THE CERTIFICATION OF HIGH-RISK AI SYSTEMS

DIMITRIOS LINARDATOS

THE CERTIFICATION OF HIGH-RISK AI SYSTEMS[1]

Dimitrios LINARDATOS
Saarland University

Abstract

This chapter offers an analysis of the certification regime for high-risk AI systems under the EU AI Act. Although certification represents an exception within the overall structure of the AI Act, it functions as an important legal instrument: it determines market access, defines compliance obligations, and shapes the intersection of private ordering and public oversight. The chapter first reconstructs the classification logic of high-risk systems as set out in Article 6 AI Act. Two complementary pathways—one product-based, the other use-case driven—structure the risk taxonomy. However, this approach reveals inconsistencies. The reliance on existing Union harmonisation legislation can result in regulatory blind spots, particularly where third-party conformity assessments are absent despite evident fundamental rights risks. Second, the chapter distinguishes between internal and external conformity assessments, outlines the provider's duties from technical documentation to CE marking, and discusses the legal status of the EU declaration of conformity. Finally, the chapter reflects on the normative ambivalence of the AI Act's conformity assessment logic. On the one hand, it represents a functional extension of European product safety law into the digital domain. On the other, it delegates significant regulatory responsibility to private actors. The chapter concludes that the AI Act's certification regime illustrates the broader challenge of AI regulation: how to align formal legal structures with the fluid realities of algorithmic decision-making in high-risk domains.

Keywords

Certification procedures; High-risk AI and conformity assessment; EU product safety law; Notified bodies; Legal risk governance

[1] The text corresponds to a slightly expanded, partially annotated, and updated version of the manuscript of a lecture. The lecturing style has been largely retained.

1. INTRODUCTION

In practice, it is imperative that certain AI systems will need certification in accordance with the regulatory framework delineated in the EU's AI Regulation (AI Act)[2] – this is in part because the certification process requires significant investment in terms of both time and financial resources. However, the certification requirement under the AI Act is an exception. In this particular context, I would like to address three points below. (i) Which AI systems are subject to mandatory certification requirements under the provisions of the AI Act? (ii) What is the process for obtaining certification under the AI Act? (iii) What are the legal ramifications of failing to comply with certification requirements?

2. HIGH-RISK AI SYSTEMS SUBJECT TO CERTIFICATION REQUIREMENTS

As indicated by the title, certification is mandatory for AI systems that are deemed to pose a high risk. A primary objective of the AI Act is to ensure that high-risk AI systems are subject to stringent regulatory oversight, as opposed to their outright prohibition. In the case of these systems, the regulatory framework set out in the AI Act is the most strict, comprehensive and detailed (Wagner et al., 2025, mn. 6 et seq). The classification of an AI system as high-risk is contingent upon two criteria: the potential for harm in ordinary interactions and the potential impact on fundamental rights associated with the system's operations. The classification of a system as high-risk AI is carried out in accordance with Art. 6 of the AI Act, which defines more specific criteria for differentiation.

2.1. Classification according to Art. 6 para. 1 of the AI Act

According to Art. 6, para. 1, lit. a of the AI Act, an AI system's classification as high risk depends on whether it is to be used as a safety component of a product that is covered by the Union harmonisation legislation listed in Annex I or that can be classified as such as a product. Art. 6, para. 1, lit. b of the AI Act stipulates that the relevant safety component or product must undergo a so-called third-party conformity assessment with regard to placing the product on the market or it putting into service in accordance with the Union harmonisation legislation listed in Annex I of the AI Act. Hence, the concept of high-risk AI systems is strongly linked to the Union's harmonisation legislation (Leinarte 2024, pp. 262, 265). The classification as a high-risk AI system is therefore decisively influenced by whether the product is already subject to a conformity assessment in accordance with the applicable Union legislation. As a result, the

---

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

AI Act stipulates that whether a conformity assessment is required with regard to other products covered by Annex I of the AI Act is not determined by the Act itself but rather by the specified legislation that already regulates these products.

As an illustration: if a product is classified as a medicinal product and is thus subject to the obligation to undergo a conformity assessment, this remains the case when the medicinal product in question is equipped with an AI component that is relevant for the safety of the product.

