sciendo

Ius Novum

2025, vol. 19, no. 4, pp. 121–140

OBLIGATIONS OF IMPORTERS, DISTRIBUTORS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS UNDER THE AI ACT

KAROLINA KIEJNICH-KRUK*

DOI 10.2478/in-2025-0040

Abstract

The Artificial Intelligence (AI) Act distinguishes between the different actors involved in the supply chain of high-risk AI systems. The purpose of this paper is to outline and compare the obligations of importers, distributors and deployers, and to analyse the circumstances in which these obligations may be extended and aligned with those of providers of high-risk AI systems. The obligations of importers and distributors are primarily of a verification nature. In general, the obligations of distributors are more limited than those of importers, who bear the burden of primary verification of compliance by providers. In contrast, the obligations of deployers are generally not subordinate to those of providers but constitute an independent responsibility arising from the need to address the risks posed during the deployment phase of high-risk AI systems. A specific situation arises where interference with AI systems results in the imposition of obligations on a non-deployer that are equivalent to those imposed on providers of high-risk AI systems. This is because AI-based systems are, among other things, susceptible to changes in their purpose in ways that are independent of their design and the intentions of their providers. Proper identification and understanding of the responsibilities of the various actors in the supply chain are key to minimising the risks associated with the use of high-risk AI systems across the European Union and to avoiding the imposition of financial sanctions.

Keywords: AI Act; artificial intelligence; importers; distributors; deployers

* LLD, Assistant Professor at the Department of Criminal Procedure, Faculty of Law and Administration, Adam Mickiewicz University in Poznań (Poland), Judicial Assessor at the District Court in Jarocin, e-mail: kiejnich-kruk@amu.edu.pl, ORCID: 0000-0003-1551-5448

INTRODUCTION

The Artificial Intelligence Act[1] represents a breakthrough in the legal regulation of actors involved in the creation, supply and use of systems based on artificial intelligence (AI) technology, in particular those classified as high-risk systems. In doing so, the AI Act distinguishes between the various actors involved in the supply chain of these systems and imposes differentiated obligations upon them. The distribution of the burden and the scope of these obligations may, at times, be questionable.

Most analyses in this area, both domestically and internationally, focus on the obligations of providers, bearing in mind that they shoulder the majority of obligations under the AI Act and are the most extensively regulated.[2] However, it should not be overlooked that importers, distributors and deployers of high-risk AI systems also play an important role in the supply chain and in safeguarding fundamental rights, as well as in mitigating the risks associated with the implementation of these systems.

The purpose of this paper is to outline and compare the obligations of these three entities under the AI Act and to analyse the circumstances in which these obligations may be extended and aligned with those of providers of high-risk AI systems. In addition, the paper identifies how these entities can, in practice, fulfil their obligations and what the scope of those obligations is. These issues are not clear-cut, and sources of practical clarification remain limited. Given the frequency with which these questions arise and the constraints resulting from the format of this study, the discussion is confined to the most significant obligations and those that raise the greatest interpretative uncertainty in terms of the relevant provisions and their practical application.

OBLIGATIONS OF IMPORTERS

An importer is an entity that places on the market an AI system bearing the name or trademark of a natural or legal person whose registered office is located in a third country (Article 3(6)). 'Placing on the market' means making an AI system

[1] 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), PE/24/2024/REV/1 (OJ L 189, 12.7.2024), hereinafter referred to as 'the AI Act' or 'the Regulation'.

[2] See, *inter alia*, M. Jacobs, J. Simon, 'Assigning Obligations in AI Regulation: A Discussion of Two Frameworks Proposed by the European Commission', Digital Society, 2022, Vol. 1(6); L. Enqvist, '"Human oversight" in the EU artificial intelligence act: what, when and by whom?', *Law, Innovation and Technology*, 2023, Vol. 15, No. 2, pp. 508–535; L. Edwards, *The EU AI Act: a summary of its significance and scope*, pp. 7–8, 16; https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/ [accessed on 8 April 2025]; K. Hewson, E. Lu, *The roles of the provider and deployer in AI systems and models*, Stephenson Harwood, 2024; https://www.stephensonharwood.com/insights/the-roles-of-the-provider-and-deployer-in-ai-systems-and-models [accessed on 8 April 2025].

or AI model available for the first time on the EU market (Article 3(9)). 'A third country' is a country other than an EU Member State, as indicated in Article 2(1)(a), which presents EU Member States and third countries as alternative concepts. Typically, the third country will be the place of origin of the system's provider, which assigns its name to the system.

The obligations of importers are set out in Article 23 of the AI Act. The importer in the supply chain of high-risk AI systems plays a crucial role in relation to systems placed on the EU market and supplied by entities established in third countries. It acts as an intermediary between foreign providers and distributors or deployers within the EU. The importer assesses whether the provider has applied the standards required under the AI Act and whether the AI system concerned ensures compliance with EU requirements, thereby allowing it to be placed on the EU market.

It is necessary to consider what actions importers should take to comply with the obligations referred to in this provision. These include, in the first instance, verifying that the provider has complied with its obligations:

(1) to carry out the relevant conformity assessment procedure;
(2) to draw up the technical documentation;
(3) to affix the required CE marking and attach an EU declaration of conformity and an instruction manual; and
(4) to appoint an authorised representative.

