AI SYSTEMS USED BY GREEK ENTITIES - A PRACTICAL GUIDE

▶ www.sioufaslaw.gr

Sioufas & Associates
Law Firm

AI systems used by Greek entities- a practical guide

Greece recently enacted L.4961/2022 with regard to emerging technologies, whereby many relevant topics are covered such as 3D printing and copyright, smart contracts and Distributed Ledger Technology. On the forefront of this new legal framework is AI.

According to the AI Act a deployer is defined as a natural or legal person, public authority, agency or other body using an AI system under its authority. Deployers of AI systems have specific responsibilities given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use.

Public domain entities

Algorithmic impact assessment-transparency and registry obligations

Within this law it is expressly stated that the entities of the public domain are expressly permitted, during the exercise of their duties, to use AI systems that affect the rights of natural or legal persons, either for the procedure of decision-making or for the support of the procedure

Piraeus
6ᴬ Neou Falirou St. floor
GR-182 33, Ag. I. Renti
tel: +30 210 3673000
fax: +30 210 3673070
email: info@sioufaslaw.gr
website: www.sioufaslaw.gr

Thessaloniki
3 Nikiforou Ouranou St.

GR-546 27, Thessaloniki
tel: +30 231 6005800
fax: +30 231 6005899

Patra
65 Othonos-Amalias Ave.

GR-262 22, Patra
tel: +30 261 0226549
fax: +30 261 0242971

Romania
76 Splaiul Unirii, River Plaza Tower A 7ᵗʰ

Bucharest, District 4, P.C.040037
tel: +40 372 171778
fax: +40 372 171779
email: info@sioufaslaw.ro
website: www.sioufaslaw.ro

of decision-making, or for issuing relevant acts. Such specific use, however, must previously be expressly foreseen by a special provision of Law that contains sufficient safeguards for the protection of respective rights.

Moreover, the above-mentioned entities must perform an algorithmic impact assessment before the deployment of the AI system. It is pinpointed that this assessment does not overlap with the obligation to perform a data protection impact assessment, according to Art. 35 of the GDPR.

The algorithmic impact assessment must include the following information:

(a) the purpose pursued, including the public interest served by the use of the system,

(b) the capabilities, technical characteristics and operating parameters of the system,

(c) the type and categories of decisions taken or the acts adopted involving, or supported by, the system,

(d) the categories of data collected, processed or entered into or generated by the system,

(e) the risks that may arise for the rights, freedoms and interests of the natural or legal persons concerned or affected by the decision-making, and

(f) the expected benefit to society as a whole in relation to the potential risks and impacts that the use of the system may entail, in particular for racial, ethnic, social or age groups and categories of the population such as people with disabilities or chronic diseases.

In terms of transparency the following information must be publicly provided:

(a) the time when the system becomes operational,

(b) the operational parameters, capabilities and technical characteristics of the system,

(c) the categories of decisions taken or acts adopted involving or supported by the system and

(d) the performance of an algorithmic impact assessment.

Piraeus
6ᴬ Neou Falirou St. floor
GR-182 33, Ag. I. Renti
tel: +30 210 3673000
fax: +30 210 3673070
email: info@sioufaslaw.gr
website: www.sioufaslaw.gr

Thessaloniki
3 Nikiforou Ouranou St.
GR-546 27, Thessaloniki
tel: +30 231 6005800
fax: +30 231 6005899

Patra
65 Othonos-Amalias Ave.
GR-262 22, Patra
tel: +30 261 0226549
fax: +30 261 0242971

Romania
76 Splaiul Unirii, River Plaza Tower A 7ᵗʰ
Bucharest, District 4, P.C.040037
tel: +40 372 171778
fax: +40 372 171779
email: info@sioufaslaw.ro
website: www.sioufaslaw.ro

The entities of the public domain must ensure in this regard that every natural or legal entity affected by the decision or the act is aware of the parameters on which the decision was based in an understandable (principle of explainability) and easily accessible form.

Thirdly, the entities of the public domain are burdened with the obligation to keep an updated registry of the AI systems they use.

The registry must contain the following information:

(a) the purpose to be achieved, along with the public interest sought to be served with the use of the AI system,

(b) the time of deployment,

(c) the operational parameters, capabilities and technical characteristics of the system,

(d) the basic information of the system, i.e. trade-title, version, and producers' data,

(e) measures for the safety of the system, and

(f) the completion of an algorithmic impact assessment or a data protection impact assessment, if necessary.

Private entities

The abovementioned obligations of performing an algorithmic impact assessment and transparency and registry obligations should also be adhered to by private entities.

Registry obligations and transparency

In particular, the obligation to keep a registry of AI systems under L.4961/2022 (in electronic form) is required from medium to large-size (classification according to L.4308/2014) entities. Such obligation, however, applies exclusively to the following two areas:

(a) the compilation of profiles for consumers; and/or

(b) the evaluation of all kinds of employees and/or collaborating natural persons.