The all-encompassing objective of the AI Act is, thus, to establish an additional set of obligations that serves to reinforce the existing product safety scheme, only in in-stances where it is deemed essential to address the unique characteristics inherent to AI systems (Leinarte 2024, pp. 262, 266). This interpretation is confirmed by Art. 43, para. 3 of the AI Act, which elucidates that the provider of high-risk AI systems covered by the acts listed in Annex I, Section A of the AI Act is obliged to comply with the conformity assessment procedures required under those acts. However, the requirements set out in Section 2 of Chapter III of the AI Act apply to those high-risk AI systems and also have to be part of that assessment. Nevertheless, the Union harmonisation legislation listed in Annex I of the AI Act has a pivotal role.

In the absence of a mandatory conformity assessment as set out in the harmonised provisions listed in Annex I, Section A of the AI Act, the classification of a system as a high-risk AI system is precluded, in principle, in accordance with the stipulations of Art. 6, para. 1, lit. b of the AI Act. The legislator is thus introducing a loophole in the field of AI regulation. This is evidenced by the fact that a system may present a substantial risk to individuals' health, safety or fundamental rights, as defined in Art. 6, para. 3 of the AI Act; thus, classification as a high-risk system may be deemed warranted, contingent on the identified criticalities. However, a categorisation as a high-risk AI system cannot be made without a mandatory third-party conformity assessment.

The "transport goods" covered by Annex I, Section B of the AI Act, which are covered by the so-called old regulatory concept of product safety, represent a special case within the scope of application of Art. 6 of the AI Act. Art. 2, para. 2 of the AI Act largely excludes these products from the scope of application of the Act, meaning that the requirements of Art. 8 et seqq. of the AI Act are not directly applicable. Instead, according to Art. 112 of the AI Act, the Commission will be granted certain powers to evaluate and review the AI Act in the future. These transport goods are excluded because they are not subject to the regulatory framework introduced by the new legislative package. Rather than an internal conformity assessment, they are subject to an official safety inspection (Leinarte 2024, pp. 262, 268 et seq.).

In summary, the categorisation of a system as high-risk pursuant to Art. 6, para. 1 of the AI Act is predicated, in large part, on the *principles of product safety law*.

2.2. Classification according to Art. 6, para. 2 of the AI Act

In contrast, an *application-related* classification is made in Art. 6, para. 2 of the AI Act, which stipulates that, in addition to the high-risk AI systems listed in para. 1 of Art. 6 of the AI Act, the systems listed in Annex III of the AI Act are also to be classified as high-risk. The catalogue in Annex III of the AI Act includes, for example, systems for remote biometric identification, systems for categorisation or emotion recognition, any systems that are part of critical infrastructures and those that are used in law enforcement, migration issues, the administration of justice and so on. In this case, as well, the intended use of the work is of the utmost importance, outweighing the context (Sousa e Silva, 2025, para. 73; see also Hacker, 2023, p. 7).

In principle, these systems are deemed to present a substantial risk of harm to the health, safety or fundamental rights of natural persons (Sousa e Silva, 2025, para. 58 et seqq). In the absence of such risks, the classification of the AI system as high-risk is precluded. It is important to note that there is no freely available risk assessment option; instead, the list provided in Annex III of the AI Act is decisive in itself. This schematic concept has the clear objective of ensuring legal certainty: it is intended to prevent legal addressees from being subject to the uncertainties of the interpretation of largely undefined legal terms, which would have been necessary if a free risk classification had been provided for. Accordingly, in accordance with the prevailing act's conceptual framework, the addressees are expected to be capable of ascertaining, through the implementation of a designated catalogue, the extent to which they are subject to the stipulations outlined within Chapter III, Section 2 of the AI Act.

The strictly defined list yields the welcome effect that the possibility of "category jumps" is ruled out: if the legislator had provided for the possibility of subsequent classification as a high-risk AI system based on the demonstrated activities in the application, providers would have been required to consider the possibility of impending illegality.