The conformity assessment procedure is governed by Article 43 of the AI Act and is the responsibility of the provider to conduct. By contrast, the importer's task is to verify formally that the provider has fulfilled this obligation; the importer is not required to assess whether the procedure has been carried out correctly.[3] This verification can be undertaken by consulting the database established under Article 71 of the AI Act. According to Annex VIII, Section A, the database must contain information about the authorised representative, include copies of the EU declaration of conformity and the instructions for use, and provide information on certification. The EU declaration of conformity must state that the high-risk AI system concerned complies with the requirements set out in Section 2, including those relating to conformity assessment. The notion of 'adequacy' should relate to the form of the procedure, not to the quality of its execution. The conformity assessment procedure may be carried out in accordance with Annex VI or Annex VII. Where the conformity assessment procedure and the technical documentation are prepared in accordance with Annex VII, the results of the procedure are externalised in the form of a decision by the notifying body and a certificate. Consequently, verification is only possible by consulting the database referred to in Article 71 of the AI Act.

The obligation to verify whether the provider has prepared the technical documentation may likewise be fulfilled by consulting the database created under Article 71 of the AI Act.[4] The duty is to verify formally that such documentation exists, rather than to assess its accuracy.

---

[3] L. Riede, O. Talhoff, 'Article 23', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, 2024, p. 510.

[4] See Annex VIII, Section A.

The obligations to affix the required CE marking to the system and to include an EU declaration of conformity and an instruction manual rest with the provider. The first two are specified in Article 16(1)(g) and (h), while the third – the instruction manual – forms part of the technical documentation referred to in Article 11(1).[5] The importer is required to verify formally that the provider has complied with these obligations. It is also possible to verify the existence of the EU declaration of conformity and the instruction manual by consulting the database established pursuant to Article 71 of the AI Act.[6] With regard to verification of the CE marking, guidance is provided by Article 48(3), which stipulates that the marking shall be affixed to the AI system in a visible, legible and indelible manner. If, owing to the nature of the high-risk AI system, it is not possible or reasonable to label the system in this way, the marking shall be affixed to the packaging or, where appropriate, to the accompanying documentation.

The provider's obligation to appoint an authorised representative is laid down in Article 22. The importer's duty is limited to verifying that such a representative has been appointed. This verification is performed by consulting the database, in which information about the representative must be recorded.[7]

It is good practice to draw up a verification protocol in which importers indicate the measures taken to verify the provider's compliance with EU regulations and, if necessary, attach relevant documents (for example, printouts from the database or photographs).

Obligations are also imposed on importers to refrain from certain actions. According to Article 23(2) of the AI Act, if an importer has sufficient reason to believe that a high-risk AI system does not comply with the Regulation, or that it or its documentation is falsified, the importer shall not place such a system on the market until it has been ensured that the system complies with the Regulation. This is therefore an absolute prohibition.

A question that must be answered is what constitutes 'sufficient reasons' for believing that a product has been supplied with falsified documentation or does not comply with EU requirements. The importer's positive obligations to verify systems are set out in paragraph 1 of the provision, as previously discussed. However, the importer may – but is not required to – undertake additional verification activities when assessing the compliance of the provider's actions and the system's conformity with EU standards. For example, the importer may obtain relevant information from media reports or whistleblowers. If such information indicates that a high-risk AI system poses a risk within the meaning of Article 79(1), the importer must notify the authorities indicated in that provision and suspend the import process. The process of placing the system on the market may resume once the dossier has been completed or amended, the relevant procedures have been finalised, or – although this case is not expressly provided for in the Regulation – when it is

5 See Annex IV, point 1(h).
6 See Annex VIII, Section A.
7 Ibidem.

established that the importer's objections were unfounded, for example, due to an incorrect conformity assessment.

An important obligation is also provided in Article 23(6) of the AI Act. This article specifies the nature of the cooperation expected from importers in relation to the competent authorities. According to this provision, importers are required, upon a reasoned request, to provide the authorities with all necessary information and documentation. The notion of a competent authority relates to the supervision of the standards set out in Articles 8–15. These entities include national market surveillance authorities,[8] authorities responsible for the protection of fundamental rights,[9] and the EU authority – the AI Office. Sectoral bodies will also be involved, such as data protection supervisory authorities.[10]

It must be recognised that an inappropriate legislative technique has been applied here, namely the use of different terms to describe identical concepts. The expressions 'competent national authorities' and 'relevant national authorities' should be synonymous in meaning (this is also the case in other language versions, such as Polish). In several other linguistic versions these terms are identical – for instance, *autorités compétentes* (French), *autoridades competentes* (Spanish), and *autorità competente* (Italian). These expressions are synonymous and should be interpreted as referring to the same concept.

The concept of a 'reasoned request' must be linked to the competence and duties of the authorities concerned. This means that the purpose of obtaining information or documentation from importers must relate to the authority's intention to fulfil its statutory obligations. These will primarily be supervisory functions, the proper performance of which requires a range of information concerning the operation of a high-risk AI system.

The purpose of establishing the obligation to cooperate is to demonstrate that the high-risk AI system complies with the requirements set out in Section 2. These are as follows:

(1) the establishment of a risk management system,[11]
(2) proper data management,[12]
(3) preparation of technical documentation,[13]
(4) event logging,[14]
(5) transparency of operations and the provision of information to deployers,[15]
(6) human oversight,[16] and
(7) achievement of accuracy, robustness, and cybersecurity in the systems applied.[17]

---

[8] See Article 74.
[9] See Article 77.
[10] See recital 10 of the Preamble.
[11] See Article 9.
[12] See Article 10.
[13] See Article 11.
[14] See Article 12.
[15] See Article 13.
[16] See Article 14.
[17] See Article 15.

