THE LAW 5321/2026 ABOUT THE IMPLEMENTATION IN GREECE OF THE REGULATION 2024/1689 (AI ACT)

By Achilleas Christodoulou, Senior Associate, at A. & K. METAXOPOULOS AND PARTNERS LAW FIRM

On 20.07.2026 the Greek law 5321/2026 "*measures of implementation for Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Regulation) - Amendment of Law 4961/2022 (Government Gazette 146) and other provisions*" has been published in the Government Gazette, which adopts measures for the implementation in Greece of the Regulation 2024/1689 (hereinafter the "***AI ACT***").

The purpose of law 5321/2026 regarding the AI, according to art. 1 of the law, is to create a framework for the supervision of AI systems[1], in order to ensure a high level of protection of health, safety and fundamental rights when using these systems and also to support innovation, through the adoption of law measures for the implementation in Greece of the AI ACT.

Some of the significant issues that are regulated by the provisions of the law 5321/2026 are:

i. The designation of national competent authorities and single points of contact;

ii. the assessment of notified bodies;

iii. the establishment of a national AI regulatory sandbox;

[1] It is noted that not all the AI systems are regulated by AI ACT. See indicatively par. 63 and 64 of the Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), dated 29.07.2025, according to which: "*(63) Only certain AI systems are subject to regulatory obligations and oversight under the AI Act. The AI Act's risk-based approach means that only those systems giving rise to the most significant risks to fundamental rights and freedoms will be subject to its prohibitions laid down in Article 5 AI Act, its regulatory regime for high-risk AI systems covered by Article 6 AI Act and its transparency requirements for a limited number of pre-defined AI systems laid down in Article 50 AI Act. The vast majority of systems, even if they qualify as AI systems within the meaning of Article 3(1) AI Act, will not be subject to any regulatory requirements under the AI Act*" and "*(64) The AI Act also applies to general-purpose AI models, which are regulated in Chapter V of the AI Act. The analysis on the differences between AI systems and general-purpose AI models is outside the scope of these Guidelines*".

iv. the administrative penalties regarding the breaches of the obligations imposed regarding AI and

v. the introduction of a new crime regarding the transparency obligation and deepfakes.

I. THE DESIGNATION OF NATIONAL COMPETENT AUTHORITIES AND SINGLE POINTS OF CONTACT

1. Market Surveillance Authorities

First of all, the independent public authority, **Hellenic Data Protection Authority** (hereinafter "***H.D.P.A.***"), which has the mission of the supervision of the application of the General Data Protection Regulation (G.D.P.R.) and the relevant domestic legislation about the protection of personal data, is designated in accordance with art. 70 par. 1 of the AI ACT as the **Market Surveillance Authority**[2] regarding: **a)** the AI systems falling within the prohibited practices of Article 5 of the AI ACT, **b)** high-risk AI systems referred to in Annex III of the AI ACT and **c)** AI systems for which transparency obligations are provided for, in accordance with article 50 of the AI ACT. H.D.P.A. is also designated as a **Single Point of Contact** in accordance with art. 70 par. 2 of the AI ACT.

In addition, the law provides that the market surveillance authorities, which have been designated under national legislation to implement an EU Directive or to implement measures for an EU Regulation, as listed in Section A of Annex I to the AI ACT, are designated as market surveillance authorities for high-risk AI systems related to products covered by that harmonisation legislation.

The law also regulates the issues of the exercise of the right to lodge a complaint with a market surveillance authority provided by art. 85 of the AI ACT. A unified system of lodging complaints is created for complaints either before H.D.P.A. or any other market surveillance authority (see above paragraph) and the details about the procedure related to filing and handling of a complaint are outlined.

Moreover, the law includes articles imposing the cooperation of H.D.P.A. and any other market surveillance authority with other authorities in Greece (e.g. customs authorities, ministries etc).

2. Notifying Authority

[2] According to art. 3, definition 26 of the AI ACT: "*market surveillance authority means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020*"

The independent authority, **Hellenic Telecomunications and Post Commission** (hereinafter "***H.T.P.C.***"), which has the mission to regulate, monitor and supervise the sectors of electronic communications, radio frequency spectrum and postal services, in Greece, has been designated as the **Notifying Authority**[3] in accordance with article 28 of the AI ACT.

In addition, a Coordination Center for know-how in AI is established in H.T.P.C. which, inter alia, shall provide support, advisory, training etc to the market surveillance authorities.