Consider the following case. A court reporter has written about various nasty cases: fraud, predatory theft and cases of blackmailing – pretty much everything that is imaginable in a court reporter's career. Now he wants to explore the finer aspects of culture and society in life and therefore he decides to write a cultural article. This is the first time he has tried his hand at this, so he is curious to see how the article will be received. He has heard about an AI-powered search engine and decides to give it a try. He enters his name, the place of work and the term "article". The results of the search are surprising: he reads that he is a convicted abuser, that he escaped from a psychiatric ward, that he is guilty of illegal possession of firearms. Furthermore, it is alleged that he has misappropriated the pensions of poor widows in an immoral manner, namely as an unscrupulous undertaker. The user inquires with the chatbot as to whether it is

certain that the individual in question is responsible for all the crimes in question. The chatbot confirms this and goes on to state that the individual in question was also involved in other criminal activities.

A journalist from Tübingen reported a comparable occurrence.[3] It is evident that the individual's human dignity has been profoundly violated. In the event that the fundamental rights sensitivity of the AI behaviour in question is taken into consideration, and if this is deemed to be sufficient for a category shift, then the chatbot would consequently be classified as a high-risk AI system owing to its behaviour. This would necessitate deactivation, as the obligations of providers of high-risk AI systems would have been violated, particularly because the systems would not have been certified as high-risk AI systems. Therefore, it would be prudent to ensure that "spontaneous" category shifts do not pose any potential legal concerns. It would impose an unreasonable burden on the provider to deactivate the system at the slightest unexpected occurrence.

From the perspective of legislators, the creation of a formal concept carries with it the potential for regulatory loopholes to emerge, given the rapid pace of technological advancement. This issue is addressed by Art. 7 of the AI Act, which empowers the Commission to adopt delegated acts to amend Annex III of the AI Act. In conceptual terms, this enables the Commission to subsequent close identified gaps. This is further evidenced by Art. 7 of the AI Act, which stipulates that, when deciding whether to include a system in Annex III of the AI Act, the Commission must consider the extent to which the use of an AI system has already harmed health and safety, had a detrimental impact on fundamental rights and so forth. To be quite clear: first, damage must be identified, and then a solution can be proposed in accordance with the relevant regulations.

A critical analysis of the broad categories enumerated in Annex III of the AI Act suggests that certain AI systems could be misclassified as high-risk solely due to the context of their use, even when no actual risk is present (see Mantelero, 2025, p. 316). However, such a view would overlook the essential corrective role of Art. 6, para. 3 of the AI Act: this provision, which derogates from Art. 6, para. 2 of the AI Act, stipulates that an AI system listed in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of individuals – including instances where it does not materially influence the outcome of decision-making.

---

3 Cf. SWR aktuell, 16.8.2024 (https://kurzlinks.de/7mvo).

3. CONFORMITY ASSESSMENT

As was already indicated, the need for a conformity assessment has a dual role. *First*, it serves as a differentiating criterion between "normal" AI systems and high-risk AI systems. *Second*, it creates a safety obligation for the provider.

The AI Act delineates two distinct types of conformity assessment: the majority of conformity assessments are conducted internally, hence by the provider himself (for more details, see Linardatos, 2025, s. 8). Conversely, administrative conformity assessment (for more details, see Roth-Isigkeit, 2025, s. 9) represents a notable exception to this rule. In the latter case, certification by the competent authority is required, thus external certification takes place. The internal conformity assessment procedure is concluded with the issue of a declaration of conformity, the CE marking and the registration of the AI system.

The standards on the conformity assessment process based on internal control are specified by Annex VI of the AI Act. The provider has *first* to verify that the established quality management system is in compliance with the requirements set out in Art. 17 of the AI Act so that he meets his "behavioural obligations" (Moretti et al., 2025, s. 2.2). *Second*, the provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in the AI Act. *Third*, the provider is also required to verify that the design and development process of the AI system, together with its post-market monitoring,[4] as referred to in Art. 72 of the AI Act, is consistent with the system's technical documentation.

In terms of external control, the assessment of the quality management system is carried out in conjunction with an evaluation of the relevant technical documentation by a competent authority, which in the AI Act is called a "notified body". The procedure of the external control is further specified in Annex VII of the AI Act. The external assessment procedure is supplemented with regulations on the surveillance and scrutiny of the approved quality management system.