The abovementioned registry, must contain the following information:

(a) a description of the operating parameters, capabilities and technical characteristics of the system,

Piraeus
6ᴬ *Neou Falirou St.*
floor
GR-182 33, Ag. I. Renti
tel: +30 210 3673000
fax: +30 210 3673070
email: info@sioufaslaw.gr
website: www.sioufaslaw.gr

Thessaloniki
3 Nikiforou Ouranou St.

GR-546 27, Thessaloniki
tel: +30 231 6005800
fax: +30 231 6005899

Patra
65 Othonos-Amalias Ave.

GR-262 22, Patra
tel: +30 261 0226549
fax: +30 261 0242971

Romania
76 Splaiul Unirii, River Plaza Tower A 7ᵗʰ

Bucharest, District 4, P.C.040037
tel: +40 372 171778
fax: +40 372 171779
email: info@sioufaslaw.ro
website: www.sioufaslaw.ro

(b) the number and status of the natural persons concerned or likely to be concerned,

(c) the technical information relating to the supplier or external partners involved in the development or operation of the system,

(d) the period of operation of the system, and

(e) the measures taken to ensure their safe operation.

Apart from the abovementioned transparency provisions that private entities should adopt as the provisions for public entities foresee, article 50 of the AI Act specializes how the transparency obligations for providers and deployers are applied in each case.

Adoption of Ethical data use and data governance policies

More importantly, such private entities are also obliged to establish and maintain an ethical data use policy, which shall include information on the measures, actions and procedures it applies in relation to data ethics in the use of systems of AI.

To this end high-quality data and access to them play a vital role. High-quality data sets for training, validating and testing require the implementation of appropriate data governance and management practices. Data sets should be relevant, sufficiently representative and, as much as possible, free of errors and complete with regard to each purpose. Additionally, data sets should have appropriate statistical properties as regards the persons in relation to whom the high-risk system is intended to be used with specific attention to possible biases. In order to ensure that fundamental rights are protected, deployers of high-risk AI systems shall perform a fundamental rights impact assessment prior to its use.

High risk AI systems and respective obligations

In terms of high-risk AI-systems, the obligations imposed by the AI Act are:

(a)   to have a risk-management system in place,

(b)   to ensure the quality and relevance of data sets used,

(c)   to have technical documentation and record-keeping, transparency, human oversight, robustness, accuracy and cyber-security

 (Arts 8,9,10,11,12,13,14 and 15 of the AI Act).

Deployers should, in particular, take appropriate technical and organizational measures to ensure they use high-risk AI systems in accordance with the instructions of use (Art. 26 of AI Act). Furthermore, deployers should ensure that the persons assigned to implement the instructions for use and human oversight as set out in the AI Act have the necessary competence, in particular an adequate level of AI literacy, training and authority to properly fulfil those tasks.

Private entities must understand how the high-risk AI system will be used and should therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use and the persons or groups of persons likely to be affected, including vulnerable groups. Where deployers have identified a serious incident, they should immediately inform first the provider, then the importer or distributor and the relevant market surveillance authorities of that incident.

It is highlighted that high-risk AI systems should be designed in a manner to enable deployers to understand how the AI system works, evaluate its functionality, and comprehend its strengths and limitations. High-risk AI systems should be accompanied by appropriate information in the form of instructions of use. Such information should include the characteristics, capabilities and limitations of performance of the AI system. Those would cover information on possible known and foreseeable circumstances related to the use of the high-risk AI system, including deployer action that may influence system behaviour and performance, under which the AI system can lead to risks to health, safety and fundamental rights (rec. 72). Where appropriate, illustrative examples, for instance on the limitations and on the intended and precluded uses of the AI system, should be included.

To the extent the private entity/deployer exercises control over the input data, that deployer shall ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system. Deployers of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months. In order to ensure that fundamental rights are protected, deployers of high-risk AI systems shall perform a fundamental rights impact assessment prior to its use (Art. 27).

It is important to note that the European Commission has approved the guidelines to specify the use cases that will be forbidden as of 2 February 02, 2025, according to the

Piraeus
6ᴬ Neou Falirou St. floor
GR-182 33, Ag. I. Renti
tel: +30 210 3673000
fax: +30 210 3673070
email: info@sioufaslaw.gr
website: www.sioufaslaw.gr

Thessaloniki
3 Nikiforou Ouranou St.
GR-546 27, Thessaloniki
tel: +30 231 6005800
fax: +30 231 6005899

Patra
65 Othonos-Amalias Ave.
GR-262 22, Patra
tel: +30 261 0226549
fax: +30 261 0242971

Romania
76 Splaiul Unirii, River Plaza Tower A 7ᵗʰ
Bucharest, District 4, P.C.040037
tel: +40 372 171778
fax: +40 372 171779
email: info@sioufaslaw.ro
website: www.sioufaslaw.ro

Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

For more information on AI and employment please check https://www.sioufaslaw.gr/en/ai-and-employment-in-greece.

Therefore, private entities play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system.

Marios D. Sioufas
Deputy Managing Partner
LL.M. in Intellectual Property Law – Queen Mary University of London