

Law Alert

The associate law firm of EY Greece



Law 4961/2022 regulates the utilization and use of a basic set of contemporary advanced technologies with significant economic and social impact. It thus creates the conditions for the rapid adoption and development of these technologies in Greek economy and society, with the ultimate goal of promoting the country's digital transformation. In this respect, the new Law establishes horizontal and vertical obligations for public bodies as well as for natural persons and private entities that produce, distribute, utilize and make use of these technologies.

On July 27, 2022, Law 4961/2022 "on emerging information and communication technologies, the reinforcing of digital governance and other provisions" was published in the Government Gazette (GG 146/A/27-07-2022).

The new Law establishes a coherent legislative framework for artificial intelligence ("AI"), the Internet of Things (IoT), the provision of postal services using Unmanned Aircraft Systems ("UAS"), distributed ledger technologies ("DLT") and smart contracts, as well as three-dimensional printing ("3D Printing").

Law 4961/2022 enacts sectoral obligations for providers of products and services related to AI, IoT and UAS in transport, and horizontal regulations for the use of AI and three-dimensional printing, while laying the foundations for conducting transactions with DLTs and smart contracts.

The provisions of the new Law have an impact on the digital transformation of the public sector and on the sectors of technology and digital economy, while they develop a horizontal effect on the digitization of transactions.

1. Context and Purpose

The regulations of the new Law 4961/2022 are developed in four parts, which concern, among others, the digital upgrade of public administration (Part A') and the utilization of advanced technologies (Part B').

In particular, Part A' of the Law (articles 1-27) aims to establish the adequate institutional framework for the exploitation of the potential of AI by public and private sector bodies under conditions of fairness and security, as well as to strengthen the resilience of the public administration against cyber threats. In the context of serving this purpose, Part A of the Law includes regulations for (a) the development of artificial intelligence, and (b) the enhancement of information security and data protection.

Furthermore, Part B of the Law (articles 28-57) aims at the exploitation by the public sector and the private market of the potential unleashed by advanced technologies in line with good practices, with the ultimate goal of consolidating the digital transformation of the country. For this purpose, Part B of the Law includes regulations regarding (i) the Internet of Things ("IoT"), (ii) Unmanned Aircraft Systems ("UAS"), (iii) distributed ledger, and (iv) 3D printing.

2. Provisions on Al

Pending the adoption of the Artificial Intelligence ("AI") Act by the European Union ("EU"), Law 4961/2022 introduces a national framework to regulate the use of AI technologies in the public and private sectors.

This national legal framework provides for the following obligations per category of obligated entities:

A. Public Bodies

- Provision by Statute: Except for the Ministries of National Defense and Citizen Protection, the use of Al systems is permitted only by a special provision by statute, which includes appropriate safeguards for the protection of the rights of natural or legal persons affected by these systems.
- Algorithmic Impact Assessment: Before using an Al system, in addition to performing an impact assessment of Regulation (EU) 2016/679 ("GDPR"), any public body has the obligation of executing an algorithmic impact assessment to

- assess the risks that may arise to the rights, freedoms and legitimate interests of the persons affected by such AI system. A Presidential Decree shall specify the appropriate safeguards for the protection of the rights of persons affected by the use of AI systems.
- Operational Transparency: Each public body publicly discloses information, inter alia, about the commencement of operation and the operating parameters of the AI system under consideration as well as on the decisions taken or supported through it. Any allegations on violations of transparency obligations are examined by the National Transparency Authority.
- Register of AI Systems: Each public body maintains a register of the AI systems it uses.

B. Private Entities

- Al in the Employment Context: Prior to the initial use of an Al system, which affects the decision-making process concerning employees, existing or prospective, and has an impact on their conditions of employment, selection, recruitment or evaluation, each entity shall provide relevant information to the employee. The relevant obligation also applies to digital platforms in respect of natural persons linked to them by employment contracts or independent service provision or project agreements. For any violation of this obligation, penalties are imposed by the Labour Inspectorate.
- Ethical Use of Data: Any medium or large private sector entity within the meaning of article 2 of Law 4308/2014, should adopt a policy for the ethical use of data, which includes information on the measures, actions and procedures it applies to data ethics issues when using Al systems. In addition, any such company, which prepares a corporate governance statement in accordance with article 152 of Law 4548/2018 (A' 104), must include, in the relevant statement, information about its data ethics policy. A Joint Ministerial Decision shall specify the content of such policies.
- Register of AI Systems: Each medium or large private sector entity within the meaning of article 2 of Law 4308/2014 maintains a register of the AI systems it uses.
- Public Procurement: In any public procurement procedure for the design or development of an Al system, the contractor bears the following obligations:

- The contracting authority is provided with information necessary to fulfil its transparency requirements on AI system operation;
- ii. The AI system is delivered in such a way so that the contracting authority is enabled to study its modus operandi and parameters, to further improve it and to publish or make available, in any way, those improvements; and
- iii. Appropriate measures are taken to bring the Al system in line with applicable laws, in particular, regarding the protection of human dignity, the respect for private life and the protection of personal data, non-discrimination, equality between women and men, freedom of expression, universal access for persons with disabilities, workers' rights and the principle of good administration.