3.1. Criteria for demarcation

According to Art. 43, para. 2 of the AI Act, for high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI of the AI Act, which does not provide for the involvement of a notified body. The systems mentioned relate to: critical infrastructure, education, employment, worker management, access to self-employment and so on.

---

4 This is deemed to be quite challenging based on the findings of Wagner et al. (2025, mn. 547 et seqq).

Accordingly, the involvement of a notified body is provided for systems that are referred to in point 1 of Annex III of the AI Act, which pertain to biometrics, in particular: remote biometric identification systems or AI systems intended to be utilized for emotion recognition.

Furthermore, any product subject to the legislation set out in the AI Act in Annex I, Section A of the New Legislative Framework will continue to be subject to certification by a notified body in accordance with the applicable rules. If a product contains an AI system, to which the requirements of AI Act as well as requirements of the Union harmonisation legislation listed in Section A of Annex I of the AI Act apply, the providers are responsible for ensuring that their product is fully compliant with all applicable requirements under applicable Union harmonisation legislation. However, to promote coherence, avoid duplication and reduce additional burdens, providers may opt to incorporate the required testing procedures, reporting obligations, and any other accompanying information or documentation for their product into the compliance materials and processes already mandated under the Union harmonisation legislation listed in Section A of Annex I of the AI Act, where appropriate.

3.2. Internal conformity assessment

Internal and external conformity assessments aim to verify that high-risk systems comply with the requirements laid out in the AI Act. When evaluating these requirements, the intended purpose of the use of the system needs to be taken into account, as does the reasonably foreseeable misuse of that system. Indeed, the system's qualification within the coordinate system of the AI Act is not determined by the system itself. Rather, it is determined by the intended use of the AI system by the provider (cf. Arts 3(12), 8 AI Act). This offers the provider the option to exclude the application of the AI Act in its entirety, provided that the system's documentation explicitly states that the system is not intended for a specific purpose *and* that the provider has implemented adequate preventive measures (see, in a similar vein, Sousa e Silva, 2025, para. 11, without the technical clarification provided here, which is, however, mandatory).

With this in mind, the lifespan of any AI system begins with the design phase, and is followed by the preparation of the corresponding technical documentation and the specification of the system's rationale therein. In the context of conformity assessment, such technical documentation is of central importance, as it serves as the primary reference point for demonstrating regulatory compliance. Thereafter, the system undergoes both design finalisation and testing. The training phase encompasses all tasks necessary to ensure that the model produces reliable and consistent outputs, aligned with its intended function. The most challenging part here is to gather enough training data free of bias (see the findings by Wagner et al., 2025, mn. 498 et seqq).

Following the training, the system must undergo testing. This testing is distinct from the evaluation phase and must be completed prior to its commencement. Specifically, the provider is not permitted to initiate the evaluation phase – characterised by the conformity assessment – until the AI system has been subjected to all requisite testing procedures. It is essential that the product intended for deployment or market release be thoroughly tested to verify its reliability and safety. In the event that the testing yields deficiencies, the provider is compelled to undertake a comprehensive re-evaluation of the design and testing procedures, in addition to revising the technical documentation in accordance with the identified shortcomings. Only upon completion of these corrective measures can the supplier proceed with a subsequent conformity assessment. The objective of the conformity assessment is to furnish conclusive evidence that the system meets the legal and technical requirements. In the event of failure during the evaluation phase, it is evident that the system is not yet ready for market release or for deployment. Consequently, the development process must be reinitiated to ensure that the system is not released prematurely or in a faulty form.

If the conformity assessment indicates that the AI system in questions meets the statutory requirements set forth in Annex VI and Art. 17 of the AI Act, then it may be put into operation or placed on the market. An essential consideration is whether the system complies with the relevant harmonised standards, or with specific parts of such standards, whose references have been published in the Official Journal of the European Union pursuant to Regulation (EU) No 1025/2012 (see for details Linardatos, 2025, s. 8, mn. 17 et seq). However, prior to doing so, the provider is obliged – in accordance with Art. 47 of the AI Act – to prepare a written EU declaration of conformity that can be read by a machine, or that is signed in a physical or electronic format, for each high-risk AI system. This declaration must be kept at the disposal of the relevant national authorities for a period of ten years following the placement of the high-risk AI system on the market or its introduction into service.