II. THE ASSESSMENT OF NOTIFIED BODIES

The law also includes provisions about the application of conformity assessment bodies[4] for notification[5] and the procedure of assessment of the application in accordance with at. 31 of the AI ACT by the notifying authority (i.e. H.T.P.C.).

Especially regarding the assessment of conformity, in accordance with Annex VII of the AI ACT, of high-risk AI systems to be put into operation by authorities responsible for law enforcement, immigration and asylum in Greece, the law expressly designates H.D.P.A. as notifying body (which obviously will have to act separately from its capacity as the Market Surveillance Authority).

III. ESTABLISHMENT OF A NATIONAL AI REGULATORY SANDBOX

Art. 57 par. 1 of the AI ACT imposes the obligation to each Member State to establish at least one AI regulatory sandbox at national level. Implementing this obligation, the law provides that an AI regulatory sandbox is established at the H.T.P.C. and the competent authorities about its operations will be both H.T.P.C. and H.D.P.A. and in addition all the other market surveillance authorities shall participate as well.

---

[3] According to art. 3, definition 19 of the AI ACT: "*notifying authority means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring*".

[4] According to art. 3, definition 21 of the AI ACT: "*conformity assessment body means a body that performs third-party conformity assessment activities, including testing, certification and inspection*".

[5] According to art. 3, definition 22 of the AI ACT: "*notified body means a conformity assessment body notified in accordance with this Regulation and other relevant Union harmonisation legislation*".

It is noted that the law 5321/2026 includes a diversion from the default position of AI ACT regarding the approval for a real-world testing plan. More specifically:

According to art. 60 par. 4 of the AI ACT:

"*4. Providers or prospective providers may conduct the testing in real world conditions only where all of the following conditions are met:*

[…]

(b) the market surveillance authority in the Member State where the testing in real world conditions is to be conducted has approved the testing in real world conditions and the real-world testing plan; <u>where the market surveillance authority has not provided an answer within 30 days, the testing in real world conditions and the real-world testing plan shall be understood to have been approved</u>; where national law does not provide for a tacit approval, the testing in real world conditions shall remain subject to an authorisation;

[…]"

On the other hand, art. 13 par. 2 of the law 5321/2026 provides that:

"*2. The required approval, based on paragraph 4 of article 60 of the Regulation on AI, of the testing of AI systems in real conditions and of the testing plan in real conditions, by the H.D.P.A. or the competent market surveillance authority of paragraph 2 of article 3, is provided only after the express written permission of the aforementioned competent authority. <u>The inaction of the thirty (30) day deadline of subpar. b) of paragraph 4 of article 60 of the Regulation on AI shall not be deemed to constitute approval</u>.*"

IV. THE ADMINISTRATIVE PENALTIES REGARDING THE BREACHES OF THE OBLIGATIONS IMPOSED REGARDING AI

First of all, the law provides that H.D.P.A. and all the other market surveillance authorities as well, have the powers provided by art. 14[6] and 16[7] of the Regulation 2019/1020, for the compliance of the products with the EU harmonization legislation[8].

In addition, the law provides that H.D.P.A. and all the other market surveillance authorities may: **a)** issue warnings to operators that an AI system that is being considered to be placed on the market or put into operation is likely to infringe the provisions of the AI ACT or law 5321/2026; **b)** order operators to comply in a specific manner and within a specified period

---

[6] Powers of market surveillance, investigation and enforcement, including the powers: **a)** to require relevant documents, technical specifications, data or information on compliance and technical aspects of the product; **b)** to require relevant information on the supply chain/ distribution network; **c) t**o require relevant information required for the purpose of ascertaining the ownership of websites; **d)** to carry out unannounced on-site inspections and physical checks of products; **e)** to enter any premises, land or means of transport; **f)** to start investigations in order to identify non-compliances and bring them to an end; **g)** to require economic operators to take appropriate action to bring an instance of non-compliance to an end or to eliminate the risk; **h)** to take appropriate measures where an economic operator fails to take appropriate corrective action or where the non-compliance or the risk persists, including the power to prohibit or restrict the making available of a product on the market or to order that the product is withdrawn or recalled; **i)** the power to impose penalties; **j)** to acquire product samples, including under a cover identity, to inspect those samples and to reverse-engineer them in order to identify non-compliance and to obtain evidence; **k)** where no other effective means are available to eliminate a serious risk i. to require the removal of content referring to the related products from an online interface or to require the explicit display of a warning to end users when they access an online interface; or ii. where a request according to point (i) has not been complied with, to require information society service providers to restrict access to the online interface, including by requesting a relevant third party to implement such measures.

