Ius Novum
2025, vol. 19, nr 4, s. 129–149

OBOWIĄZKI IMPORTERÓW, DYSTRYBUTORÓW I PODMIOTÓW STOSUJĄCYCH SYSTEMY AI WYSOKIEGO RYZYKA NA GRUNCIE AI ACT

KAROLINA KIEJNICH-KRUK*

DOI: 10.26399/iusnovum.v19.4.2025.40/k.kiejnich-kruk

Streszczenie
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (AI Act) wyszczególnia różne podmioty uczestniczące w łańcuchu dostaw systemów AI wysokiego ryzyka. Cele niniejszego artykułu to: przedstawienie oraz porównanie obowiązków: importerów, dystrybutorów oraz podmiotów stosujących oraz analiza okoliczności, w których obowiązki te mogą zostać rozszerzone i zrównane z obowiązkami dostawców systemów AI wysokiego ryzyka. Obowiązki importerów oraz dystrybutorów w znacznej mierze mają charakter weryfikacyjny. Nadto, obowiązki dystrybutorów są bardziej ograniczone niż obowiązki importerów, na których spoczywa ciężar pierwotnej weryfikacji spełnienia zadań przez dostawców. Odmiennie, obowiązki nałożone na podmioty stosujące nie mają zazwyczaj charakteru wtórnego wobec obowiązków dostawców. Są odrębnymi zadaniami, wynikającymi z chęci przeciwdziałania zagrożeniom, jakie niesie za sobą etap stosowania systemów AI wysokiego ryzyka.

W artykule omówiono również sytuacje szczególne, w których ingerencja w systemy AI powoduje, że na podmiot niebędący dostawcą nałożone zostają obowiązki zrównane z obowiązkami dostawców systemów AI wysokiego ryzyka. Jest tak dlatego, że systemy oparte na technologii sztucznej inteligencji są podatne m.in. na zmiany ich przeznaczenia, w sposób niezależny od sposobów ich zaprojektowania oraz woli dostawców. Właściwa detekcja

* dr, adiunkt w Zakładzie Postępowania Karnego Wydziału Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu (Polska), asesor sądowy w Sądzie Rejonowym w Jarocinie, e-mail: kiejnich-kruk@amu.edu.pl, ORCID: 0000-0003-1551-5448

i zrozumienie obowiązków poszczególnych podmiotów w łańcuchu dostaw są ważne dla minimalizacji ryzyk związanych z wykorzystanie systemów AI wysokiego ryzyka w całej Unii Europejskiej oraz w celu uniknięcia sankcji pieniężnych przez wskazane podmioty.

Słowa kluczowe: AI Act, sztuczna inteligencja, importerzy, dystrybutorzy, podmioty stosujące

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

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

WSTĘP

Akt w sprawie sztucznej inteligencji[1] (dalej jako: AI Act lub rozporządzenie) stanowi przełom w zakresie prawnych regulacji podmiotów zaangażowanych w tworzenie, dostawy i wykorzystanie systemów opartych na technologii sztucznej inteligencji. Szczególne miejsce zajmują regulacje dotyczące systemów AI, uznawanych za systemy wysokiego ryzyka. AI Act wyróżnia przy tym różne podmioty uczestniczące w łańcuchu dostaw tych systemów, nakładając na nie zróżnicowane obowiązki. Rozkład ciężaru i zakres owych obowiązków mogą niekiedy budzić wątpliwości.

Większość analiz w tym zakresie, na gruncie zarówno krajowym, jak i międzynarodowym, skupiona jest na obowiązkach dostawców, mając na uwadze, że zostały

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), PE/24/2024/REV/1, Dz. Urz. UE L 2024/1689 z dn. 12.07.2024.

one uregulowane najszerzej i to właśnie na tych podmiotach spoczywa większość obowiązków przewidzianych w AI Act[2]. Nie można jednak tracić z pola widzenia, że również importerzy, dystrybutorzy i podmioty stosujące systemy AI wysokiego ryzyka odgrywać będą istotną rolę w łańcuchu dostaw i zabezpieczeniu praw podstawowych, a także w ograniczeniu ryzyk związanych z wdrażaniem tych systemów.

Cele niniejszego artykułu to: przedstawienie oraz porównanie obowiązków tych trzech podmiotów wynikających z AI Act oraz analiza okoliczności, w których obowiązki te mogą zostać rozszerzone i zrównane z obowiązkami dostawców systemów AI wysokiego ryzyka. Nadto, w pracy wskazano, w jaki sposób podmioty te – w praktyce – mogą się ze swoich obowiązków wywiązać i jaki jest ich zakres. Kwestie te nie są bowiem jednoznaczne, a źródła pozyskania praktycznych wyjaśnień – ograniczone. Z uwagi na obszerność zagadnienia oraz ograniczenia wynikające z formy opracowania, omówienie ograniczone zostało do obowiązków najważniejszych oraz tych budzących najwięcej wątpliwości w zakresie wykładni przepisów bądź praktyki ich stosowania.

OBOWIĄZKI IMPORTERÓW

Importer to podmiot, który wprowadza do obrotu system AI opatrzony nazwą lub znakiem towarowym osoby fizycznej lub prawnej mającej siedzibę w państwie trzecim (art. 3 pkt 6). „Wprowadzenie do obrotu" oznacza udostępnienie po raz pierwszy systemu AI lub modelu AI ogólnego przeznaczenia na rynku unijnym (art. 3 pkt 9). Państwo trzecie jest państwem innym niż państwa członkowskie UE, co wynika z przepisu art. 2 ust. 1 pkt a (przedstawienie państw Unii oraz państw trzecich jako pojęć alternatywnych). Zazwyczaj z państwa trzeciego będzie pochodził dostawca systemu, opatrując go swoją nazwą.

Obowiązki importerów zostały określone w art. 23 AI Act. Importer w łańcuchu dostaw systemów AI wysokiego ryzyka pełni istotną rolę w zakresie systemów oferowanych na rynku unijnym, a dostarczanych przez podmioty z państw trzecich. Stanowi on pomost pomiędzy dostawcami zagranicznymi a dystrybutorami lub podmiotami stosującymi systemy AI na terenie UE. Importer ocenia, czy dostawca zastosował standardy wynikające z AI Act i czy dany system AI zapewnia zgodność z normami unijnymi pozwalającymi mu funkcjonować na unijnym rynku.

Konieczne jest odniesienie się do tego, jakie działania powinni podjąć importerzy, aby spełnić obowiązki, o jakich mowa w przepisie. Należy do nich – w pierwszej kolejności – sprawdzenie, czy dostawca uczynił zadość swoim obowiązkom:

---

[2] Zob. m.in.: M. Jacobs, J. Simon, *Assigning Obligations in AI Regulation: A Discussion of Two Frameworks Proposed By the European Commission*, „Digital Society" 2022, nr 1 (6); L. Enqvist, *'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?*, „Law, Innovation and Technology" 2023, nr 15 (2), s. 508–535; L. Edwards, *The EU AI Act: A Summary of Its Significance and Scope*, s. 7–8, 16, https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/ (dostęp: 8.04.2025); K. Hewson, *The Roles of the Provider and Deployer in AI Systems and Models*, https://www.stephensonharwood.com/insights/the-roles-of-the-provider-and-deployer-in-ai-systems-and-models (dostęp: 8.04.2025).

1) czy przeprowadził odpowiednią procedurę oceny zgodności,
2) czy sporządził dokumentację techniczną,
3) czy opatrzył system wymaganym oznakowaniem CE oraz dołączył deklarację zgodności UE i instrukcję obsługi,
4) czy ustanowił upoważnionego przedstawiciela.