The AI Act does not specify the scope of the information or documents subject to the obligation to provide them. In the absence of a regulatory limitation, all information and documentation that the competent authority may require to assess the compliance of a high-risk AI system with the requirements set out in Section 2 of the Regulation are subject to the obligation of transmission. This information and documentation must be provided in a language easily understood by those authorities. The term should refer to the relevant language version.[18] In the case of national authorities, this will be the official language of the country concerned (or another, if the authority so indicates). In the case of EU bodies, reference should be made to the rules of procedure of those institutions.[19] If language requirements are not specified, any of the 24 official EU languages should be considered acceptable.[20]

Article 23(7) of the AI Act also imposes a general obligation on importers to cooperate with the relevant national authorities, including market surveillance authorities (in the field of AI as well as sectoral authorities, such as those responsible for personal data protection or competition rules) and other authorities for the protection of fundamental rights. Importers are required to cooperate with these authorities concerning any actions undertaken by them in relation to the high-risk AI system supplied by the importer. The aim of these measures is, in particular, to reduce or limit the risks posed by such systems. Certain cooperation obligations are specified in other provisions of the Regulation, for example those concerning the provision of documentation and information, as well as notification obligations. Paragraph 7 should therefore be understood as imposing a general obligation on importers to cooperate beyond the specific duties expressly detailed in the Regulation. At the same time, the provisions do not set out a catalogue of actions with which importers are obliged to cooperate. The duty to cooperate extends to any action undertaken by the authority concerned that falls within its competence. In other words, an importer may refuse to cooperate only if the authority's request to take a specific action (or omission) concerns a matter that lies beyond its competence.

Failure to comply with the obligations referred to above is subject to an administrative fine, the amount of which is specified in Article 99.

OBLIGATIONS OF DISTRIBUTORS

The obligations of distributors of high-risk AI systems are laid down in detail in Article 24. These are mainly verification obligations. The distributor acts as an intermediary (most often as a vendor or service provider) and does not influence the design of AI systems or their subsequent use. Consequently, its responsibilities

---

[18] L. Riede, O. Talhoff, 'Article 23', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU*…, op. cit., p. 513.

[19] In accordance with Article 6 of Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385), hereinafter referred to as 'the Regulation No 1', the institutions may lay down detailed rules for the use of the language regime in their rules of procedure.

[20] See Article 1 of Regulation No 1.

in providing high-risk AI systems are considerably less extensive than those of providers and deployers. The verification duties of distributors are also more limited than those of importers and are of a more formal nature.

It is the distributor's responsibility to verify that the other entities involved in the supply chain of a high-risk AI system have properly fulfilled their obligations, as provided in Article 16(b) and (c) and Article 23(3) of the AI Act, respectively. The provider or importer (in cases where the high-risk AI system is placed on the market from a third country) is required to confirm to the distributor that the high-risk AI system includes:

(1) CE conformity marking,
(2) copies of the EU declaration of conformity,
(3) instructions for use,
(4) information on the AI system, on its packaging or in the accompanying documentation, indicating the name, registered trade name or registered trademark and the address at which the provider or importer can be contacted, and
(5) a quality management system that complies with Article 17.

Once again, it is good practice to prepare a verification protocol in which distributors record the measures taken to verify the provider's compliance with EU regulations and, if necessary, attach relevant documentation (for example, a database printout or photographs).

The verification of part of the data is carried out by checking the database established under Article 71. According to Annex VIII, Section A, the database must contain information on the authorised representative, include copies of the EU declaration of conformity and the instructions for use, and contain certification details and provider information. Information concerning the CE marking must be verified by the distributor in the database of the relevant certification body. A copy of the declaration of conformity should be presented to the distributor, along with confirmation that the provider has an appropriate quality management system in place. The quality management system takes the form of written policies, procedures and instructions;[21] therefore, a copy may be shown. The distributor can verify the existence of information relating to the provider and importer by inspecting the system's packaging, the accompanying physical documentation, or by reproducing the documentation under test conditions in the case of electronic documentation or information incorporated within the system itself.

Under Article 24(2), a distributor is obliged not to make a high-risk AI system available if, in its assessment, the system does not meet the requirements set out in Section 2 of Chapter III (Articles 8–15). As with importers and their corresponding obligation of omission, this provision should be understood to mean that the distributor's obligation to perform a positive verification is limited solely to checking that the AI system possesses the necessary documents and required features. This obligation does not extend to verifying whether the system in fact meets the substantive requirements of Articles 8 to 15 of the AI Act. It may be assumed that obtaining a CE certificate and an EU declaration of conformity signifies that the

[21] See Article 17.

system complies with those requirements. However, this assumption may prove to be unfounded. If the distributor obtains information – from any source – indicating that the AI system may not comply with these requirements (and such information need not be confirmed; a reasonable assumption suffices), the distributor must not make the AI system available.

As in the case of importers, such information may originate, for instance, from media reports (for example, when it is revealed that a particular provider does not design high-risk AI systems in accordance with data collection requirements for training) or from whistleblowers. It is also possible that a distributor may undertake verification activities beyond those required by law, and the results of those activities may provide grounds to believe that the system does not meet the prescribed requirements.

It has been aptly noted in the legal doctrine[22] that this obligation is more limited than that imposed on importers. This may be explained by the fact that distributors typically have less detailed insight into the functionality of AI systems and less direct contact with the providers of high-risk AI systems. It has also been observed that, in practice, Article 23(2) may be interpreted as a stricter version of Article 24(2); however, it is debatable whether this is in fact the case. If the distributor does not have a 'sufficient' reason for concern, it can hardly be expected to take targeted action to refrain from making the system available on the market.[23]

A specific obligation of the distributor arises where a high-risk AI system poses a risk within the meaning of Article 79(1).[24] In such a situation, the distributor shall inform the provider or the importer of the system, as the case may be, of the existence of that risk. Against the background of this obligation, the question arises as to whether the distributor has a positive duty to act to verify the existence of such a risk, or whether, as with the other requirements listed in paragraph 2, the obligation to provide information arises only when the distributor becomes aware of such a circumstance, without being under a duty to actively seek it. Given that this obligation is provided for in Article 24(2) and not in paragraph 1, the absence of its inclusion in the closed catalogue of duties in paragraph 1 should be interpreted to mean that there is no positive obligation to verify whether a system poses the risk referred to in Article 79(1). Obtaining the CE marking and the declaration of conformity should, in principle, exclude the existence of such a risk. However, it may occur that once the system has been labelled, certain characteristics or forms of use are revealed that justify considering it as a product posing a risk to health, safety or the fundamental rights of individuals.