[7] Regarding the market surveillance measures of art. 16 of the Regulation, the market surveillance authorities instruct the relevant economic operator to take appropriate and proportionate corrective action to bring a non-compliance to an end or to eliminate the risk within a period they specify. The relevant corrective action required to be taken by the economic operator may include: a) bringing the product into compliance, including by rectifying formal non-compliance as defined by the applicable Union harmonisation legislation, or by ensuring that the product no longer presents a risk; b) preventing the product from being made available on the market; c) withdrawing or recalling the product immediately and alerting the public to the risk presented; d) destroying the product or otherwise rendering it inoperable; e) affixing to the product suitable, clearly worded, easily comprehensible warnings of the risks that it might present, in the language or languages determined by the Member State in which the product is made available on the market; f) setting prior conditions for making the product concerned available on the market; g) alerting the end users at risk immediately and in an appropriate form, including by publication of special warnings in the language or languages determined by the Member State in which the product is made available on the market. If the economic operator fails to take corrective action or where the non-compliance or the risk persists, market surveillance authorities shall ensure that the product is withdrawn or recalled, or that its being made available on the market is prohibited or restricted, and that the public, the Commission and the other Member States are informed accordingly.

[8] According to art. 1 par. 1 of the Regulation: "*1. The objective of this Regulation is to improve the functioning of the internal market by strengthening the market surveillance of products covered by the Union harmonisation legislation referred to in Article 2, with a view to ensuring that only compliant products that fulfil requirements providing a high level of protection of public interests, such as health and safety in general, health and safety in the workplace, the protection of consumers, the protection of the environment and public security and any other public interests protected by that legislation, are made available on the Union market*".

of time with the AI ACT or law 5321/2026; **c)** issue reprimands to operators when an AI system has infringed the provisions of the AI ACT or law 5321/2026; **d)** impose the administrative fines provided for in Article 99 of the AI ACT; **e)** threaten or impose periodic financial penalties when the operators do not comply with its orders, not exceeding, if the infringement is committed by an undertaking, two percent (2%) of the average daily total worldwide turnover or income in the previous financial year (the periodic penalty ceases when the operator demonstrates full compliance).

The law explicitly provides that these measures may also be imposed on public sector bodies, as well.

Furthermore, according to article 99 par. 7 of the AI ACT:

"*7. When deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and, as appropriate, regard shall be given to the following:*

(a) the nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

(b) whether administrative fines have already been applied by other market surveillance authorities to the same operator for the same infringement;

(c) whether administrative fines have already been applied by other authorities to the same operator for infringements of other Union or national law, when such infringements result from the same activity or omission constituting a relevant infringement of this Regulation;

(d) the size, the annual turnover and market share of the operator committing the infringement;

(e) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement;

(f) the degree of cooperation with the national competent authorities, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the degree of responsibility of the operator taking into account the technical and organisational measures implemented by it;

(h) the manner in which the infringement became known to the national competent authorities, in particular whether, and if so to what extent, the operator notified the infringement;

(i) the intentional or negligent character of the infringement;

(j) any action taken by the operator to mitigate the harm suffered by the affected persons".

In addition to the above, the law 5321/2026 provides that H.D.P.A. and the other market surveillance authorities in the context of imposing administrative penalties, may take into account also whether the provider or implementing body under consideration has taken sufficient measures to ensure an adequate level of literacy in the field of AI, in accordance with Article 4 of the AI ACT.

Moreover, in the framework of a dispute settlement procedure established by a decision of H.D.P.A., H.D.P.A. and the other market surveillance authorities may take also into account whether the operator under examination admits the alleged violation of the relevant provisions of the AI ACT or the law 5321/2026.

It is noted that law 5321/2026 expressly provides that the decisions of H.D.P.A. and of the other market surveillance authorities can be appealed before the Supreme Administrative Court (Council of the State).