Procedura oceny zgodności została omówiona w art. 43 AI Act, a jej przeprowadzenie jest obowiązkiem dostawcy. Zadaniem importera jest natomiast weryfikacja formalna dopełnienia obowiązku przez dostawcę. Nie musi on przy tym sprawdzać, czy ocena ta została przeprowadzona poprawnie[3]. Weryfikacja ta jest możliwa poprzez sprawdzenie bazy danych utworzonej na podstawie art. 71 AI Act. Zgodnie z załącznikiem VIII sekcją A w bazie muszą zostać umieszczone informacje o przedstawicielu, winny zostać dołączone kopie deklaracji zgodności UE oraz instrukcji obsługi, a także informacja o certyfikacji. Należy jednak zwrócić uwagę, że w deklaracji zgodności UE musi znaleźć się stwierdzenie, iż dany system AI wysokiego ryzyka spełnia wymogi ustanowione w sekcji 2, w tym w zakresie oceny zgodności. Pojęcie „odpowiedniość" należy odnieść do trybu tej procedury, nie do jakości jej wykonania. Procedura oceny zgodności może zostać przeprowadzona zgodnie z załącznikiem VI lub VII. W wypadku, gdy procedura oceny zgodności i dokumentacji technicznej przeprowadzana jest zgodnie z załącznikiem VII, jej wyniki uzewnętrzniane są w formie decyzji jednostki notyfikującej oraz certyfikatu, a zatem weryfikacja możliwa jest wyłącznie poprzez wgląd w bazę danych, o jakiej mowa w art. 71 AI Act.

Również obowiązek weryfikacji, czy dostawca dokumentację techniczną sporządził, jest możliwy poprzez sprawdzenie bazy danych utworzonej na podstawie art. 71 AI Act[4]. Jest to obowiązek sprawdzenia, czy formalnie dokumentacja ta została sporządzona, a nie weryfikowanie prawidłowości tej dokumentacji.

Obowiązki opatrzenia systemu wymaganym oznakowaniem CE oraz dołączenia deklaracji zgodności UE i instrukcji obsługi spoczywają na dostawcy. Dwa pierwsze zostały wskazane w art. 16 ust. 1 lit. g i h. Instrukcja obsługi stanowi natomiast część dokumentacji technicznej, o której mowa w art. 11 ust. 1[5]. Importer ma obowiązek weryfikacji, czy dostawca – formalnie – sprostał owym obowiązkom. Weryfikacja istnienia deklaracji zgodności UE i instrukcji obsługi jest również możliwa poprzez sprawdzenie bazy danych utworzonej na podstawie art. 71 AI Act[6]. W zakresie możliwości weryfikacji oznakowania CE, wskazówkę zawiera przepis art. 48 ust. 3. Zgodnie z tym przepisem oznakowanie umieszcza się na systemie AI w sposób widoczny, czytelny i trwały. W razie, gdy z uwagi na charakter systemu AI wysokiego ryzyka oznakowanie systemu w taki sposób nie jest możliwe lub zasadne, oznakowanie to umieszcza się na opakowaniu lub – w stosownych przypadkach – w dołączonej do systemu dokumentacji.

---

[3] L. Riede, O. Talhoff, *Art. 23*, w: *The EU Artificial Intelligence (AI) Act: A Commentary*, red. C.N. Pehlivan, N. Forgó, P. Valcke, Alphen aan den Rijn: Wolters Kluwer Law International, 2025, s. 510.

[4] Zob. załącznik VIII sekcja A.

[5] Zob. załącznik IV pkt 1 lit. h.

[6] Zob. załącznik VIII sekcja A.

Obowiązek ustanowienia przez dostawcę upoważnionego przedstawiciela przewidziany został w art. 22. Obowiązek importera ogranicza się do weryfikacji, czy taki przedstawiciel został ustanowiony. Jest to możliwe poprzez sprawdzenie bazy danych, w której muszą zostać umieszczone informacje o przedstawicielu[7].

Dobrą praktyką jest sporządzenie protokołu weryfikacji, w którym importerzy wskazują środki podjęte w celu weryfikacji zgodności działań dostawców z regulacjami UE oraz, w razie potrzeby, dołączają odpowiednie dokumenty (wydruk z bazy danych, fotografie).

Dalej, na importerów nałożono również obowiązki zaniechania określonych działań. Zgodnie z treścią art. 23 ust. 2 AI Act, gdy importer ma wystarczające powody, aby uważać, że system AI wysokiego ryzyka jest niezgodny z tym rozporządzeniem lub został sfałszowany lub sfałszowana została dołączona do niego dokumentacja, nie wprowadza tego systemu do obrotu dopóty, dopóki nie zostanie zapewniona jego zgodność z tym rozporządzeniem. Jest to więc zakaz o charakterze bezwzględnym.

Należy odpowiedzieć sobie na pytanie, czym są „wystarczające powody" dla uznania, że produkt zaopatrzony został w sfałszowaną dokumentację, lub też że nie spełnia wymogów unijnych. Podkreślenia wymaga fakt, że pozytywne obowiązki importera w zakresie weryfikacji systemów zostały wskazane w ust. 1 przepisu i omówione powyżej. Może on jednak – choć nie musi – podjąć inne (dodatkowe) działania weryfikacyjne w zakresie oceny zgodności działań dostawcy i funkcjonowania systemu z normami unijnymi. Przykładowo, może taką informację pozyskać z przekazów medialnych czy od sygnalistów. Jeżeli informacje te pokazują, że system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1, importer ma obowiązek powiadomić organy wskazane w przepisie oraz wstrzymać proces importu. Proces wprowadzenia do obrotu może być podjęty w przypadku uzupełnienia dokumentacji, modyfikacji dokumentacji, dopełnienia procedur lub – choć wyraźnie nie wskazano tego przypadku w przepisie – w momencie ustalenia, że zastrzeżenia importera były błędne, tj. wynikały z nieprawidłowej oceny zgodności.

Istotny obowiązek został również przewidziany w art. 23 ust. 6 rozporządzenia. Określono tam kwestię współpracy importerów z właściwymi organami. Zgodnie z tym przepisem na uzasadniony wniosek importerzy zobowiązani są do przekazania organom wszelkich niezbędnych informacji i dokumentacji. Pojęcie „odpowiedni organ" łączyć należy z nadzorem nad dochowaniem standardów określonych w art. 8–15. Są to krajowe organy nadzoru rynku[8], organy ochrony praw podstawowych[9] oraz unijny organ: Urząd ds. AI. Będą to również organy sektorowe, np. organy nadzoru z zakresu ochrony danych osobowych[10].

Uznać przy tym należy, że zastosowano tu nieprawidłowe zasady techniki legislacyjnej, tj. użyto odmiennych określeń w przypadku tożsamych pojęć. Znaczeniowo zrównać należy pojęcia „odpowiednie organy krajowe" i „właściwe organy krajowe" (tak również w innych wersjach językowych, np. *competent/relevant*

[7] Zob. załącznik VIII sekcja A.
[8] Zob. art. 74.
[9] Zob. art. 77.
[10] Zob. pkt 10 Preambuły.

(j. angielski). W niektórych wersjach językowych pojęcia te są tożsame: np. *autorités compétente* (j. francuski), *autoridades competentes* (j. hiszpański), *autorità competente* (j. włoski). Są to pojęcia synonimiczne i należy je wykładać jednakowo.

Pojęcie „uzasadniony wniosek" należy wiązać z zakresem kompetencji i zadań określonych organów. Oznacza to, że cel pozyskania informacji lub dokumentacji od importerów musi wiązać się z wolą wypełnienia obowiązków przez organ. Będą to przede wszystkim obowiązki nadzorcze, dla których prawidłowego wykonania konieczne jest posiadanie wielu informacji o funkcjonowaniu systemu AI wysokiego ryzyka.