3.2.1. Declaration of conformity

The EU declaration of conformity shall state that the high-risk AI system concerned meets the requirements defined by Section 2 of the AI Act. It "shall be translated into a language that can be easily understood by the national competent authorities of the Member States in which the high-risk AI system is placed on the market or made available" – typically English. The declaration of conformity shall contain the information set out in Annex V of the AI Act, which includes:

- AI system name and type and any additional unambiguous reference allowing the identification and traceability;
- the name and address of the provider;
- a "statement that the AI system is in conformity with this Regulation and, if applicable, with any other relevant Union law";
- references to all relevant harmonised standards used.

From a dogmatic point of view, the declaration of conformity is a declaration of knowledge and responsibility (see, similarly, Sousa e Silva, 2025, para. 16). It can, for example, be the foundation for civil liability claims initiated by a user. While the AI Act does not directly address civil liability, providers and operators will be held accountable based on his declaration of conformity under the new Product Liability Directive (PLD).[5]

3.2.2. CE marking and registration

The CE marking shall be affixed to high-risk AI systems in a manner that is clearly visible, easily legible, and permanent. If, due to the nature of the high-risk AI system, it is not feasible or appropriate to affix the marking directly to the system, then the CE marking shall instead be placed on the AI system's packaging or in the documentation accompanying the AI system, as appropriate..

In addition, before placing the AI system on the market or putting the system into service, a high-risk AI system that is included in Annex III of the AI Act has to be registered in the EU database for high-risk AI systems, in accordance with the stipulations set out in Art. 71 of the AI Act.

3.3. Interim summary

The answer to our first question can be summarised like this: to a large extent, there is no need for an independent third-party verification of conformity. The internal conformity assessment is the prevailing method. This approach has the benefit of reducing procedural costs and activating superior private knowledge and experience. It is generally the case that companies are better placed than other entities to assess and evaluate their system. They are so-called *repeat players*. In order to safeguard the interests of users and other third parties, they are subject to control measures at other levels, for example through appropriate market surveillance or ex post claims, for instance under the aforementioned PLD.

3.4. External conformity assessment

As mentioned before, the third-party conformity assessment by a notified body is relevant for AI systems in the area of biometrics.

A notified body is, according to Art. 3, no. 22 of the AI Act, a conformity assessment body notified in accordance with the Act and other relevant Union harmonisation legislation. Member States shall designate a notifying body, which in turn shall designate the notified body in accordance with Art. 30 of the AI Act and the national law of a Member State.

---

5 Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

The requirements relating to the notified bodies are set out in Art. 31 of the AI Act. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks, as well as suitable cybersecurity requirements (Art. 31, para. 2 AI Act). It is imperative that the organisational structure, allocation of responsibilities, lines of reporting and operation of notified bodies is such that confidence is assured in their performance and results of the conformity assessment activities that they conduct (Art. 31, para. 3 AI Act).

3.4.1. Specifics of examination

The external conformity assessment is subject to administrative procedures. It is therefore initiated on the application of the provider. Annex VII of the AI Act specifies which information must be attached to the application. It is imperative that the information provided includes, in particular, the technical documentation and a more detailed description of the organisational structure of the provider's quality management system, as well as an account of the measures and procedures implemented to ensure that the quality management system is adequate for the legal requirements. In contrast to the provider, the authority is unable to directly experience the quality management system in question. Instead, it relies on a comprehensive and transparent representation of the provider's internal organisational structure. Consequently, the provider's application must be meticulously prepared, with a particular focus on the documentation, which should be comprehensive and detailed, providing clear and informative insights.

3.4.2. Approval

A positive decision by the notified body will be notified to the provider or its authorised representative. The notification shall contain the conclusions of the assessment of the quality management system and the reasoned assessment decision. An approval, according to Art. 44 of the AI Act, comes with a certification that is issued by the notified body in accordance with Annex VII and which shall be drawn up in a language that can be easily understood by the relevant authorities in the Member State in which the notified body is established. In the event that Annex I, Section A of the AI Act is deemed to be applicable, this certification will also attest to compliance with the harmonised regulations as set out in this section.

