law provides that the first sale of a copy of a database within the Union by the rightholder or with his consent shall exhaust the right to control the resale of that copy within the Union. In addition, it is clearly stated that public lending does not constitute an act of extraction or re-utilization.

It should be further stated that the sui generis right of the maker of a database applies irrespective of whether that database or the content thereof are protected under copyright law or under other provisions. The protection afforded to the maker of a database does not prejudice other potential rights over its content. With regard to the transfer of this right, the law provides that it may take place either with or without any consideration or that its exploitation may be assigned by the means of either a license or a contract.

The three-step test is also in this case applicable since paragraph 4 provides that in the case where the normal exploitation of a database or the legitimate rights of the maker of a database may be prejudiced through the repeated and systematic extraction and/or re-utilization of insubstantial parts of the content of the database, such acts shall not be permitted.

Moreover, it is provided that the maker of a database that had been made available to the public by any means cannot prevent the legitimate user of the database from extracting and/or re-using insubstantial parts of its content, being evaluated (i.e. the parts) either qualitatively or quantitatively, irrespective of the objective pursued at each case at issue. In the case where that user is entitled to extract and/or re-utilize only a part of the database, this provision is applicable only to that part. On the other side, the law provides for certain acts that (even) the legitimate user of a database that had been made available to the public shall not undertake; namely, to perform acts that conflict with the normal exploitation of that database or that unjustifiably prejudice the legitimate interests of its maker, and to cause damage to the holders of copyright or of related rights over the works or performances integrated into that database. We should also underline that any agreements contrary to this provision (paragraph 5) shall be deemed as null and void.

On the other hand, the right of the maker of a database is subject to certain exceptions and limitations under the scope of providing the legitimate user of a database that had been made available (by any means) to the public the ability to extract and/or re-utilize a substantial part of its content in the following cases; a) in the case where such an extraction is made for educational or research purposes, provided that the source is quoted, and to the extent that it is justified on the grounds of the non-commercial purpose (profoundly) pursued; b) when the extraction and/or re-utilization is made for reasons of public safety or within the scope of administrative or judicial procedures.

The Greek legislator had further clarified that this sui generis right applies to databases
whose makers or rightholders are citizens of a Member - State or in the case where they have their habitual residence within the Union territory. It is also applicable to companies and enterprises that had been established in accordance with the law of a Member – State, and whose registered offices, central administration or main establishment is located within the Union. Moreover, the interpretation given under Articles 9 and 11 of the Directive 96/9/EC on the legal protection of databases had been introduced as such to national law thus it is dictated that in the case where certain company or enterprise has exclusively its registered office within the Union territory, business activities shall be genuinely and on an ongoing basis aligned to the economy of a Member – State. Last, the exceptions and limitations provided under the revised Article 28A –as amended on the grounds of implementation at national level of the Directive 2017/1564/EE- are also applicable to the sui generis right of the maker of a database.

The last paragraph of Article 45A, Law No. 2121/1993 provides for certain rules on the term of protection of this right; first, it is stated it shall run from the date of completion of the making of the database and shall expire fifteen (15) years from the 1st of January of the year following the date of completion. In the case of a database that had been made available to the public in any means prior to the expiration of the term of protection, the latter shall be calculated from the 1st of January of the year that follows the date on which the database was first made available to the public. Lastly, it is stated that any substantial modification, being evaluated on either qualitative or quantitative terms, of the content of a database, in particular any substantial modification resulting from the accumulation of successive addendums, deletions or alterations that result to the consideration of the relevant investment as a new substantial one, being also here evaluated on qualitative or quantitative terms, which would result in the database being considered to be a substantial new investment, attracts –in relation to the database deriving from this investment- a right of the same term of protection.

14. What key protections exist for personal data?

The protection of personal data and privacy of individuals constitutes a fundamental human right. Data protection laws grant the data subjects, i.e. individuals, certain rights and imposes certain responsibilities on data controllers. In Greece, the data protection regime is primarily set out in the General Data Protection Regulation 2016/679 (EU) (GDPR) and Law 4624/2019, incorporating the Regulation 2016/679 (EU) (GDPR) and the Directive 2016/680 implementing into national law. Moreover, while the e-Privacy Law (Law 3471/2006) applies mainly to the electronic communications sector, certain provisions are not sector-specific, such as the provisions on unsolicited communications.