Celem ustanowienia obowiązku współpracy jest wykazanie zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2. Są to następujące wymogi:

1) ustanowienie systemu zarządzania ryzykiem[11],
2) właściwe zarządzanie danymi[12],
3) sporządzenie dokumentacji technicznej[13],
4) rejestrowanie zdarzeń[14],
5) zachowanie przejrzystości działania i udostępnianie informacji podmiotom stosującym[15],
6) nadzór ze strony człowieka[16],
7) osiągnięcie dokładności, solidności i cyberbezpieczeństwa dostarczanych systemów[17].

W rozporządzeniu nie precyzuje się zakresu informacji i dokumentów, które podlegają obowiązkowi przekazania. Wobec braku ograniczenia regulacji, uznać należy, że obowiązkowi przekazania podlegają wszystkie informacje i dokumenty, jakie danemu organowi mogą być potrzebne do oceny zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2 rozporządzenia. Informacje te oraz dokumenty mają zostać przekazane w języku łatwo zrozumiałym dla tych organów. Pojęcie to należy odnieść do wersji językowej[18]. W wypadku organów krajowych będzie to język urzędowy danego państwa (lub inne, jeśli organ tak wskaże). W wypadku organów unijnych – należy odwołać się do regulaminów tych instytucji[19]. W razie braku dookreślenia wymogów językowych, uznać należy, że każdy z 24 języków urzędowych w UE jest dopuszczalny[20].

W rozporządzeniu (art. 23 ust. 7) na importerów nałożono również obowiązek generalnej współpracy z odpowiednimi organami krajowymi, jakimi są organy nadzoru rynku (dotyczące AI, a także organy sektorowe, np. ochrony danych osobowych,

---

[11] Zob. art. 9.
[12] Zob. art. 10.
[13] Zob. art. 11.
[14] Zob. art. 12.
[15] Zob. art. 13.
[16] Zob. art. 14.
[17] Zob. art. 15.
[18] L. Riede, O. Talhoff, *Art. 23…*, op. cit., s. 513.
[19] Zgodnie z art. 6 Rozporządzenia nr 1 w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej (Dz.U. nr 17 z 6.10.1958, s. 385) instytucje mogą określić szczegółowe zasady stosowania systemu językowego w swych regulaminach.
[20] Zob. art. 1 Rozporządzenia nr 1 w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej (Dz.U. nr 17 z 6.10.1958, s. 385).

zasad konkurencji) i inne organy ochrony praw podstawowych. Importerzy mają obowiązek współpracy z tymi organami w zakresie wszelkich działań, jakie organy te podejmują w odniesieniu do systemu AI wysokiego ryzyka udostępnionego przez importera. Celem tych działań ma być w szczególności zmniejszenie lub ograniczenie stwarzanego przez ten system ryzyka. Pewne obowiązki współpracy zostały skonkretyzowane w innych przepisach rozporządzenia, m.in. w zakresie udostępniania dokumentacji i informacji, obowiązki notyfikacyjne. Uznać należy, że w omawianym ust. 7 nakłada się na importerów obowiązek współpracy w zakresie wykraczającym poza skonkretyzowane w rozporządzeniu obowiązki. Jednocześnie, przepisy nie wskazują katalogu działań, do których importer jest obowiązany w ramach współpracy. Obowiązek współpracy rozciąga się na wszelkie działania, jakie dany organ podejmuje w ramach swoich kompetencji. Innymi słowy, importer może odmówić współpracy jedynie wtedy, gdy wezwanie organu do podjęcia określonych działań (lub zaniechań) dotyczy sfery wykraczającej poza jego kompetencje.

Brak zastosowania się do wskazanych obowiązków sankcjonowany jest poprzez nałożenie administracyjnej kary pieniężnej w wysokości określonej w art. 99.

OBOWIĄZKI DYSTRYBUTORÓW

Obowiązki dystrybutorów systemów AI wysokiego ryzyka określono szczegółowo w art. 24. Są to przede wszystkim obowiązki weryfikacyjne. Dystrybutor jest swego rodzaju pośrednikiem (najczęściej będzie to sprzedawca czy usługodawca), nie ma jednak wpływu na to, jak systemy AI zostały zaprojektowane lub jak będą wykorzystywane. Stąd jego obowiązki w zakresie udostępniania systemów AI wysokiego ryzyka są znacznie mniejsze niż obowiązki dostawców i podmiotów stosujących. Obowiązki weryfikacyjne dystrybutora są również bardziej ograniczone niż w wypadku importera, i bardziej sformalizowane.

Obowiązkiem dystrybutora jest zweryfikowanie, czy pozostałe podmioty zaangażowane w łańcuch dostawy systemu AI wysokiego ryzyka w prawidłowy sposób wykonały swoje obowiązki określone odpowiednio w art. 16 lit. b i c oraz w art. 23 ust. 3 AI Act. Dostawca lub importer (w przypadkach, w których system AI wysokiego ryzyka jest wprowadzany do obrotu z państwa trzeciego) ma obowiązek potwierdzić wobec dystrybutora, że system AI wysokiego ryzyka zawiera:

1) oznakowanie zgodności CE,
2) kopię deklaracji zgodności UE,
3) instrukcję obsługi,
4) informację – w systemie AI, na jego opakowaniu lub w dołączonej do niego dokumentacji – o nazwie, zarejestrowanaej nazwie handlowaej lub zarejestrowanym znaku towarowym i adresie, pod którym można się skontaktować z dostawcą lub importerem,
5) informację, że dostawca wprowadził system zarządzania jakością zgodny z art. 17.

Ponownie, wskazać należy, że dobrą praktyką jest sporządzenie protokołu weryfikacji, w którym importerzy wskażą środki podjęte w celu weryfikacji zgodności

działań dostawców z regulacjami UE oraz, w razie potrzeby, dołączą odpowiednie dokumenty (wydruk z bazy danych, fotografie).

Weryfikacja części danych następuje poprzez sprawdzenie bazy danych utworzonej na podstawie art. 71. Zgodnie z załącznikiem VIII sekcją A w bazie muszą zostać umieszczone informacje o przedstawicielu, dołączone kopie deklaracji zgodności UE oraz instrukcji obsługi, informacja o certyfikacji, dane dostawcy. Informacje o oznaczeniu CE dystrybutor ma obowiązek zweryfikować w bazie właściwej jednostki certyfikującej. Kopia deklaracji zgodności powinna zostać okazana dystrybutorowi, podobnie jak potwierdzenie tego, że dostawca posiada odpowiedni system zarządzania jakością. System zarządzania jakością przyjmuje formę pisemnych polityk, procedur i instrukcji[21], możliwe jest więc okazanie ich kopii. Istnienie informacji o dostawcy i importerze dystrybutor może sprawdzić przez ogląd opakowania systemu, sprawdzenie dołączonej w formie fizycznej dokumentacji lub odtworzenie systemu w warunkach testowych, w przypadku dokumentacji w formie elektronicznej lub zawarcia informacji w ramach systemu.

W myśl art. 24 ust. 2 dystrybutor jest zobowiązany do nieudostępniania systemu AI wysokiego ryzyka, jeśli w jego ocenie nie spełnia on wymogów ustanowionych w sekcji 2 rozdziału III (art. 8–15). Podobnie jak w wypadku importera i nakładanych obowiązków zaniechania, przepis ten należy rozumieć w ten sposób, że obowiązek pozytywnej weryfikacji przez dystrybutora ograniczony jest wyłącznie do sprawdzenia, czy system AI ma dokumenty i cechy omówione powyżej. Obowiązek ten nie dotyczy weryfikacji, czy system spełnia wymogi określone w art. 8–15 AI Act. Przyjmuje się bowiem, że uzyskanie certyfikatu CE oraz deklaracji zgodności UE pozwala na przyjęcie założenia o zgodności systemu z tymi wymogami. Założenie to jednak może okazać się kontrfaktyczne. Jeżeli dystrybutor pozyska informacje – z jakichkolwiek źródeł – wskazujące, że system AI może nie spełniać tych wymogów (przy czym nie musi być to informacja potwierdzona, wystarczające jest uzasadnione przypuszczenie), obowiązany jest do nieudostępniania systemu AI.