The procedure for identifying a product as posing a risk, and for undertaking corrective action and notification, is carried out by the supervisory authority. By interpreting the phrase 'poses a risk', which employs the indicative rather than the conditional mood (as in the case of other risks described in this provision), it may

---

[22] L. Riede, O. Talhoff, 'Article 24', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence*…, op. cit., p. 521.

[23] T. Fülöp, P. Poindl, 'Article 27', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence*…, op. cit., p. 522.

[24] See Article 79.

be concluded that confirmed knowledge is required in this regard; that is, it cannot rest merely on a reasonable assumption. In this context, the 'creation of a risk' refers to an abstract hazard. It is not necessary that harm be caused to any entity, nor is it necessary to establish certainty that a risk to health, safety or fundamental rights will materialise. This means that any non-compliance of the system – arising, for instance, from the processing, collection or selection of data – may be likely to adversely affect rights such as privacy, non-discrimination or personal data protection, regardless of whether those risks actually materialise or whether any damage results.

Article 24(3) makes distributors responsible for the high-risk AI system for as long as it remains in their possession. Regardless of whether the system is stored in digital or tangible form, if it is modified or if AI Act compliance assessments become outdated, responsibility lies with the distributor. In this context, cybersecurity obligations are of particular significance. It is necessary to take proactive measures, similar to those required of providers,[25] aimed at preventing unauthorised third-party access to the system that could alter its use or affect its results or operational effectiveness by exploiting vulnerabilities. The distributor bears responsibility for the ineffectiveness of any such measures.

The obligations set out in Article 24(4) mirror those provided for in paragraph 2, although they concern situations in which irregularities have already been identified after the high-risk AI system has been made available. As the likelihood of threats to the rights of users increases in such cases, the obligations of the distributor are correspondingly greater. The distributor is required to take the corrective measures necessary to ensure that the high-risk AI system complies with the requirements set out in Section 2, to withdraw it from the market or from use, or to ensure that such corrective measures are taken by the provider, importer or relevant operator, as appropriate. This obligation corresponds to that imposed on providers under Article 20.

Corrective measures are actions aimed at bringing a high-risk AI system into compliance with the requirements set out in Articles 8–15. Consequently, they require the identification of non-compliance and the modification of the system in such a way as to achieve conformity.[26] By analogy with paragraph 2, the distributor is obliged to inform the provider or importer of the system, as well as the competent authorities, when a high-risk AI system poses a risk to health, safety or fundamental rights.

The obligations laid down in paragraphs 5 and 6 duplicate those of importers as set out in Article 23(6) and (7), although they are phrased somewhat differently. Once again, failure to comply with these obligations is subject to the imposition of an administrative monetary penalty.[27]

---

[25] See Article 15.
[26] See Article 20.
[27] See Article 99.

OBLIGATIONS OF ENTITIES USING HIGH-RISK AI SYSTEMS

The obligations of entities applying high-risk AI systems are mainly set out in Article 26 of the AI Act. For those applying high-risk AI systems (referred to as deployers), the EU legislature imposes – immediately after providers – a significant number of obligations. Importantly, the notion of an applying entity is not synonymous with that of a person using or benefiting from the system.[28] The obligations provided for in this provision in the case of the use of AI systems in recruitment processes are imposed, for example, on the entrepreneur and not on the employee from the human resources department who operates the system (software).

As indicated in recital 93 of the Preamble, the risks associated with AI systems may arise from the manner in which they are used. Therefore, entities deploying high-risk AI systems play a key role in ensuring the protection of fundamental rights, supplementing the obligations of the provider during the system's development. These entities understand how the high-risk AI system will be used and are able to identify potential risks that were not foreseen at the design stage.

The provisions of Article 26(1)–(4) impose the following obligations on those deploying high-risk AI systems:

(1) to take technical and organisational measures to monitor the compliance of the AI system with the operating instructions;
(2) to entrust supervision to individuals who possess the necessary competence, training and authority, as well as adequate support; and
(3) to the extent that they have control over the input data, to ensure the adequacy and sufficient representativeness of such data with regard to the purpose of the high-risk AI system.

Technical and organisational measures aimed at monitoring compliance of the AI system with the user manual may include, for example, the establishment of appropriate procedures to be followed whenever an anomaly is detected by a user, regular internal audits to verify compliance with the manual, periodic staff training, or the introduction of automatic alerts in cases where the results significantly deviate from the average.

Supervisory responsibilities entail the introduction of a principle of *human-on-the-loop* control over system operation, rather than active *human-in-the-loop* participation.[29] This means that the human role is to oversee the functioning of the system rather than to actively interact with it – for example, by continuously providing feedback on the accuracy of the results as part of an ongoing learning process. At the same time, such supervision must be genuine and not merely formal. The supervisor must possess appropriate competence, training and authority, that is, knowledge and experience regarding the operation of high-risk AI systems, the applicable standards and the risks associated with their violation, the potential for irregularities, and the correct responses to their detection. It is advisable

[28] See Article 3(4).