Based on the above-mentioned legal framework, processing of personal data must meet the following fundamental data protection principles and requirements regarding data subjects’ rights:

Lawfulness
The legal basis for the legitimate processing of personal data, according to the GDPR, might be consent, performance of a contract with the data subject, compliance with a legal obligation, protection of the individual’s vital interests, performance of a task carried out in the public interest or protection of the controller’s or a third party’s legitimate interest. For special categories of data (eg, data related to health, race, political or religious beliefs) processing is prohibited, unless one of the conditions defined in Article 9 paragraph 2 of the GDPR apply (eg, explicit consent, processing necessary for preventive or occupational medicine, etc).

In its recent Decision No 26/2019, the HDPA imposed a fine on a controller for invoking consent as the legal basis for processing personal data of employees, thus giving them a false impression that processing of their data depends on their consent.

Transparency and fairness

Processing of personal data must be carried out in a fair and transparent manner. Controllers must provide data subjects with clear information concerning the processing of their data (eg, which data is processed, how, why, by whom, the recipients of the data). This information must be provided in a brief, easily accessible, comprehensible, clear and simple manner.

Purpose limitation

Collection and processing of personal data by controllers must be based on specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes shall not be considered to be incompatible with the initial purposes.

Article 24 of Law 4624/2019 provides that the authorities may process personal data for different purposes when such processing is necessary for them to exercise their duties. When it comes to private entities, processing of data for different purposes is allowed following a request from the authorities for reasons of national and public security, if it is necessary for the prosecution of criminal offences, or for the establishment, exercise or defence of legal claims, which are not overridden by the interests of data subjects (Article 25 of Law 4624/2019).

Data minimisation

Controllers must only process as much data as necessary. Data processed should be adequate, relevant and limited to what is necessary for the purposes of processing.
Indicatively, the HDPA has issued Opinion 4/2013 and relevant official decisions restricting the processing of criminal records and providing that, if not required by law, these should be replaced by solemn declarations of employees which would only refer to convictions for specific crimes related to the main activity of the controller.

Accuracy

Personal data must be accurate and kept up-to-date. In this context, an immediate erasure or rectification of inaccurate data is mandatory for controllers.

Storage limitation

Personal data should be retained for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, for scientific or historical research or statistical purposes subject to implementation of the appropriate technical and organisational measures.

The HDPA has defined specific retention periods (eg, Opinion 1/2011 on CCTV defining a retention period of 15 working days, without prejudice to sector-specific provisions) in certain cases where no statutory retention period is defined.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Any breach of confidentiality, integrity or availability by “accidental or deliberate action” constitutes a data breach.

Accountability

According to the principle of accountability, controllers and processors must design their processes and technical and organisational systems in such a way that they can prove before the supervisory authorities or courts that they are fully compliant with the applicable framework for personal data (Law 4624/2019, GDPR). The introduction of the principle of accountability shifts the “burden of proof” of compliance from the data protection authorities to controllers and processors. The GDPR provides controllers and processors with a range of regulatory methods and tools for this purpose, such as:
· keeping records of processing activities;

· implementation of security measures;

· data protection impact assessments;

· appointment of a data protection officer;

· compliance with data breach notification obligations; and

· encouraging the adoption of codes of conduct.

Data Subjects’ rights

Controllers must ensure data subjects’ rights with respect to processing of their personal data and ensure that they may exercise them, as well. Data subjects have the right to request:

· Access to their personal data;

· Rectification of their personal data if it is inaccurate or incomplete.

· Deletion of their personal data, unless their processing is necessary for the exercise of legal rights of the Controller for the fulfillment of a legal obligation, for public interest reasons or for defending its legal rights before judicial or other Authorities.

· Restriction of processing of their personal data only for specific purposes.