Podobnie jak w przypadku importerów, informacje te mogą pochodzić np. z mediów (np. podczas ujawnienia, że dany dostawca, projektując systemy AI wysokiego ryzyka, nie przestrzega zasad gromadzenia danych treningowych) czy od sygnalistów. Istnieje również możliwość wystąpienia sytuacji, w której dystrybutor podjął działania weryfikacyjne wykraczające poza obligatoryjne i wyniki tych działań dają podstawę do uznania, że wymogi systemu nie są spełnione.

Trafnie wskazuje się w doktrynie[22], że obowiązek ten jest bardziej ograniczony w porównaniu z obowiązkiem importera. Może to wynikać z faktu, że dystrybutor często ma mniej szczegółowy wgląd w funkcjonalność systemów AI oraz mniej bezpośredni kontakt z dostawcą systemu AI wysokiego ryzyka. Słusznie wskazano, że w praktyce art. 23 ust. 2 może być odczytywany jako bardziej rygorystyczny art. 24 ust. 2, wątpliwe jest, czy tak jest w rzeczywistości. Jeśli powód do niepokoju po stronie dystrybutora nie jest „wystarczający", trudno oczekiwać, że dystrybutor

[21] Zob. art. 17.

[22] L. Riede, O. Talhoff, *Art. 24*, w: *The EU Artificial Intelligence (AI) Act…*, op. cit., s. 521.

podejmie działania ukierunkowane na powstrzymanie się od udostępnienia systemu na rynku[23].

Szczególnego rodzaju obowiązek dystrybutora pojawia się w sytuacji, w której system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1[24]. W takiej sytuacji dystrybutor informuje o tym – stosownie do przypadku – dostawcę lub importera systemu. Na tle tego obowiązku pojawia się pytanie, czy dystrybutor posiada pozytywny obowiązek działania w zakresie weryfikacji ryzyka, czy – jak w wypadku innych wymogów z ust. 2 – obowiązek poinformowania aktualizuje się dopiero wtedy, gdy dystrybutor poweźmie taką wiedzę, nie musi jednak jej sam aktywnie poszukiwać. Mając na uwadze fakt, że obowiązek ten został przewidziany w art. 24 ust. 2, a nie w ust. 1, brak jego wymienienia w katalogu zamkniętym w ust. 1 należy interpretować jako brak pozytywnego obowiązku weryfikacji, czy system stwarza ryzyko, o którym mowa w art. 79 ust. 1. Uzyskanie oznaczenia CE i deklaracji zgodności co do zasady powinno wykluczyć takie ryzyko. Może się jednak okazać, że system już po uzyskaniu oznaczeń ujawni cechy lub formy stosowania, które pozwolą na uznanie, że stanowi on produkt stwarzający ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych osób.

Procedurę uznania produktu za stwarzający ryzyko i działań naprawczych i notyfikacyjnych prowadzi organ nadzoru. Wykładnia sformułowania „stwarza ryzyko", w którym użyto trybu oznajmującego, nie zaś przypuszczającego (jak w przypadku innych zagrożeń opisanych w tym przepisie), pozwala uznać, że wymagana jest w tym zakresie wiedza (potwierdzona informacja), nie może to być jedynie uzasadnione przypuszczenie. W tym kontekście „stworzenie ryzyka" odnosi się do zagrożenia o charakterze abstrakcyjnym. Nie jest konieczne wyrządzenie szkody żadnemu podmiotowi, ani pewność co do tego, że ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych się ziści. Oznacza to, że wszelkie niezgodności systemu związane np. z danymi (ich przetwarzaniem, gromadzeniem, doborem) będą mogły mieć niekorzystny wpływ na prawo do prywatności, niedyskryminacji, ochrony danych osobowych – niezależnie od tego, czy takie ryzyko się faktycznie ziści i czy jakakolwiek szkoda zostanie wyrządzona.

W art. 24 ust. 3 została nałożona na dystrybutorów odpowiedzialność za system AI wysokiego ryzyka w okresie, w jakim pozostaje on w ich dyspozycji (posiadaniu). Niezależnie od tego, czy system ten przechowywany jest w formie cyfrowej, czy materialnej, w razie modyfikacji systemu lub dezaktualizacji ocen zgodności z wymogami AI Act, odpowiedzialność spoczywa na dystrybutorze. W tym kontekście szczególne znaczenie mają obowiązki w zakresie cyberbezpieczeństwa. Konieczne jest podjęcie aktywnych działań, analogicznych do działań podejmowanych przez dostawców[25], ukierunkowanych na uniemożliwienie dostępu do systemu nieupoważnionym osobom trzecim, mającym na celu zmianę wykorzystania systemu, zmianę wyników lub skuteczności jego działania poprzez wykorzystanie

---

[23] T. Fülöp, P. Poindl, *Art. 24*, w: *The EU Artificial Intelligence (AI) Act…*, op. cit., s. 522.
[24] Zob. art. 79.
[25] Zob. art. 15.

słabych punktów systemu. Dystrybutor ponosi odpowiedzialność za ewentualny brak skuteczności tych działań.

Obowiązki przewidziane w art. 23 ust. 4 stanowią lustrzane odbicie obowiązków przewidzianych w ust. 2, z tą różnicą, że dotyczą sytuacji, w której nieprawidłowości zostały zidentyfikowane już po udostępnieniu systemu AI wysokiego ryzyka. Z uwagi na to, że w tej sytuacji ryzyko zagrożeń dla praw podmiotów wzrasta, obowiązki dystrybutora są większe. Jest on obowiązany podjąć działania naprawcze konieczne do zapewnienia zgodności systemu AI wysokiego ryzyka z wymogami przewidzianymi w sekcji 2, do wycofania go z rynku lub wycofania go z użytku, lub zapewnia podjęcie takich działań naprawczych przez, stosownie do przypadku, dostawcę, importera lub odpowiedniego operatora. Jest to również odzwierciedlenie obowiązku dostawcy określonego w art. 20.

Działania naprawcze są działaniami ukierunkowanymi na uzyskanie zgodności systemu AI wysokiego ryzyka z wymogami określonymi w art. 8x15. Wymaga się zatem zidentyfikowania niezgodności i modyfikacji systemu w sposób, który ową zgodność zapewnia[26]. Analogicznie do ust. 2, dystrybutor ma obowiązek poinformować dostawcę lub importera systemu oraz organy właściwe w zakresie przedmiotowego systemu AI wysokiego ryzyka w przypadku, w którym system ten stwarza ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych.

Z kolei obowiązki przewidziane w ust. 5 i 6 stanowią powielenie obowiązków importerów określonych w art. 23 ust. 6 i 7, choć zostały sformułowane nieco odmiennie. Ponownie, brak zastosowania się do wskazanych obowiązku sankcjonowany jest poprzez nałożenie administracyjnej kary pieniężnej[27].

OBOWIĄZKI PODMIOTÓW STOSUJĄCYCH SYSTEMY AI WYSOKIEGO RYZYKA

Obowiązki podmiotów stosujących systemy AI wysokiego ryzyka zostały w większości określone w art. 26 AI Act. Na podmioty stosujące systemy AI wysokiego ryzyka prawodawca unijny nakłada – zaraz po dostawcach – szczególnie wiele obowiązków. Co ważne, pojęcie podmiotu stosującego nie jest synonimiczne do pojęcia osoby użytkującej system czy korzystającej z niego[28]. Obowiązki przewidziane w tym przepisie w wypadku korzystania z systemów AI w procesach rekrutacji nałożone są, przykładowo, na przedsiębiorcę, a nie na pracownika z działu kadr, który użytkuje system (program).