Pursuant to Art. 44, para. 2 of the AI Act, certification shall be valid for the period it indicates, which shall not exceed five years for AI systems covered by Annex I and four years for AI systems covered by Annex III of the AI Act. At the provider's request, the validity of a certificate may be renewed for additional periods, each not exceeding five years for AI systems falling under Annex I and four years for AI systems covered by Annex III of the AI Act – provided that a reassessment is conducted in line with the relevant conformity assessment procedures

Where a notified body finds that an AI system no longer meets the requirements set out in Section 2 of the AI Act, it shall, according to Art. 44, para 3 of the AI Act and taking account of the principle of proportionality, suspend or withdraw the certificate issued or impose restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body is required to provide clear reasons for its decision.

3.4.3. Surveillance

The suspension or withdrawal of certification is contingent on the notification body's surveillance of the deployed AI systems. The purpose of the surveillance carried out by the notified body referred is to make sure that the provider duly complies with the terms and conditions of the approved quality management system. According to Annex VII(5) of the AI Act, for assessment purposes the provider shall allow the notified body to access the premises where the design, development and testing of the AI systems is taking place. The provider shall also share all necessary information with the notified body, which shall carry out periodic audits to make sure that the provider maintains and applies the quality management system and shall provide the provider with an audit report.

It is evident that the legislator has reached certain practical limits, as evidenced by the fact that it orders access to the provider's premises. The relevance of the place where the system was designed to the system in use is questionable if one assumes that the system can exhibit properties in real-world use that cannot be determined in the provider's laboratory (see Linardatos, 2022, pp. 58, 64). It therefore remains to be seen how effective this right of access will be.

3.4.4. Breach of duty

If an AI system is put into legal circulation or put into operation without the necessary certification having been obtained, this clearly constitutes a violation of the law, which may result in fines under Art. 99 et seq. of the AI Act. Furthermore, the legally responsible party must withdraw the system from the market or discontinue its offer. However, in cases where the non-compliance is merely formal in nature, the less severe corrective measures set out in Art. 83 of the AI Act are to be applied.

Given the evidentiary basis for the administrative and punitive consequences, a brief overview of the civil law implications is of more interest. Natural persons are entitled to compensation under Art. 5 of the PLD if the product is faulty. For the purposes of the PLD, "product" means "all movables, even if integrated into, or interconnected with, another movable or an immovable"; this includes "electricity, digital manufacturing files, raw materials and software" (Art. 4, para. 1 PLD). Hence, all AI systems qualify as a "product" in that sense. According to Art. 7, para. 1 of the PLD, a product shall be considered defective where it does not provide the

safety that a person is "entitled to expect or that is required under Union or national law". For safety reasons, a formal consideration is appropriate here: an AI system for which the necessary certification has not been obtained is considered defective, regardless of whether it produces faulty output during use. An exception applies only in the case of purely formal non-compliance pursuant to Art. 83 of the AI Act, unless the non-compliance referred to in Art. 83, para. 1 of the AI Act persists and the market surveillance authority of the Member State took "appropriate and proportionate measures to restrict or prohibit the high-risk AI system being made available on the market or to ensure that it is recalled or withdrawn from the market without delay in accordance with Art. 83, para. 2 of the AI Act.

4. FINAL REMARKS AS CONCLUSION

The regulation of product safety in the context of AI systems is an intricate and manifold undertaking, reflecting the complexity of these technologies and their applications. One of the most pressing challenges lies in the significant costs imposed on providers, particularly due to the extensive documentation requirements. While these demands aim to enhance accountability and transparency, they undeniably place a considerable burden on developers and manufacturers – a regrettable but perhaps unavoidable consequence of ensuring safety and compliance in high-risk domains.