· To withdraw at any time their consent to the processing of their personal data for marketing purposes and/or targeted advertising. In such case, their processing by the Controller will be suspended, nevertheless this will not impact the legitimacy of any processing performed until the time of withdrawal.

15. Are there restrictions on the transfer of personal data overseas?

The applicable personal data protection legal framework imposes restrictions on the transfer of personal data outside the European Economic Area (EEA), to third countries or international organisations. Personal data may be transferred outside the EEA, where the recipient of the personal data has provided adequate safeguards (eg, model clauses and/or binding corporate rules) or if the Commission has made an “adequacy decision” – in other words, if it has decided the country has an adequate level of data protection. Individuals’ rights must be enforceable and effective legal remedies for individuals must be available
following the transfer.

In addition, according to Article 75 and following Law 4624/2019 (implementing Directive 680/2016), if the requirements are met then data transfers to countries outside the EEA authorities or to international organisations are also allowed in the context of prosecution of criminal offences.

16. **What is the maximum fine that can be applied for breach of data protection laws?**

Article 83 of the GDPR states that supervisory authorities shall impose administrative fines that shall be effective, proportionate and dissuasive.

There are two tiers of administrative fines that can be levied as penalties for non-compliance with the GDPR, depending on the specific articles of the Regulation that the organisation has breached. In specific, data security breaches will be subject to the lower level, whereas infringements of an individual’s privacy rights will be subject to the higher level.

- Up to €10 million, or 2% annual global turnover – whichever is higher.
- Up to €20 million, or 4% annual global turnover – whichever is higher.

In Greece, regarding the private sector, the GDPR’s provisions (General Data Protection Regulation), apply, as there is no further specialization in the applicable national law (L. 4624/2019). The two highest till today fines imposed by the HDPA to a private sector company under the new regulatory framework for the protection of personal data concern the Hellenic Telecommunications Organization (O.T.E.). Specifically, these are two fines totaling € 400,000 on the one hand for non-compliance with the right of objection and breach of the principle of data protection as well as breach of the principle of accuracy and data protection by design during the storage of its subscribers’ personal data.

On the other side, regarding the public bodies acting as Controllers, the national Law 4624/2019 (art. 39) sets a maximum fine of €10 million.

However, the HDPA can take a range of corrective actions, such as the following, given that not all GDPR infringements lead to serious fines:

- Issuing warnings and reprimands;
- Imposing a temporary or permanent ban on data processing;
- Ordering the rectification, restriction or erasure of data; and
17. **What additional protections have been implemented, over and above the GDPR requirements?**

In addition to the above-mentioned applicable legal framework (pls see answer in question No 8), the HDPA at regular intervals or when it deems it necessary, issues guidelines and recommendations to the Controllers regarding issues that require clarification. For example, recently the HDPA issued guidelines for the processing of personal data for the management of Covid-19, as well as the taking of security measures in the context of remote working, dated on 18.03.2020 and 15.04.2020 respectively.

Other than that, the Greek State, proceeded to a specialization of GDPR’s provisions regarding the consent of minor. In particular, according to the Article 8 of the GDPR, the Member States were able to provide for the age at which a minor may consent alone to the processing of her/his personal data, provided that it is between 13 and 16 years of age. The national Law 4624/2019 on protection of personal data set this age at 15 years old. As a result, if the Greek minor is under 15 years of age, the processing of his/her personal data is legal only after the consent of his / her legal representative has been given.

18. **Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?**

The E-commerce Directive (Directive 2000/31/EC), which was transposed into Greek legislation by PD 131/2003, contains specific rules in connection with the applicable law for information society services and is also applicable to cloud services.

Furthermore, when it comes to personal data protection in cloud services, the EU’s General Data Protection Regulation 2016/679 (GDPR) applies, alongside the local implementation Law No 4624/2019 on the Protection of Personal Data, which introduces specific criminal penalties for illegal processing of personal data, in addition to the administrative penalties already applicable under the GDPR.

As far as cybersecurity is concerned, which is largely connected to the cloud computing services, the legal framework that applies to cloud providers offering computing services, as digital service providers, is the Greek Law 4577/2018, which transposes the Network and Information Security Directive 2016/1148/EU (NIS).