Jak wskazano w punkcie 93 Preambuły, ryzyko związane z systemami AI może wynikać ze sposobu ich wykorzystania. Podmioty stosujące systemy AI wysokiego ryzyka odgrywają zatem istotną rolę w zapewnianiu ochrony praw podstawowych w uzupełnieniu obowiązków dostawcy podczas rozwoju systemu AI. Podmioty te rozumieją, jak wykorzystywany będzie system AI wysokiego ryzyka i mogą

[26] Zob. art. 20.
[27] Zob. art. 99.
[28] Zob. art. 3 pkt 4.

identyfikować potencjalne ryzyko, które nie zostało przewidziane na etapie projektowania systemu.

W przepisach art 26 ust. 1–4 nakłada się na podmioty stosujące systemy AI wysokiego ryzyka następujące obowiązki:

1) podjęcie środków technicznych i organizacyjnych mających na celu monitorowanie zgodności działania systemu AI z instrukcją obsługi,
2) powierzenie sprawowania nadzoru osobom fizycznym, które mają niezbędne kompetencje, przeszkolenie i uprawnienia, a także niezbędne wsparcie,
3) w zakresie, w jakim sprawuje on kontrolę nad danymi wejściowymi, zapewnienie adekwatności i wystarczającej reprezentatywności danych wejściowych w odniesieniu do przeznaczenia systemu AI wysokiego ryzyka.

Środkami technicznymi i organizacyjnymi ukierunkowanym na monitorowanie zgodności działania systemu AI z instrukcją obsługi będą na przykład: stworzenie właściwych procedur na wypadek wykrycia nieprawidłowości przez jakiegokolwiek użytkownika, regularny audyt wewnętrzny weryfikujący zgodność korzystania z instrukcją obsługi, cykliczne szkolenia dla pracowników, czy wprowadzenie automatycznych alertów w przypadku wyników znacząco odbiegających od przeciętnych.

Obowiązki nadzorcze polegają na wprowadzeniu zasady kontroli działania systemu przez człowieka (ang. *human-on-the-loop*) raczej niż aktywnego udziału w procesie decyzyjnym (ang. *human-in-the-loop*)[29]. Oznacza to, że rola człowieka polega na nadzorze działania systemu, a nie na aktywnej interakcji z systemem, np. poprzez dostarczanie informacji zwrotnej o prawidłowości wyników jako stałego elementu procesu uczenia. Jednocześnie, nadzór ten musi być rzeczywisty, a nie pozorny. Osoba nadzorująca musi legitymować się odpowiednimi kompetencjami, przeszkoleniem i uprawnieniami, tj. posiadać wiedzę i doświadczenie z zakresu działania systemów AI wysokiego ryzyka, obowiązujących standardów i istniejących zagrożeń ich naruszenia, ryzyka wystąpienia nieprawidłowości i właściwej reakcji na ich wykrycie. Pożądane jest, aby osoby sprawujące nadzór zmieniały się cyklicznie, gdyż – jak pokazują wyniki badań – osoby fizyczne relatywnie często stają się znużone lub rozproszone podczas pracy z systemami autonomicznymi[30]. Nie mogą zatem aktywnie nadzorować systemów AI przez długi czas bez zwiększania ryzyka niewykrycia nieprawidłowości. Wiąże się to również z efektem psychologicznym, polegającym na tym, że osoby fizyczne zakładają, że systemy te nie mogą zawieść czy „się pomylić", co jednak niejednokrotnie się zdarza[31].

W przedmiocie danych wejściowych, podmiot stosujący ma obowiązek zapewnienia adekwatności i wystarczającej reprezentatywności danych wejściowych w odniesieniu do przeznaczenia systemu AI wysokiego ryzyka. Dane wejściowe oznaczają dane dostarczone do systemu AI lub bezpośrednio przez niego pozyskiwane,

---

[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, nr 54 (2), s. 1076–1084.

[30] R. Weitkunat, M. Bestle, *Computerized Mackworth Vigilance Clock Test*, „Computer Methods and Programs in Biomedicine" 1990, nr 32 (2), s. 147–149.

[31] R. Weitkunat, M. Bestle, *Computerized Mackworth…*, op. cit., s. 147–149.

na podstawie których system ten generuje wynik[32]. Co do zasady, architektura systemu przewiduje, jakie dane wejściowe należy dostarczyć, aby otrzymać wynik. Przykładowo, w systemach rekrutacyjnych adekwatnymi danymi będą informacje o wykształceniu. Jednak już dostarczenie danych o rasie może powodować, że wyniki okażą się dyskryminujące. Wydaje się, że wymóg reprezentatywności danych nie będzie dotyczył wszystkich przykładów zastosowań systemów AI wysokiego ryzyka. Przykładowo, urzędy pracy czy podmioty prywatne prowadzące rekrutację nie mają wpływu na to, jakie osoby zgłoszą się do danego konkursu (czy np. będą to same kobiety).

Wskazać można kazus wykorzystania takiego systemu przez administrację publiczną. W maju 2014 r. polskie Ministerstwo Pracy i Polityki Społecznej wprowadziło system zautomatyzowanego podejmowania decyzji, mający na celu przeciwdziałanie bezrobociu poprzez kategoryzację osób poszukujących pracy; osoby te podzielono na trzy odrębne grupy na podstawie określonych cech[33]. Proces kategoryzacji rozpoczynał się od wywiadu komputerowego, po którym wprowadzono różne czynniki do bazy danych, a każdemu z nich przypisano określoną punktację. System uwzględniał dwie istotne zmienne: „odległość od rynku pracy" i „gotowość do wejścia lub powrotu na rynek pracy". Poprzez te kryteria system oceniał czynniki utrudniające wejście na rynek, takie jak płeć, wiek i wykształcenie. System ten spotkał się ze znaczną krytyką ze względu na brak przejrzystości, kwestie ochrony danych osobowych, możliwą dyskryminację oraz brak rzeczywistego nadzoru ze strony człowieka[34]. Przepisy umożliwiające wykorzystanie systemu były przedmiotem badania przez Trybunał Konstytucyjny w zakresie braku środka zaskarżenia, a także w kwestii uregulowania systemu w formie rozporządzenia[35]. Trybunał wskazał, że w jego ocenie profilowanie nie jest sprawą ani decyzją lub orzeczeniem w rozumieniu Konstytucji. Samo gromadzenie danych czy ich przetwarzanie nie przesądza o sytuacji prawnej danego podmiotu. Z tego powodu uznano, że przepisy, mimo braku środka zaskarżenia czynności ustalenia dla bezrobotnego profilu pomocy, są zgodne z art. 45 ust. 1 i art. 78 Konstytucji. Dodano jednak, że właściwą formą regulacji jest ustawa, nie zaś rozporządzenie.

Dalej, w art. 26 w ust. 5, powtórzono obowiązek monitorowania zgodności stosowania systemu z instrukcją obsługi, uzupełniając go o obowiązek przekazania dostawcy systemu danych dotyczących skuteczności działania systemów AI wysokiego ryzyka[36]. W stosownych przypadkach mogą być to również dane pozwalające

---

[32] Zob. art. 3 pkt 33.

[33] Ministerstwo Pracy i i Polityki Społecznej, *Profilowanie pomocy dla osób bezrobotnych. Podręcznik dla pracowników powiatowych urzędów pracy*, 2014, https://panoptykon.org/sites/default/files/podrecznik_profilowania.pdf (dostęp: 5.02.2025).

[34] J. Niklas, K. Sztandar-Sztanderska, K. Szymielewicz, *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Warszawa 2015, s. 33, https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf (dostęp: 5.02.2025); K. Sztandar-Sztanderska, M. Zielenska, *When a Human Says 'No' to a Computer: Frontline Oversight of the Profiling Algorithm in Public Employment Services in Poland*, „Sozialer Fortschritt" 2022, nr 71 (6), s. 468.

[35] Wyrok TK z 6.06.2018 r., K-53/16, OTK-A 2018/38.