[29] R. Pinto, T. Mettler, M. Taisch, 'Managing supplier delivery reliability risk under limited information: Foundations for a human-in-the-loop DSS', *Decision Support Systems*, 2013, Vol. 54, Issue 2, pp. 1076–1084.

for supervisors to rotate periodically, since research indicates that individuals often become fatigued or distracted when working with autonomous systems.[30] Consequently, they cannot maintain effective supervision of AI systems for extended periods without an increased risk of undetected anomalies. This is also related to the psychological tendency of individuals to assume that such systems cannot fail or make errors – a presumption that is frequently incorrect.[31]

With regard to input data, the applying entity is obliged to ensure the adequacy and sufficient representativeness of the input data in relation to the purpose of the high-risk AI system. Input data refers to data provided to, or directly extracted by, the AI system from which it generates results.[32] As a general rule, the architecture of the system determines what input data must be provided in order to produce a given output. For example, in recruitment systems, the relevant data will include information concerning education. However, the inclusion of data on race could lead to outcomes that appear discriminatory. It appears that the requirement for data representativeness will not apply to all instances of high-risk AI system deployment. Job centres or private recruiters, for example, have no control over who chooses to apply for a given position (for instance, whether the applicants will all be women).

A case study concerning the use of such a system by public administration should be mentioned. In May 2014, the Polish Ministry of Labour and Social Policy introduced an automated decision-making system aimed at tackling unemployment by categorising jobseekers into three distinct groups based on specific characteristics.[33] The categorisation process began with a computer interview, after which various factors were entered into a database, with each factor assigned a particular score. The system took into account two key variables: 'distance from the labour market' and 'readiness to enter or re-enter the labour market'. These criteria assessed factors that hindered entry into employment, such as gender, age and education. The system has been subject to considerable criticism due to its lack of transparency, data protection concerns, potential discriminatory effects and the absence of genuine human oversight.[34] The provisions enabling the use of the system were examined by the Constitutional Court in relation to the lack of a legal remedy and the question of whether the system had been correctly regulated by means of a regulation.[35] The Court held that profiling does not constitute a case, decision or ruling within the meaning of the Constitution. The mere collection or processing of data does not determine the

---

[30] R. Weitkunat, M. Bestle, 'Computerized Mackworth vigilance clock test', *Computer Methods and Programs in Biomedicine*, 1990, Vol. 32, Issue 2, pp. 147–149.

[31] Ibidem, pp. 147–149.

[32] See Article 3(33).

[33] Ministry of Labour and Social Policy, *Profilowanie pomocy dla osób bezrobotnych. Podręcznik dla pracowników powiatowych urzedów pracy*, 2014; https://panoptykon.org/sites/default/files/podrecznik_profilowania.pdf [accessed on 5 February 2025].

[34] J. Niklas, K. Sztandar-Sztanderska, K. Szymielewicz, *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Warszawa, 2015, p. 33; https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf [accessed on 5 February 2025]; K. Sztandar-Sztanderska, M. Zielenśka, 'When a Human Says "No" to a Computer: Frontline Oversight of the Profiling Algorithm in Public Employment Services in Poland', *Sozialer Fortschritt*, 2022, Vol. 71, No. 6, p. 468.

[35] Judgment of the Constitutional Court of 6 June 2018, K-53/16, *OTK-A*, 2018/38.

legal situation of an individual. For this reason, it was held that, despite the absence of a means to challenge the act of determining a profile for an unemployed person, the provisions were compatible with Article 45(1) and Article 78 of the Constitution. However, the Court concluded that the appropriate form of regulation should be a statute rather than a regulation.

Furthermore, Article 26(5) reiterates the obligation to monitor the compliance of system use with the user manual, supplementing it with the duty to provide the system provider with data concerning the performance of the high-risk AI system.[36] Where appropriate, this may also include data necessary for analysing interactions with other AI systems. The AI Act does not specify the form of data transmission, its timing, frequency or on whose initiative – the provider's or the deployer's – the data should be transmitted. Nevertheless, it should be assumed that the transmission of data should take place on a durable medium, either electronic or paper, or in the form of an electronic or paper document. The frequency of data transmission should correspond to the monitoring plan established by the provider on the basis of the template developed by the Commission pursuant to Article 72(3) of the AI Act. The deployer is required to collect the data on an ongoing basis (a duty implied by the relevant provision) and to transmit it to the provider without undue delay.[37]

In the event that deployers identify the occurrence of a serious incident, they shall immediately inform the provider, followed by the importer or distributor, and the relevant market surveillance authorities. Pursuant to Article 3(49) of the AI Act, a serious incident means an incident or malfunction of an AI system that directly or indirectly results in any of the following events:

(a) the death of a person or serious harm to a person's health,
(b) serious and irreversible interference with the management or operation of critical infrastructure,
(c) a breach of the obligations provided for in Union law that are intended to protect fundamental rights, or
(d) serious damage to property or to the environment.

If the deployer is unable to contact the provider, the EU legislature requires the corresponding application of Article 73 of the AI Act. In such a case, the deployer is obliged to notify the market surveillance authorities of the Member State in which the incident occurred. Notification must be made immediately, and, in any case, no later than 15 days after the deployer becomes aware of the serious incident; and in the case of a serious and irreversible disruption to the management or operation of critical infrastructure, no later than two days after the operator becomes aware of that incident. These time limits define the period between becoming aware of the incident and notifying the authority. Accordingly, the provider's response to the deployer's notification must occur more swiftly; otherwise, the deployer must notify the authority within the deadline. This will be particularly demanding in the case of the two-day deadline; however, it appears that the deployer may notify the authorities almost simultaneously with the provider if the latter fails to respond

[36] See Article 72(2).
[37] See Article 72.

immediately. It should also be recalled that such an obligation, in any case, already rests with that deployer.