Another legislative act related to cybersecurity is Act No 3674/2008, which states the obligations of network operators and electronic communication service providers in terms of network security, decryption, system and supervision. Other provisions relevant to confidentiality of communications concern the criminalisation of the various acts of unlawful interception and further use of unlawfully acquired communications data (see articles...
370–370D of the Greek Criminal Code) and the prohibition of using such unlawfully acquired evidence in the criminal procedure (see Article 177 of the Greek Code of Criminal Procedure).

Ultimately, there is also specific legal framework that applies to regulated sectors, when it comes to cloud computing services, such as the public administration sector (the Greek Law No 4623/2019 and Law No 3979/2011 (the “e-governance” law) have been implemented, imposing on public administrations the obligation to acquire computer programs after conducting a particular market evaluation on cloud providers and other software solutions) and the financial services sector (Act No 2577/2006 and Act No 2597/2007 of the Governor of the Central Bank of Greece with regard to internal control and privacy systems for the banking sector, as well as in Law No 3431/2006 and Law No 2472/1997, to the extent that they do not conflict with the provisions of the GDPR.)

19. **Are there specific requirements for the validity of an electronic signature?**

For electronic signatures, the requirements set out in the eIDAS Regulation (EU 910/2014) came into direct effect to all EU member-states, including Greece. Greece generally supports the concept of a Qualified Electronic Signature (QES), meaning that an independent accreditation for these signatures by an approved certification body is required. Although Recital 49 of the eIDAS Regulation (EU No 910/2014) allows Member States to set requirements regarding the type of electronic signature that will be required in certain circumstances, no such law has been voted in Greece.

Regarding the accreditation itself, Greece follows the European Telecommunications Standards Institute standards for the technical requirements of the Qualified Electronic Signatures, as well as the Decision of the Hellenic Telecommunications & Post Commission, which offers a list of Qualified Trust Service Providers publicized at its site.

It should be noted, however, that, although electronic signatures have been increasingly used in the public sector, QES have not been extensively used in the private sector in practice (with the exception of certain industries, such as finance and banking) and thus, its acceptance by the courts, tax authorities, business registry, labour and social security authorities has not been tested. According to eIDAS Regulation, the provisions set therein do not affect the national law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form. This means that certain cases are not typically appropriate for electronic signatures, including documents than need to be notarized or hand written (indicatively, among others, contracts to purchase or transfer real property, grants/donations, certain deeds governed by the law of successions, etc).

Furthermore, companies and individuals that wish to participate in public tenders are obliged to use digital signature (Qualified Electronic Signature). In order to be able to use a QES, the individual interested would have to be certified by a Qualified Trust Service Provider (QTSP) and use qualified signature creation devices (QSCD).
20. **In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?**

Not automatically. Especially for the employees, even in cases where the outsourcing of IT services takes place between associated companies, the employee cannot be transferred to the outsourcing supplier automatically. In practice, this tend such as assets and third-party contracts, a contractual provision has to exist to their agreements in order for the transfer to take place automatically to the outsourcing supplier.

More analytically, under Greek law, neither employees’, assets’ nor third – party or any type of contracts concerning not only IT but any kind of services could be automatically transferred to any other person that than the initial counterparty, entailing the event of an outsourcing which is subject to the contractual terms that are mutually agreed (profoundly) on an ad hoc basis thus subject to the freedom of contracts.

The principle of freedom of contracts derives from and is inexorably intertwined with economic freedom as provided by the Greek Constitution, and is further analyzed to the freedom to conclude or not a (given) contract, the freedom to choose the counterparty and the freedom to determine the exact content of a contract, meaning the contractual clauses that shall be binding upon the parties. Consequently, no one is (or could be) obliged to conclude a contract with the content of which he/she does not agree -and be respectively committed to the execution of a given clause-, profoundly covering contractual terms provided under an agreement concluded between third – parties. On the contrary, the determination of the exact content of contractual clauses is subject to the free willing of the parties and the relevant negotiations provided that they are not contrary to the law - profoundly referring to constitutional provisions and the mandatory rules provided under Greek legal system- or morality. These limitations applicable to the freedom of contracts -as in any individual right- are complemented by the obligation to respect the rights of third – parties meaning that a given contract shall not be cumbersome and shall not generate obligations for third – parties.