The provisions of Law 4961/2022 on Al technologies do not affect the rights and obligations provided for in the GDPR and Law 4624/2019 on the protection of personal data.

Finally, the new Law establishes, on the one hand, a Coordinating Committee for AI with responsibilities for the drafting of the National Strategy for AI and, more generally, the formulation of policy around AI and, on the other hand, a Committee for the supervision of the strategy, which ensures the implementation, the coordination of the competent bodies and manages its enforcement.

To carry out their work, the two committees receive data and know-how from the AI Observatory, which monitors and reports on technological developments and policies around AI in the country and at an international level.

3. Provisions on Information Security & Data Protection

Law 4961/2022 further establishes the following institutions for shielding the country against threats related to information and network security:

The General Directorate of Cybersecurity of the Ministry of Digital Governance is designated as the National Cybersecurity Certification Authority in accordance with article 58 of Regulation (EU) 2019/881. Ministerial decisions shall define the monitoring procedure and the bodies assessing the products, services and ICT procedures vis-a-vis the

- requirements of European cybersecurity certificates, as well as the relevant sanctions in case of non-compliance.
- The Ministry of Digital Governance establishes the Hybrid Threat Analysis Observatory, i.e. the advisory body of the National Cybersecurity Authority with responsibility related to the analysis and prevention of hybrid threats in the field of cybersecurity.
- The General Directorate of Cybersecurity of the General Secretariat for Telecommunications and Post of the Ministry of Digital Governance is designated as the national coordination centre as per Article 6 of Regulation (EU) 2021/887.
- In each central government body, an Information and Communication Systems Security Officer ("ICSSO") is appointed, with the task of supervising the security of the entity's network and information systems and ensuring the issuance of a risk analysis plan and the security policy of the Body's ICT systems.
- Each public body having a critical infrastructure also designates a Security Coordinator, who carries the duties of the ICSSO for this particular infrastructure.

As per the new Law, providers of public electronic communication networks have in place and align with an information security risk assessment plan, which they update on an annual basis. Also, a procurement plan in relation to the equipment obtained and the participation of third-party suppliers.

Finally, a register of data protection officers of public sector bodies is established as well as a relevant committee for the exchange of expertise and cooperation with ISDPS.

4. Provisions on IoT

According to the definitions of Law 4961/2022, Internet of Things ("IoT") constitutes any technology that:

(a) allows devices or a group of interconnected or related devices, through their internet connection, to perform automatic processing of digital data; and (b) enables the collection and exchange of digital data, in order to offer a variety of services to users, with or without human participation.

Law 4961/2022 imposes legal obligations on manufacturers, importers / distributors and operators of IoT devices, indicatively:

- Manufacturers should accompany IoT devices with a declaration of compliance with the technical safety specifications, indicated in the law, as well as instructions for use and safety information.
- Each manufacturer should have a management process in a device with IoT technology, in cases where it is ascertained by the user that: a) a security incident occurs, or b) a vulnerability exists in the security parameters of the device.
- Importers and distributors should verify that the IoT appliances they import or distribute are accompanied by a relevant declaration of compliance.
- IoT operators should follow the technical safety specifications of each device.
- IoT operators should appoint an IoT Security Officer to monitor the security measures of IoT technology devices, provided for by the law.
- Each IoT operator should maintain a register of IoT devices, updated on an annual basis and, in any event, when putting into service a new IoT device.
- Each IoT operator should carry out an impact assessment of the planned personal data processing operations related to the operation of the IoT technology device.

The National Cybersecurity Authority is appointed as the competent authority to oversee the IoT security framework implementation. The Authority has the power to:

- Require from manufacturers, importers or distributors of IoT devices to take all necessary corrective actions in order to comply with the applicable legislation.
- Order the temporary withdrawal from the market of IoT appliances presenting risks and their replacement in the market only if such risks have been removed.

Upon the Authority's recommendation, the competent body of the Ministry of Digital Governance may impose penalties of up to \leqslant 15,000 and, in case of relapse, of up to \leqslant 100,000 on non-compliant manufacturers, importers, distributors and operators.

Ministerial decisions will specify the technical specifications and safety measures of IoT technology devices, the obligations of manufacturers, importers and suppliers of such products as well as the relevant sanctions in case of non-compliance.