[36] Zob. art. 72 ust. 2.

na analizę interakcji z innymi systemami AI. W AI Act nie precyzuje się formy przekazania danych, terminu, częstotliwości ani tego, z czyjej inicjatywy – dostawcy czy podmiotu stosującego – dane powinny być przekazywane. Przyjąć jednak należy, że przekazanie danych winno nastąpić na utrwalonym nośniku, elektronicznym lub papierowym, lub w formie dokumentu – elektronicznego lub papierowego. Częstotliwość przekazywania danych należy dostosować do planu monitorowania, który zostanie przez dostawcę stworzony na podstawie wzoru opracowanego przez Komisję na podstawie ar. 72 ust. 3 AI Act. Podmiot stosujący ma obowiązek gromadzić dane na bieżąco (obowiązek ten wynika pośrednio z omawianego przepisu) i przekazać je dostawcy bez zbędnej zwłoki[37].

W razie, gdy podmioty stosujące stwierdzą wystąpienie poważnego incydentu, natychmiast informują o tym incydencie najpierw dostawcę, a następnie importera lub dystrybutora oraz odpowiednie organy nadzoru rynku. Zgodnie z art. 3 pkt 49 AI Act poważny incydent oznacza incydent lub nieprawidłowe działanie systemu AI, które bezpośrednio lub pośrednio prowadzą do któregokolwiek z poniższych zdarzeń:

a) śmierci osoby lub poważnego uszczerbku na zdrowiu osoby;
b) poważnego i nieodwracalnego zakłócenia w zarządzaniu infrastrukturą krytyczną lub jej działaniu;
c) naruszenia obowiązków przewidzianych w prawie Unii, których celem jest ochrona praw podstawowych;
d) poważnej szkody na mieniu lub poważnej szkody dla środowiska.

Jeżeli podmiot stosujący nie jest w stanie skontaktować się z dostawcą, prawodawca unijny nakazuje stosować odpowiednio art. 73 AI Act. Podmiot stosujący ma w tym przypadku obowiązek samodzielnie zawiadomić organy nadzoru rynku tego państwa członkowskiego, w którym wystąpił dany incydent. Zgłoszenie powinno nastąpić natychmiast, nie później jednak niż w terminie 15 dni od dnia, w którym podmiot stosujący dowiedział się o wystąpieniu poważnego incydentu; natomiast w przypadku poważnego i nieodwracalnego zakłócenia w zarządzaniu infrastrukturą krytyczną lub jej działaniu – nie później niż w terminie dwóch dni od dnia, w którym podmiot stosujący dowiedział się o wystąpieniu tego incydentu. Terminy te określają czas między informacją o incydencie a poinformowaniem organu, stąd ewentualna reakcja dostawcy na zawiadomienie podmiotu stosującego musi nastąpić szybciej; w razie jej braku – podmiot stosujący zawiadamia organy z dochowaniem terminu. Będzie to szczególnie wymagające w przypadku terminu dwudniowego, wydaje się jednak, że podmiot stosujący może zawiadomić organy niemal jednocześnie z dostawcą – w razie braku natychmiastowej reakcji dostawcy. Przypomnieć bowiem należy, że taki obowiązek i tak na podmiocie tym spoczywa.

W odniesieniu do podmiotów stosujących będących instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie przepisów prawa Unii dotyczących usług finansowych, obowiązek w zakresie monitorowania omówiony powyżej uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi uzgodnień, procedur i mechanizmów zarządzania wewnętrznego na podstawie

[37] Zob. art. 72.

odpowiednich przepisów dotyczących usług finansowych. AI Act czyni więc wyjątek dla instytucji finansowych (będą to głównie banki), przyjmując, że są one wyłączone z obowiązku przekazywania danych dostawcy, czy informowania podmiotów o znacznym ryzyku bądź poważnych incydentach, jeżeli podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie przepisów prawa Unii dotyczących usług finansowych. Jest tak dlatego, że regulacje te zawierają zbliżone obowiązki, a instytucje finansowe podlegają ściśle organom nadzoru w tym zakresie.

Nie jest więc tak, że informacje o ryzyku czy incydentach nie zostaną przekazane - zostaną one przedstawione w trybie szczególnych procedur przewidzianych dla instytucji finansowych (np. art. 96 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE; art. 17 i n. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011).

W ust. 6 nałożono na podmioty stosujące systemy AI wysokiego ryzyka obowiązek przechowywania generowanych automatycznie przez ten system rejestrów zdarzeń. Okres ich przechowywania powinien być nie krótszy niż 6 miesięcy, o ile inne przepisy go nie modyfikują. Zgodnie z art. 16 lit. e rejestry zdarzeń przechowują dostawcy – o ile znajdują się one pod ich kontrolą. W przepisie art. 25 ust. 6 uzupełnia się więc tę regulację, wskazując, że kiedy znajdują się one pod kontrolą podmiotu stosującego, on odpowiada za przechowanie rejestrów zdarzeń przez określony okres czasu[38]. Jest bardziej prawdopodobne, że takie rejestry będą pod kontrolą podmiotu stosującego, gdy system AI jest wdrażany w jego infrastrukturze. Mniej prawdopodobne, że takie rejestry będą pod jego kontrolą, gdy system AI jest mu dostarczany jako usługa zewnętrzna (outsourcing).

Szczególny obowiązek nałożony został przez art. 26 ust. 8 na podmioty stosujące systemy AI wysokiego ryzyka, będące publicznymi organami lub instytucjami, organami i jednostkami organizacyjnymi Unii. Są one obowiązane do rejestracji, o jakiej mowa w art. 49. Zgodnie bowiem z art. 49 ust. 3 jeszcze przed oddaniem do użytku lub wykorzystaniem systemu AI wysokiego ryzyka wymienionego w załączniku III, podmioty stosujące rejestrują się, wybierają system i rejestrują jego wykorzystanie w bazie danych UE, o której mowa w art. 71. Wyłączone są systemy AI infrastruktury krytycznej, tj. systemy AI przeznaczone do wykorzystywania jako związane z bezpieczeństwem elementy procesów zarządzania krytyczną infrastrukturą cyfrową, ruchem drogowym i procesów ich działania lub zaopatrzenia w wodę, gaz, ciepło lub energię elektryczną. Inaczej niż dostawcy, podmioty stosujące nie rejestrują systemu, a jedynie siebie jako podmiot stosujący.

Nie jest jasne sformułowanie „przed oddaniem do użytku", mając na uwadze fakt, że oddanie do użytku systemu AI następuje przez dostawcę. Zgodnie z art. 3

[38] Zob. art. 19.

pkt 11 AI Act „oddanie do użytku" oznacza dostarczenie systemu AI do pierwszego użycia bezpośrednio podmiotowi stosującemu lub do użytku własnego w Unii, zgodnie z jego przeznaczeniem. Możliwa jest sytuacja, o jakiej mowa w art. 25, w którym to podmiot stosujący dokonuje takich modyfikacji systemu, że uważany jest za dostawcę systemu, podlega jednak wtedy obowiązkom przewidzianym dla dostawców – w zakresie oddania do użytku, i podmiotów stosujących – w zakresie wykorzystania.

Jeżeli podmioty stosujące ustalą, że system AI wysokiego ryzyka, który zamierzają wykorzystywać, nie został zarejestrowany w bazie danych UE, o której mowa w art. 71, nie stosują tego systemu i informują o tym dostawcę lub dystrybutora. Podmiot stosujący jest zobowiązany do powstrzymania się od stosowania systemu do czasy rejestracji w bazie UE. W AI Act nie precyzuje się formy i terminu przekazania informacji, przyjąć jednak należy, że powinno to nastąpić bez zbędnej zwłoki i w formie pozwalającej na utrwalenie faktu przekazania informacji.