As a result, the outsourcing of IT -as of any- services is subject to the general principle of freedom of contracts -under the aforementioned limitations-, meaning that any relevant issue -including the employment status or assets- shall not be considered as being “automatically” transferred to any third – party unless otherwise provided by contract.

21. **If a software program which purports to be a form of A.I. malfunctions, who is liable?**

Artificial Intelligence is not specifically regulated nor is there a specific legislative framework to cover its applications in Greece. Therefore, all legal questions, including the ones related to liability, are primarily approached based on the Greek Civil Code, although this may very often lead to dead ends. Additionally, all AI technologies in Greece ought to meet the essential health and safety requirements laid down in the EU safety legislation (as it has been
transposed into Greek law), such as Directive (EC) 2006/42 on machinery (the safety legislation applicable to robots), Directive 2014/53/EU on radio equipment (which applies to all products that use the radio frequency spectrum, including embedded software) and Directive 2001/95/EC on general product safety.

Additionally, EU product liability regime also applies, introduced by the Product Liability Directive (D 85/374/EEC) and was implemented by amendments of the Greek Consumer Protection Law No. 2251/1994. This framework, which applies to all new digital technologies, establishes a strict liability regime against the producers of defective products, holding them liable when these defective products cause damage to natural persons or their property, while the injured consumers are not required to prove the fault of the producer.

On the other hand, for the tortious liability to be attributable to a party, the Greek Civil Code sets out five conditions that need to be fulfilled cumulatively: a) human behaviour, b) illegal action, c) fault, d) damage and e) causal link between behaviour and damage. It is obvious that if a software program characterised as Artificial Intelligence causes damage, some of the abovementioned conditions are rather difficult to substantiate, especially one party’s fault and the causal link between the human behaviour and the damage occurred.

Up until today, it appears that the current legal framework of extra-contractual liability, despite the challenges, can be applied to damage causes by A.I. softwares. However, taking into account the new generation of AI which approaches operational autonomy and behavioural unpredictability through their capacity to analyse and learn from their environments, it will be increasingly more difficult to identify the natural person at fault for the damage caused by the AI software which means that all implicated parties should aim to act proactively when operating A.I. software in Greece and regulate contractually all possible aspects of liability for such systems, while aiming to an insurance coverage as well.

22. **What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?**

In Greece, the legal and regulatory framework that governs cybersecurity issues mainly consists of Law 4070/2012 (particularly Article 37 thereof) and ADAE Regulations 165/2011 and 205/2013 (as in force, amended with ADAE Decision 99/2017). According to the applicable provisions of the above, operators offering internet access networks and/or services should maintain and implement security policies, supported by relevant analytical procedures. In addition to the above, provisions of the Data Protection Law apply which require data controllers and processors to ensure the implementation of appropriate organisational and technical measures to ensure protection of personal data. All of this entire framework is subject to obligations arising from the GDPR in force, applicable since 25 May 2018. Another legislative act related to cybersecurity is Law No 3674/2008,

which states the obligations of network operators and electronic communication service providers in terms of network security, decryption, system and supervision.
In addition, in December 2018, Law 4577/2018 entered into force incorporating into Greek law Directive 2016/1148/EU (NIS), establishing measures to achieve a high level of security of network and information systems. The aforementioned law, inter alia, sets specific obligations for ‘basic services operators’, namely all public or private entities (of the kind referred to in Annex I), including regarding digital infrastructure: internet traffic exchange points (IXP), domain name system (DNS) service providers, and Top Level Domain Names Registry (TLD), that meets specific criteria. The criteria are as follows: (a) the entity should be providing a service essential for the maintenance of critical social or economic activities; (b) the provision of this service should be based on network and information systems; and (c) it should be causing a serious disruption to the provision of the service in question as defined in Article 5 by any event. Moreover, businesses falling within the scope of Law 4577/2018 have certain obligations, among which are: to adopt technical and organisational measures for the security of networks and information systems; to adopt measures to prevent and minimise the impact of incidents affecting the security of networks and information systems; to notify without undue delay the National Cybersecurity Authority and the Hellenic Data Protection Authority of incidents with a serious impact on business continuity, while providing additional information regarding the severity of the relevant incident and to cooperate with the competent authorities. In addition, the Law 4411/2016 which nationally implemented the Directive EU 2013/40 and the Budapest Convention on Cybercrime that accordingly transformed the Greek Criminal Code refers to the criminalization of illegal actions against the maintenance of information systems.