With regard to entities that are financial institutions subject to requirements concerning their internal management systems, arrangements or procedures under Union financial services law, the monitoring obligation shall be deemed fulfilled where the financial institution complies with the relevant provisions of that law. The AI Act thus establishes an exception for financial institutions (primarily banks), exempting them from the obligation to report provider data or to inform entities of significant risks or serious incidents, provided they are already subject to requirements relating to internal management systems, arrangements or procedures under EU financial services legislation. This exception exists because such regulations already impose analogous obligations, and financial institutions are strictly supervised by the competent authorities in this respect.

Accordingly, information on risks or incidents will still be transmitted, but through the specific procedures applicable to financial institutions, such as those provided for in Article 96 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC; and in Article 17 et seq. of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the operational digital resilience of the financial sector, amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011).

Paragraph 6 requires those deploying high-risk AI systems to retain the event logs that are automatically generated by the system. The retention period should be no less than six months, unless otherwise provided by other provisions. According to Article 16(e), event logs shall be kept by providers for as long as the logs remain under their control. The provision in Article 25(6) thus complements this regulation by indicating that, when the logs are under the control of the deployer, it is the deployer's responsibility to store the event records for a specified period.[38] It is more likely that such records will be under the control of the deploying entity when the AI system is operated within its own infrastructure. It is less likely that such records will fall under its control when the AI system is provided as an external service (outsourcing).

A specific obligation is imposed by Article 26(8) on deployers of high-risk AI systems that are public bodies or institutions, or bodies and agencies of the Union. They are required to register as referred to in Article 49. Indeed, pursuant to Article 49(3), deployers must register themselves, select the relevant system and register its use in the EU database referred to in Article 71, even before putting into use or operating a high-risk AI system listed in Annex III. Excluded from this obligation are AI systems constituting critical infrastructure, that is, AI systems intended for use as safety process elements in the management of critical infrastructures, such as digital networks, traffic systems and processes, or in their operation or in the

[38] See Article 19.

supply of water, gas, heat or electricity. Unlike providers, deployers do not register the system itself but only themselves as deployers.

The expression 'before commissioning' is not entirely clear, since the commissioning of an AI system is carried out by the provider. According to Article 3(11) of the AI Act, 'commissioning' means the delivery of an AI system for first use directly to the deployer or for its own use within the Union in accordance with its intended purpose. A situation referred to in Article 25 may arise in which a deployer modifies a system in such a way that it becomes classified as a system provider. In that case, it would be subject both to the obligations of providers with regard to commissioning and to those of deployers concerning use.

If deployers establish that a high-risk AI system they intend to use has not been registered in the EU database referred to in Article 71, they shall refrain from using that system and shall inform the provider or distributor accordingly. The deploying entity is obliged to abstain from using the system until it has been registered in the EU database. The AI Act does not specify the form or timing of the provision of such information; however, it should be assumed that this must be done without undue delay and in a manner that allows the fact of the notification to be recorded.

As with other actors in the supply chain, paragraph 12 introduces a general obligation to cooperate with the relevant authorities in any actions these authorities undertake in relation to the high-risk AI system for the purpose of implementing the AI Act. All the observations made concerning the obligations of importers and distributors in this respect apply here as well. Failure to comply with the obligations laid down in Article 26 of the AI Act is subject to an administrative fine.[39]

The provisions of the AI Act also impose another, in principle, key obligation on deployers – namely, to assess the impact of high-risk AI systems on fundamental rights, as provided for in Article 27. A discussion of this issue lies beyond the scope of this paper; however, unlike other obligations, it has been the subject of doctrinal analysis that may serve as guidance for practitioners and deployers.[40]

ASSUMPTION OF PROVIDER OBLIGATIONS

Article 25 of the AI Act regulates the modification of liability for high-risk AI systems in certain circumstances. Paragraph 1 sets out the situation in which, after the marketing or commissioning of a high-risk AI system, an entity other than the original provider interferes with the system in such a way that – by the intention of the legislature – it results in the assumption of the responsibilities and obligations of the system provider.

The inclusion of this provision stems from the fact that operators may use AI systems available on the market, modify them and, in doing so, effectively create a new system, for example, one tailored to the profile of a specific business.

[39] See Article 99.

[40] See, *inter alia*, A. Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template', *Computer Law & Security Review*, 2024, No. 54, and sources cited therein.

The original system then serves as the foundation for the functioning of the modified system.

The personal scope of the provision encompasses distributors, importers, deployers or other entities. It appears that the term 'third party' should be understood as referring to any entity undertaking the activities described in paragraph 1. This term should not, however, be equated with the term 'third party' used elsewhere in the AI Act to refer to an entity performing the conformity assessment.[41]

The actions that result in the transfer of responsibility for a high-risk AI system are listed in Article 25(1). These actions – by a distributor, importer, deployer or other third party – include:

(1) the inclusion by one of these entities of its name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements providing otherwise for the sharing of responsibilities;
(2) making a material change to a high-risk AI system already placed on the market or put into service, such that it remains a high-risk AI system; and
(3) changing the purpose of an AI system, including a general-purpose AI system that is not classified as a high-risk AI system and that has already been placed on the market or put into service, in such a way that the AI system concerned becomes a high-risk AI system.

The first action concerns the inclusion of a name or trademark on a high-risk AI system, without prejudice to contractual arrangements providing for a different allocation of responsibilities. The final part of the provision means that the parties (the original provider and the distributor, importer, deployer or other third party) may agree that, despite the labelling, liability and the status of provider are not transferred to another party. By applying *a contrario* interpretation to the last sentence of paragraph 2, it should be assumed that if the indications are affixed in a manner contrary to such an agreement, responsibility as provider is transferred to the party introducing the indications. However, that party remains liable to the original provider for conduct contrary to the agreement. This regulation therefore has a protective function for users and an indirect sanctioning function for those who introduce the labelling.