Przepis ustępu 12, podobnie jak w wypadku innych podmiotów w łańcuchu dostaw, wskazuje blankietowy obowiązek współpracy z odpowiednimi właściwymi organami przy wszelkich działaniach, które organy te podejmują w odniesieniu do systemu AI wysokiego ryzyka, w celu wykonywania tego rozporządzenia. Zastosowanie mają wszystkie uwagi poczynione na gruncie obowiązków importerów i dystrybutorów w tym zakresie. Brak zastosowania się do wskazanych w art. 26 AI Act obowiązków sankcjonowany jest poprzez nałożenie administracyjnej kary pieniężnej[39].

Przepisy rozporządzenia nakładają na podmioty stosujące jeszcze jeden, w zasadzie główny obowiązek. Jest nim przeprowadzenie określonej w art. 27 oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych. Omówienie tego zagadnienia znacznie przekracza ramy tego opracowania, w przeciwieństwie jednak do innych obowiązków, doczekało się analiz doktrynalnych, które mogą służyć jako wskazówki dla praktyków i podmiotów stosujących[40].

PRZEJĘCIE OBOWIĄZKÓW DOSTAWCÓW

W art. 25 AI Act uregulowano kwestię modyfikacji odpowiedzialności za systemy AI wysokiego ryzyka w określonych okolicznościach. W ust. 1 określono sytuację, w której podmiot inny niż pierwotny dostawca, już po wprowadzeniu do obrotu lub oddania do użytku systemu AI wysokiego ryzyka, ingeruje w pewien sposób w system, co powoduje – zgodnie z założeniami prawodawcy – przejęcie odpowiedzialności oraz obowiązków dostawcy systemu.

Istnienie tego przepisu stanowi konsekwencję tego, że operatorzy mogą wykorzystywać dostępne na rynku systemy AI, modyfikując je i tworząc *de facto* nowy

---

[39] Zob. art. 99.

[40] Zob. m.in. 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, nr 54, i powoływane tam źródła.

system, np. dostosowany do profilu danej działalności. System pierwotny stanowi bazę funkcjonowania nowego systemu.

Zakres podmiotowy przepisu obejmuje dystrybutora, importera, podmiot stosujący lub inną stronę trzecią. Wydaje się, że pojęcie strony trzeciej należy odnieść do jakiegokolwiek innego podmiotu, podejmującego działania opisane w ust. 1. Nie należy tego utożsamiać z pojęciem „strona trzecia", używanym w przepisach AI Act do określenia podmiotu przeprowadzającego ocenę zgodności[41].

Działania przenoszące odpowiedzialność za system AI wysokiego ryzyka zostały enumeratywnie wyliczone w art. 25 ust. 1. Do tych działań – podejmowanych przez dystrybutora, importera, podmiot stosujący lub inną stronę trzecią – należą:

1) umieszczenie przez jeden z tych podmiotów swojej nazwy lub znaku towarowego w systemie AI wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku, bez uszczerbku dla ustaleń umownych przewidujących, że podział obowiązków następuje w inny sposób;
2) dokonanie we wprowadzonym już do obrotu lub oddanym do użytku systemie AI wysokiego ryzyka istotnej zmiany w taki sposób, że pozostaje on systemem AI wysokiego ryzyka;
3) zmiana przeznaczenia systemu AI, w tym systemu AI ogólnego przeznaczenia, który nie został zaklasyfikowany jako system AI wysokiego ryzyka i który został już wprowadzony do obrotu lub oddany do użytku, w taki sposób, że dany system AI staje się systemem AI wysokiego ryzyka.

Pierwszym działaniem jest umieszczenie nazwy lub znaku towarowego w systemie AI wysokiego ryzyka, bez uszczerbku dla ustaleń umownych przewidujących, że podział obowiązków następuje w inny sposób. Ostatnią część przepisu należy rozumieć w ten sposób, że strony (dostawca pierwotny i dystrybutor, importer, podmiot stosujący lub inna strona trzecia) mogą porozumieć się w ten sposób, że mimo umieszczenia oznaczeń, nie dochodzi do przeniesienia odpowiedzialności i statusu dostawcy na inny podmiot. Stosując wykładnię *a contrario* z ust. 2 zdanie ostatnie, przyjąć należy, że w wypadku umieszczenia oznaczeń w sposób sprzeczny z ustaleniami, odpowiedzialność dostawcy przechodzi na podmiot wprowadzający oznaczenia. Odpowiada on jednak wobec pierwotnego dostawcy za postępowanie niezgodne z porozumieniem. Regulacja taka ma charakter gwarancyjny dla podmiotów stosujących oraz pośrednio sankcjonujący dla podmiotów wprowadzających oznaczenia.

Drugim działaniem jest dokonanie istotnej zmiany w systemie w taki sposób, że pozostaje on systemem AI wysokiego ryzyka. Pojęcie „istotna zmiana" zostało zdefiniowane w art. 3 pkt 23. Prawodawca unijny nie podał przykładowych sytuacji, które mieściłyby się w ramach tego pojęcia. Stworzenie takiego wyliczenia byłoby trudne z uwagi na bardzo różne specyfiki systemów określanych mianem systemów AI wysokiego ryzyka. Istotne zmiany będą w szczególności dotyczyć modyfikacji w zakresie celu stosowania systemu (poszerzenie lub zwężenie zakresu; nie będzie natomiast istotną zmianą jedynie modyfikacja rodzajów otrzymywanych rezultatów) lub znaczny wpływ na sposób działania systemu (np. zakres wykorzystywanych

[41] Zob. art. 3 pkt 21.

danych walidacyjnych, sposób przetwarzania danych, reguły przetwarzania, zasady nadzoru człowieka). Inne zmiany, nieposiadające charakteru istotności, nie wywołują konsekwencji opisanych w przepisie, ale wciąż muszą zostać ocenione z punktu widzenia ustaleń między dostawcą a podmiotem identyfikującym, a także regulacji unijnych i krajowych z zakresu bezpieczeństwa produktu oraz nadzoru rynku w tym zakresie.

Trzecim działaniem jest zmiana przeznaczenia dowolnego systemu AI w taki sposób, że dany system AI staje się systemem AI wysokiego ryzyka. Nie zastrzeżono tu wymogu istotności zmiany, przyjąć jednak należy, że każda zmiana, która prowadzi do zmiany kwalifikacji systemu, jest zmianą istotną. Oznacza to, że jeżeli w wyniku jakiejkolwiek modyfikacji system AI, który nie był kwalifikowany jako system wysokiego ryzyka, powinien zostać tak zakwalifikowany, podmiot modyfikujący zyskuje status, obowiązki i odpowiedzialność dostawcy.

Wynik wykładni językowej jednoznacznie wskazuje, że porozumienia umowne mogą wyłączyć konsekwencje podejmowanych działań przewidziane w przepisie wyłącznie w przypadku, o jakim mowa w art. 25 ust. 1 lit. a). Wynik ten jest również usprawiedliwiony wykładnią celowościową. Należy bowiem wskazać, że celem wprowadzenia omawianego przepisu jest zachowanie pewności prawa[42]. Użytkownik końcowy, organy nadzorcze czy operatorzy nie powinni więc mieć wątpliwości, na kim spoczywają obowiązki dostawcy. W wypadku porozumień umownyc, pewność ta jest znacznie ograniczona z uwagi na fakt, że nie są one jawne, mogą podlegać ograniczeniom wynikającym z przepisów krajowych lub okazać się sporne między stronami. Nie jest więc trafne stwierdzenie, że wykładnia celowościowa przemawia za tym, że art. 25 ust. 1 lit. a)–c) należy interpretować jednolicie w odniesieniu do możliwości i zakresu umownego podziału obowiązków[43].

W powyższych przypadkach podmiot modyfikujący przejmuje obowiązki dostawcy, określone w art. 16 AI Act.