Nevertheless, the regulation represents a thoughtful and progressive extension of existing product safety legislation (for a critical overview, see Sousa e Silva, 2025, para. 11). The AI Act does not overrule but complements the existing legislation in different sectors (Evas, 2024, pp. 98, 99). Manufacturing processes, especially for innovative and complex systems, are inherently prone to errors. To address this, robust quality assurance and comprehensive risk management frameworks are indispensable. The regulation effectively incorporates these principles, ensuring that safety standards keep pace with technological advancements. Indeed, certain companies have expressed confidence in their ability to comply with the regulatory stipulations outlined by the AI Act. This confidence is rooted in their existing operational presence within a stringent regulatory framework, such as the Medical Devices Regulation. Consequently, these companies anticipate synergy effects that will facilitate their compliance with the requirements of the AI Act (Wagner et al., 2025, mn 663 et seqq).

A notable feature of the AI Act is its delegation of conformity assessments to the private sector. This approach leverages the empirical knowledge and expertise of industry actors while simultaneously alleviating the administrative burden on state institutions. However, this privatised model raises important questions, particularly from the user's perspective. For most users, the processes underlying market approval – whether through internal controls or official certifications – remain opaque. As a result, official certification may have limited impact on enhancing user confidence, as the distinction between internal and external oversight is rarely apparent or meaningful to end users.

REFERENCES

Evas, T. (2024). The EU Artificial Intelligence Act: Advancing innovation for Trustworthy AI. *Journal of AI Law and Regulation (AIRe)*, *1*(1), 98–101.

Hacker, P. (forthcoming atıfta 2023?). AI regulation in Europe: From the AI Act to future regulatory challenges. In J. Adams-Prassl and I. Ajunwa (Eds.), *Handbook on Algorithmic Governance and the Law*. Oxford University Press. https://arxiv.org/abs/2310.04072.

Leinarte, E. (2024). The Classification of High-Risk AI Systems Under the EU Artificial Intelligence Act. *Journal of AI Law and Regulation (AIRe)*, *3*(1), 262–280.

Linardatos, D. (2022). Auf dem Weg zu einer europäischen KI-Verordnung – ein (kritischer) Blick auf den aktuellen Kommissionsentwurf. *Zeitschrift für das Privatrecht der Europäischen Union (GPR)*, 58–70.

Linardatos, D. (2025). § 8. Qualitätskontrolle, Korrekturmechanismen und Code of Conduct. In E. Hilgendorf & D. Roth-Isigkeit (Eds.), *Die neue Verordnung der EU zur Künstlichen Intelligenz*, 2nd edition. CH Beck.

Mantelero, A. (2025). The AI Act: A realpolitik compromise and the need to look forward. In S. Simitis & I. Spiecker gen. Döhmann, L. Schertel Mendes & R. Campos (Eds.), *Digital Constitutionalism* (pp. 311–344). Nomos Verlagsgesellschaft.

Moretti, L., Rinaldi, L., & Schlosser, P. (Eds.) (2025). *Digital finance in the EU: Navigating New Technological Trends and the AI Revolution*. European University Institute.

Roth-Isigkeit, D. (2025). § 9. Konformitätsbewertungsverfahren, Organisation und Mittel der KI-Aufsichtsbehörden und Europäische KI-Governance. In E. Hilgendorf & D. Roth-Isigkeit (Eds.), *Die neue Verordnung der EU zur Künstlichen Intelligenz*, 2nd edition. CH Beck.

Sousa e Silva, N. (2025). The Artificial Intelligence Act: Critical overview. *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)*, *16*(1), 2.

Wagner, M., Song, Q., Borg, M., Engström, E., & Lysek, M. (2025). AI Act high-risk AI compliance challenge and industry impact: A multiple case study. SSRN. http://dx.doi.org/10.2139/ssrn.5221279.

ABOUT AUTHOR

Prof. Dr. Dimitrios LINARDATOS | Saarland University | dimitrios.linardatos[at]uni-saarland.de

Prof. Dr. Dimitrios Linardatos studied law at Philipps University of Marburg and completed his doctorate in 2013 at LMU Munich. After passing the Second State Examination, he worked as an attorney at Hengeler Mueller. From 2016 to 2021, he served as an Academic Councillor at the University of Mannheim and has been a lecturer at Mannheim Business School since 2020. Between 2021 and 2023, he held an interim professorship in Banking and Financial Market Law at the University of Liechtenstein. Since April 2023, he has been Professor of Civil Law, Law of Digitalization, and Business Law at Saarland University.