The second action concerns making a substantial change to the system, such that it remains a high-risk AI system. The notion of a 'substantial change' is defined in Article 3(23). The EU legislature has not provided examples of situations falling within this definition. Creating such a list would be difficult due to the considerable diversity of systems classified as high-risk AI systems. In particular, substantial changes will relate to modifications of the system's purpose (such as the broadening or narrowing of its scope; a mere alteration in the types of results obtained will not constitute a substantial change) or changes that significantly affect the system's operation (e.g., the scope of validation data used, the method of data processing, processing rules, or rules of human supervision). Other, non-substantial changes do not have the consequences described in the provision, although they still need to be assessed in light of the contractual arrangements between the provider and the

[41] See Article 3(21).

modifier, as well as under EU and national product safety and market surveillance regulations in this area.

The third action concerns changing the purpose of any AI system in such a way that the system in question becomes a high-risk AI system. No requirement of materiality is expressly imposed here; however, it should be assumed that any change that alters the system's classification constitutes a material change. This means that if any modification results in an AI system that was not previously classified as high-risk becoming so classified, the modifier acquires the status, duties and responsibilities of a provider.

A literal interpretation indicates that contractual agreements may exclude the consequences of actions provided for in the provision only in the case referred to in Article 25(1)(a). This result is also supported by a purposive interpretation. The purpose of the provision is to preserve legal certainty.[42] Consequently, end users, supervisory authorities and operators should not be in doubt as to which entity bears the obligations of the provider. In cases where contractual arrangements exist, this certainty is significantly diminished if the contracts are not public, are subject to national restrictions, or are potentially contentious between the parties. Thus, it cannot be maintained that a purposive interpretation supports a uniform reading of Article 25(1)(a)–(c) with respect to the possibility and extent of contractual sharing of obligations.[43]

In the situations described above, the modifier assumes the obligations of the provider as laid down in Article 16 of the AI Act.

Paragraph 2, in turn, provides that if the modifier is deemed to be the provider in accordance with paragraph 1, the original provider is no longer regarded as the provider of that specific AI system. Nevertheless, this provision also establishes certain obligations for the original provider. The original provider is required to make the necessary information available and to provide the reasonably expected technical access and other support necessary to ensure compliance with the obligations of the provider under the AI Act, particularly those relating to the criteria for assessing the compliance of high-risk AI systems.

This provision does not in any way specify the scope of the original provider's obligations, using vague concepts such as 'necessary' and 'reasonably expected', as well as an open catalogue of duties ('other support'). Given these interpretative difficulties, the obligations to provide informational or technical support should be regarded as limited strictly to those imposed on the new provider (the modifier). These will primarily include information on the functioning of the system, models or components used, training data, validation data, technical documentation, conformity assessment, certificates and labels, and compliance with the requirements of the AI Act. Verification of certain data may be carried out by consulting the database established under Article 71 of the AI Act. According to Annex VIII, Section A, the database must include information on the authorised representative,

---

42 See recital 84 of the Preamble.

43 L. Riede, O. Talhoff, 'Article 25', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence…*, op. cit., p. 531.

attached copies of the EU declaration of conformity and the user manual, as well as information on certification. However, the extraction of other data requires the cooperation of the original providers.

For example, it may occur that a competent national authority requests information from a new provider under Article 21(1). However, the latter may not possess all the necessary information, since some of the events covered by the request may have taken place prior to the modification of the system within the meaning of paragraph 1. Without this information, the provider cannot properly assess certain risks. Therefore, the provider shall request such information from the original provider in order to obtain complete data, analysis or assessment.

The request for cooperation must not extend beyond the information and support necessary for the proper fulfilment of the obligations under the AI Act which the new provider cannot obtain using its own personal, technical or financial resources – or where doing so would entail a disproportionate effort compared to the effort required from the original provider to transfer the relevant data or support. In particular, the duty to cooperate does not apply to the transfer of information, access or other forms of support that are not required for compliance with the AI Act, but are instead directed towards the economic development of the new provider, the acquisition of know-how or technological support, or the substitution of its own resources (knowledge, means, time, personnel) for those of the original provider.

Article 25(4) of the AI Act regulates the obligation to conclude a contract between the provider of a high-risk AI system and a third party supplying an AI system or other goods or services for that system, to enable the proper performance of the obligations set out in the Regulation. The provision introduces a concept not found elsewhere in the Regulation – namely, that of a third party providing an AI system with tools, services, components or processes used in, or integrated with, a high-risk AI system. These persons include all entities that supply the goods or services referred to in the provision to the high-risk AI system in question. The provision requires the provider to enter into written agreements with such entities. The question arises as to which entities supply these components and, consequently, with whom the contracts should be concluded – whether with the manufacturer, supplier or possibly a distributor with whom the supplier has a contractual relationship. It should be considered that the relevant entity is the supplier. Indeed, the provision does not refer to a 'third-party manufacturer' or a 'third-party distributor', but to a 'third-party supplier'.

An exemption from this obligation applies to third parties that make tools, services, processes or components available to the public under a free, open software licence, provided these are not purpose-built AI models. This means that a provider using such goods or services is not required to conclude the contract referred to in the first sentence of the provision. Recitals 102 and 103 of the AI Act clarify the meaning of a free and open licence.[44] Such software will generally be distributed in source code form through open repositories. According to recital 89 of the Preamble,

[44] See recitals 102 and 103 of the Preamble.

the purpose of this exemption is to relieve those working under free and open licences from liability throughout the value chain.