5. Provisions on the Use of UAS in the Context of Postal Services

The provision of postal services, for which a general or special permit has been granted, in all or part of the Greek territory, may be carried out using Unmanned Aircraft Systems ("UAS"), subject to approval by the National Telecommunications and Post Commission ("NTPC").

The use of frequencies by UAS, throughout the provision of the relevant services, is governed by the Delegated Regulation (EU) 2019/945 and the Implementing Regulation (EU) 2021/664.

The specific technical characteristics and technical safety specifications of UAS, used for the provision of postal services, as well as any other relevant issue, are determined by a decision of the Minister of Digital Governance, following an opinion of the NTPC and the Civil Aviation Authority.

6. Provisions on DLT

Law 4961/2022 defines "distributed ledger" as the repository of information that keeps records of transactions, and which is shared and synchronized between a set of DLT network nodes, using a consensus mechanism.

Furthermore, a blockchain is defined as a type of distributed ledger technology that records data in blocks, which are connected to each other in chronological order and form a chain of a consensual, decentralized and mathematically verifiable nature, which is mainly based on the science of cryptography.

Finally, a smart contract is defined as a set of coded computer functions, which is finalized and executed through distributed ledger technology in automated electronic form through instructions for the execution of actions, omissions or tolerances, which are based on the existence or not of specific conditions, according to terms recorded directly in electronic code, scheduled commands or programmed language.

For DLTs, the new Law provides for the following regulations:

- Data records or transactions may be conducted through a blockchain or other DLT, rendering valid the declarations of will exercised in such a form.
- Smart contracts bind contracting parties as per the general provisions of the Civil Code on private contracts.
- DLTs and smart contracts have the validity of proof before the courts equal to that of private documents.

7. Provisions on 3D Printing

Articles 53-57 of Law 4961/2022 provide the framework for the regulation of 3D printing.

"3D Printing" is defined in the law as the process of uniting 3D printing materials through the technique of prosthetic successive stratification of such materials by using new technologies, especially 3D printers, and aiming on printing a physical object based on a digital model.

The new Law introduces the following amendments to Law 2121/1993 on copyright regarding works of speech on 3D printing:

- Any Computer Aided Design File (C.A.D. File) is explicitly characterized as a protected work of speech, as long as it includes a source code.
- > 3D printers are expressly subject to a 4% private levy on their value for the benefit of authors and right-holders of neighbouring rights.

Moreover, the new Law prohibits the use, sharing and hosting on online platforms of digital models or digital design files with the help of a computer or digital files of a typical triangle language or digital model design databases, without the prior permission of the author or the rightful owner.

As an exception, such acts are also permitted without the author's permission if they are carried

out solely for: a) private, judicial or administrative use, b) use for the benefit of persons with disabilities, c) use for temporary or ancillary phases of a technological process that do not have independent economic significance, d) the fulfillment of educational or research purposes, e) news purposes or f) the use of images or objects in public places or exhibitions in museums or in exhibits catalogues, provided that, in the above cases, the normal utilization of the work or other protected subject-matter is not affected and the legitimate interests of the author or the rightful owner are not unduly prejudiced.

The Law also provides for liability to compensate providers of online platforms, through which digital models or digital files, without source code u related to the 3D printing process, are used, shared or hosted, if, after becoming aware of the infringement, they do not take all necessary measures to remedy.

Finally, the new Law establishes the liability of the creator or legal owner or seller, as the case may be, towards consumers for defective digital models or files related to the 3D printing process or three-dimensional printed objects or three-dimensional printers or scanners.

8. Conclusion

Law 4961/2022 sets in force a coherent national legal framework for the utilization of emerging technologies by public bodies and private entities. It is thus expected to contribute in boosting the digital transformation of the country's public and private sectors.

The new Law entered into force upon its publication in the Government Gazette, i.e. from 27.07.2022, except for the regulations on artificial intelligence, which will enter into force on 1.1.2023, and the regulations on the Internet of Things, which will enter into force on 1.3.2023.

The Law is available here.

About Platis - Anastassiadis & Associates

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 39 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis - Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:

Eirinikos Platis

Partner eirinikos.platis@gr.ey.com

Antonios Broumas

Senior Manager antonios.broumas@gr.ey.com

at the

Platis - Anastassiadis & Associates Law Partnership

Tel.: +30 210 2886 512

Email: platisanastassiadis@gr.ey.com

© 2022 All rights reserved

ey.com

Platis - Anastassiadis & Associates Law Partnership is associated with EY. Partners: E. Platis, A. Anastassiadis Partnership is registered with the Athens Bar, registration number 80240 List of our associates upon request.

This document contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global EY organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.