Other provisions relevant to confidentiality of communications concern the criminalisation of the various acts of unlawful interception, the impeding of an information system’s operation and further use of unlawfully acquired communications data (see articles 292A, 292B, 370–370D, 381A of the Greek Criminal Code) and the prohibition of using such unlawfully acquired evidence in the criminal procedure (see Article 177 of the Greek Code of Criminal Procedure). Furthermore, the Law 4411/2016, incorporating into Greek law Directive 2013/40/EU, which updated the criminal legislation in the field of cyber criminality, applies. This law punishes actions directed against information networks and in specific, against the integrity and availability of data or information systems. In specific, under the new law, article 370C of the Greek Criminal Code has been amended and hacking is now explicitly mentioned as an illegal act punishable by imprisonment. If the illegal act of hacking refers to international relations or the security of the state, the perpetrator is punished by the provisions of Article 148 on Spying.

23. **What technology development will create the most legal change in your jurisdiction?**

The Internet of Things (IoT), advanced robotics, Artificial Intelligence (AI) and autonomous systems powered by AI (e.g. drones) will result in significant legal change. For example, autonomous vehicles (reliant on network-connected sensors) require a rethinking of legal relationships, from who bears liability in the event of an injury, to the nature of driver and vehicle insurance. Smart devices may be capable of entering into contracts with other devices, using self-executing provisions in smart contracts maintained on a blockchain. These
technological developments will require a re-evaluation of basic principles of contract law. The complex enabling ecosystem and the feature of autonomous decision-making as well as the rollout of the Internet of Things bring substantial challenges in terms of the safety of connected systems, products and services, as well as for businesses’ liability. Many different layers are involved in these emerging digital technologies and, therefore, it could be difficult to determine who is technically and legally responsible for any ensuing damage. Also, legislation should address the issues of free movement of data, interconnected robots and AI network security, protection of personal data, and privacy in communication between humans, robots and AI.

24. **Which current legal provision/regime creates the greatest impediment to economic development/commerce?**

The increasing momentum for privacy protections that fail to address big data and use of artificial intelligence could create serious impediments to economic growth. This is why an optimal balance should be achieved between predictability of the regulatory environment and adaptability to scientific and technological progress. In other words, the forthcoming regulatory regime should strike a careful balance between protecting consumers and encouraging businesses to market innovative products.

25. **Do you believe your legal system specifically encourages or hinders digital services?**

Digital services are ruled in essence by EU legislation. As a member state of the EU, Greece implements and applies all EU legislation. National laws of Greece, not emanating from the EU, do not create any major impediments to the development of emerging digital technologies and services.

26. **To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?**

The Greek legal system is not yet completely ready to deal specifically with legal issues associated with Artificial Intelligence. The Greek legal system is not unique in facing these challenges, as artificial intelligence will require all legal systems to re-evaluate the application of basic legal principles. It is expected that AI-related issues will be resolved within the EU. It is reminded that on 19 February 2020, the European Commission published a White Paper aiming to foster a European ecosystem of excellence and trust in Artificial Intelligence20 and a Report on the safety and liability aspects of AI.21 The White Paper proposed:

- Measures that will streamline research, foster collaboration between Member States and increase investment into AI development and deployment;

- Policy options for a future EU regulatory framework that would determine the types of legal requirements that would apply to relevant actors, with a particular focus on high-risk
applications.