An example of a repository that publishes source code for algorithms under an open licence is MIT. Excluded from this exception are general-purpose AI models as defined in Article 3(63) of the AI Act. Thus, the provision distinguishes between a system and a general-purpose AI model. While the popular ChatGPT constitutes a system, a model would be, for example, GPT-4o.

The second paragraph of the provision states that the AI Office may develop and recommend voluntary model contractual provisions for agreements between providers of high-risk AI systems and third parties. These model contracts will remain non-binding and are likely to be highly general, given the specific characteristics of the industries to which such contractual provisions will apply. Nonetheless, they will undoubtedly embody sound contractual practices that may serve as valuable guidance on how to draft agreements that comply with the requirements of the AI Act. It will, however, be necessary to adapt such templates to the particular features of the high-risk AI regime, its purpose, its application, its users and the relevant industry.

CONCLUSION

In conclusion, identifying the role an actor plays in the supply chain of high-risk AI systems is of fundamental importance. The EU legislature has placed a significant burden of verification on importers and distributors. Most of this burden concerns the obligations of providers and the need to verify that providers are complying with their own responsibilities. The obligations imposed on importers and distributors primarily involve the formal verification that a particular procedure or task has been carried out, without requiring an analysis of whether it has been performed correctly. The provisions concerning the obligations imposed on importers and distributors are largely similar. Although certain differences in wording exist, these should not, in practice, lead to significant discrepancies in their application. Nevertheless, it remains the case that the obligations of distributors are generally more limited than those of importers, who bear the primary burden of verifying compliance. This is because the relationship between importer and provider is, in principle, closer than that between distributor and provider.

The situation differs for entities deploying high-risk AI systems. The obligations imposed on such entities are not usually subordinate to those of providers. They consist of independent responsibilities arising from the need to address the risks inherent in the deployment phase of high-risk AI systems. The EU legislature has assumed – rightly, it appears – that violations of fundamental rights may occur at this stage, even when the obligations intended to minimise such risks have been properly fulfilled during the development and distribution stages of high-risk AI systems. Indeed, deployers exert a crucial influence on how these systems are ultimately used, how data are protected, how results are utilised or verified, and on the procedures governing their use.

There exists a particular situation in which interference with AI systems results in the imposition of obligations on a non-provider equivalent to those of providers of high-risk AI systems. This stems from the fact that AI-based systems are, among other things, susceptible to changes in their purpose in ways that are independent of their design and of the intentions of their providers. In such circumstances, it is not justified to hold providers responsible for ensuring compliance with the requirements of the AI Act. It should, therefore, always be borne in mind that the responsibilities of importers, distributors and deployers may evolve depending on the circumstances and, in certain cases, may be equivalent to those of providers of high-risk AI systems.

BIBLIOGRAPHY

Edwards L., *The EU AI Act: A summary of its significance and scope*, Ada Lovelace Institute; https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer--The-EU-AI-Act-11-April-2022.pdf [accessed on 8 April 2025].

Enqvist L., '"Human oversight" in the EU Artificial Intelligence Act: What, when and by whom?', *Law, Innovation and Technology*, 2023, No. 2.

Fülöp T., Poindl P., 'Article 27', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, 2024.

Hewson K., Lu E., *The roles of the provider and deployer in AI systems and models*, Stephenson Harwood, 2024; https://www.stephensonharwood.com/insights/the-roles-of-the-provider-and-deployer-in-ai-systems-and-models [accessed on 8 April 2025].

Jacobs M., Simon J., 'Assigning Obligations in AI Regulation: A Discussion of Two Frameworks Proposed by the European Commission', *Digital Society*, 2022, Vol. 1(6).

Judgment of the Court of 6 June 2018, K-53/16, OTK-A 2018/38.

Mantelero A., 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template', *Computer Law & Security Review*, 2024, No. 54.

Ministry of Labour and Social Policy, *Profilowanie pomocy dla osób bezrobotnych. Podręcznik dla pracowników powiatowych urzędów pracy*, 2014; https://panoptykon.org/sites/default/files/podrecznik_profilowania.pdf [accessed on 5 February 2025].

Niklas J., Sztandar-Sztanderska K., Szymielewicz K., *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Warszawa, 2015; https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf [accessed on 5 February 2025].

Pinto R., Mettler T., Taisch M., 'Managing supplier delivery reliability risk under limited information: Foundations for a human-in-the-loop DSS', *Decision Support Systems*, 2013, Vol. 54, Issue 2.

Riede L., Talhoff O., 'Article 23', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence (AI) Act: A commentary*, Alphen aan den Rijn, 2025.

Riede L., Talhoff O., 'Article 24', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence (AI) Act: A commentary*, Alphen aan den Rijn, 2025.

Riede L., Talhoff O., 'Article 25', in: Pehlivan C.N., Forgó N., Valcke P. (eds), *The EU Artificial Intelligence (AI) Act: A commentary*, Alphen aan den Rijn, 2025.

Sztandar-Sztanderska K., Zielińska M., 'When a Human Says "No" to a Computer: Frontline Oversight of the Profiling Algorithm in Public Employment Services in Poland', *Sozialer Fortschritt*, 2022, Vol. 71, No. 6.

Weitkunat R., Bestle M., 'Computerized Mackworth vigilance clock test', *Computer Methods and Programs in Biomedicine*, 1990, Vol. 32, Issue 2.

Cytuj jako:

Kiejnich-Kruk K. (2025), *Obligations of importers, distributors and deployers of high-risk AI systems under the AI Act*, Ius Novum (Vol. 19) 4, 121–140. DOI 10.2478/in-2025-0040