V. THE INTRODUCTION OF A NEW CRIME REGARDING THE TRANSPARENCY OBLIGATION AND DEEPFAKES

A penal provision has been included under art. 23 in the law 5321/2026 with the title "*Prohibition on removing transparency marks of Article 50 of Regulation 2024/1689* ***for deep fakes content***"

More specifically, according to art. 23 of the law 5321/2026:

"*Whoever* ***removes the machine-readable annotations on the output data of AI systems****, which produce synthetic content,* ***or obstructs the proper functioning of the technical solutions of the AI system provider*** *aimed at the above-mentioned annotation of output data, in accordance with paragraph 2 of Article 50 of Regulation (EU) 2024/1689,* ***or removes or obstructs the notification of the deployer,*** *in accordance with paragraph 4 of Article 50 of Regulation (EU)*

2024/1689, regarding the fact that specific content constitutes a product of deep fake ***or*** *has been produced* ***or*** *manipulated artificially, shall be punished by imprisonment and a fine, unless the act is punished more severely by another provision*".

The drafting of the abovementioned provision seems problematic regarding its scope and more specifically whether the above criminal provision refers only to deep fakes or if it also covers any other case of removal of the relevant annotations.

First of all, the title of article 23 indicates that it is applicable only regarding the deep fakes. In addition, the explanatory statement of the law, explicitly mentions that the purpose of this provision is to ensure transparency regarding deep fakes. So, from a first read, one could conclude that it is evident that the provision is applicable only regarding deep fakes.

The definition of "deep fake" is provided in art. 3 No. 60 of the AI ACT, according to which: " *'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events* ***and would falsely appear to a person to be authentic or truthful***"

However, from the wording of the abovementioned article it is not so clear that it refers only to deep fakes. More specifically, it is not clear if the phrase "*regarding the fact that specific content constitutes a product of deep fake*" **refers only to the act of "removing or obstructing the notification of the deployer, in accordance with paragraph 4 of Article 50 of Regulation (EU) 2024/1689"** (indeed this paragraph is the only one that refers explicitly to "deep fakes"[9]**) or if it extends to the other, previously mentioned acts in this article**, i.e. removing the machine-readable annotations on the output data of AI systems, which produce synthetic content or obstructing the proper functioning of the technical solutions of the AI system provider aimed at the above-mentioned annotation of output data, in accordance with paragraph 2 of Article 50 of Regulation (EU) 2024/1689 (paragraph 2 does not refer in principle only to deep fakes but it is more general and broader, including any type of artificially generated or manipulated content[10]). If the former will be accepted as interpretation, the acts that may constitute the

[9] "*4. Deployers of an AI system that generates or manipulates image, audio or video content constituting* ***a deep fake****,* ***shall disclose that the content has been artificially generated or manipulated****. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work".*

[10] "2. *Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are* ***marked in a machine-readable format and detectable as artificially generated or manipulated****. Providers shall ensure their technical solutions are*

new crime shall include all the cases of removal, obstruction etc of the annotations imposed by the AI ACT which may not constitute a deep fake e.g. they are not essentially image, audio or video content (it could be also text according to art. 50 par. 2 of the AI ACT) or even if they do not include content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.

If, on the other hand, the interpretation that the phrase "*regarding the fact that specific content constitutes a product of deep fake*" refers to all the acts mentioned in the article, the applicability of this provision will be narrowed down solely to the cases that the generated content will fall within the definition of the deep fake (e.g. a removal of the provider's annotation of art. 50 par. 2 of the AI ACT will constitute an act of crime only regarding the deep fakes and it will not be applicable e.g. in a text).

Nevertheless, the problems of the drafting continue with the addition after the phrase "*regarding the fact that specific content constitutes a product of deep fake*" of the phrase "*or has been produced or manipulated artificially*". So, this wording **seems to extend the criminal acts beyond the deep fakes, covering any content which has been produced or manipulated artificially**. However, this does not seem to be in line both with the title of the article and the explanatory statement of the law, which refer explicitly to the deep fakes!

As the wording of the above article may create problems regarding its interpretation and applicability, it would be essential for the legislator to amend it in a way which shall create more certainty.

***

The present article constitutes only a brief, general outline of the provisions of the law and it is not a legal advice. Obviously, it may not cover all the detailed provisions of the law. For any specific situation, any interested party must seek specific legal advice from a qualified lawyer.

---

effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards. This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute criminal offences".

This article was originally edited by, and first published on, www.lexology.com. Please click here to view the original publication.