W ust. 2 wskazano z kolei, że w przypadku uznania podmiotu modyfikującego za dostawcę zgodnie z ust. 1, pierwotnego dostawcy nie uznaje się już za dostawcę tego konkretnego systemu AI. Przepis ten określa jednak obowiązki po stronie pierwotnego dostawcy. Jest on obowiązany do udostępnienia niezbędnych informacji oraz udzielenia racjonalnie oczekiwanego dostępu technicznego i innego wsparcia niezbędnego do spełnienia obowiązków określonych w AI Act, w szczególności w odniesieniu do zgodności z kryteriami oceny zgodności systemów AI wysokiego ryzyka.

Należy wskazać, że przepis ten nie precyzuje w żadnym stopniu zakresu obowiązków pierwotnego dostawcy, posługując się pojęciami nieostrymi, takimi jak „niezbędne", „racjonalnie oczekiwany", a także katalogiem otwartym obowiązków („inne wsparcie"). Uwzględniając te trudności interpretacyjne, należy uznać, że obowiązki wsparcia (informacyjnego czy technicznego) odnoszą się ściśle do obowiązków nałożonych na nowego dostawcę (podmiot modyfikujący). Będą to przede wszystkim: informacje dotyczące sposobu działania systemu, wykorzystanych modeli

---

[42] Zob. pkt 84 Preambuły.

[43] L. Riede, O. Talhoff, *Art. 25*, w: *The EU Artificial Intelligence (AI) Act…*, op. cit., s. 531.

lub komponentów, danych treningowych, danych walidacyjnych, dokumentacji technicznej, oceny zgodności, certyfikatów i oznakowań, spełnienia wymogów rozporządzenia. Weryfikacja części danych następuje poprzez sprawdzenie bazy danych utworzonej na podstawie art. 71 AI Act. Zgodnie z załącznikiem VIII sekcją A w bazie muszą zostać umieszczone informacje o przedstawicielu, dołączone kopie deklaracji zgodności UE oraz instrukcji obsługi, a także informacja o certyfikacji. Pozyskanie innych danych wymaga jednak współpracy ze strony pierwotnych dostawców.

Przykładowo, możliwa jest sytuacja, w której właściwy organ krajowy zwraca się w trybie art. 21 ust. 1 do nowego dostawcy o udzielenie informacji. Podmiot ten jednak nie posiada kompletnych informacji, część zdarzeń objętych zapytaniem miała bowiem miejsce przed modyfikacją systemu w rozumieniu ust. 1, a bez posiadania tych informacji dostawca nie może właściwie ocenić np. określonych ryzyk. Podmiot ten zwraca się więc do dostawcy pierwotnego o przekazanie mu tych informacji, w celu przekazania kompletnej informacji, analizy czy oceny.

Żądanie współpracy nie może wykraczać poza informacje i wsparcie niezbędne do prawidłowego wykonania obowiązków wynikających z rozporządzenia, których nowy dostawca nie może uzyskać wykorzystując swoje zasoby osobowe, techniczne, finansowe (lub nakład ten byłby nieproporcjonalnie duży do wysiłku przekazania danych lub wsparcia ze strony pierwotnego dostawcy). W szczególności, obowiązek współpracy nie dotyczy przekazania informacji, dostępów czy innego wsparcia, które nie są niezbędne do wykonania obowiązków wynikających z AI Act, a ukierunkowane są na rozwój gospodarczy nowego dostawcy, uzyskanie przez niego know-how, wsparcia technologicznego, zastąpienia wykorzystania swoich zasobów (wiedzy, środków, czasu, osób) zasobami dostawcy pierwotnego.

Dalej, w art. 25 ust. 4 uregulowano obowiązek zawarcia umowy pomiędzy dostawcą systemu AI wysokiego ryzyka i osobą trzecią dostarczającą system AI lub inne towary czy usługi dla tego systemu, w celu umożliwienia prawidłowego wykonania obowiązków, o jakich mowa w rozporządzeniu. W przepisie wprowadzono – niewystępujące w innych częściach rozporządzenia – pojęcie osoby trzeciej dostarczającej system AI, narzędzia, usługi, komponenty lub procesy, które są wykorzystywane w systemie AI wysokiego ryzyka lub z nim zintegrowane. Do tych osób należą wszystkie podmioty, które dostarczają wymienione w przepisie towary lub usługi do dostarczanego systemu AI wysokiego ryzyka. Przepis ten nakłada na dostawcę obowiązek zawarcia pisemnych umów z tymi podmiotami. Należy odpowiedzieć na pytanie, jakie podmioty dostarczają owe komponenty, a w związku z tym czy umowy należy zawrzeć z ich producentem, dostawcą, a może dystrybutorem, z którym dostawcę łączy stosunek zobowiązaniowy. Należy uznać, że tym podmiotem jest dostawca. Przepis nie wskazuje bowiem ani „osoby trzeciej produkującej" ani „osoby trzeciej dystrybuującej", lecz „osobę trzecią dostarczającą".

Wyłączenie spod tego obowiązku dotyczy osób trzecich udostępniających publicznie, na podstawie bezpłatnej licencji otwartego oprogramowania narzędzia, usługi, procesy lub komponenty inne niż modele AI ogólnego przeznaczenia. Oznacza to, że dostawca korzystający z takich towarów lub usług nie musi zawierać umowy, o jakiej mowa w zdaniu pierwszym przepisu. W motywach 102 i 103 AI

Act doprecyzowano, co stanowi bezpłatną i otwartą licencję[44]. Oprogramowanie to będzie co do zasady rozpowszechniane w postaci kodu źródłowego, w otwartych repozytoriach. Zgodnie z motywem 89 Preambuły ma to na celu zwolnienie podmiotów pracujących na podstawie wolnych i otwartych licencji z odpowiedzialności w całym łańcuchu wartości.

Przykładem repozytorium, w którym publikowane są kody źródłowe algorytmów na otwartej licencji, jest MIT. Wykluczone z omawianego wyjątku są modele AI ogólnego przeznaczenia, zdefiniowane w art. 3 pkt 63 AI Act. Regulacja rozróżnia przy tym system od modelu AI ogólnego przeznaczenia. Podczas gdy popularny ChatGPT jest systemem, modelem będzie np. GPT-4o.

W drugim akapicie przepisu wskazuje się, że Urząd ds. AI może opracować i zalecić dobrowolne wzorcowe postanowienia umowne dla umów zawieranych między dostawcami systemów AI wysokiego ryzyka a osobami trzecimi. Wzory umów pozostaną jednak niewiążące i z pewnością na dużym poziomie ogólności, uwzględniając specyfikę branż, których postanowienia umowne będą dotyczyć. Z pewnością jednak zawierać będą dobre praktyki umowne, stanowiące cenną wskazówkę, jak osiągnąć zgodność umów z wymogami AI Act. Konieczne będzie jednak dostosowanie wzorów do specyfiki systemu AI wysokiego ryzyka, jego celu, zastosowania, podmiotów stosujących, branży.

PODSUMOWANIE

Podsumowując, wskazać należy, że identyfikacja tego, jaką rolę w łańcuchu dostaw systemów AI wysokiego ryzyka pełni dany podmiot, jest bardzo istotna. Prawodawca unijny obciążył importerów oraz dystrybutorów w znacznej mierze obowiązkami weryfikacyjnymi. Większość ciężaru stanowi odwołanie do obowiązków nałożonych na dostawców i konieczność sprawdzenia, czy uczyniono im zadość. W znacznej mierze są to obowiązki formalnej weryfikacji, czy dana procedura lub zadanie zostały przeprowadzone, bez konieczności analizy prawidłowości ich wykonania. Regulacje w zakresie obowiązków nałożonych na importera i dystrybutora są zbliżone. Niekiedy występują różnice w ich sformułowaniu, przypuszczać jednak należy, że nie będą one miały istotnego znaczenia w praktyce. Nie przekreśla to jednak faktu, że zasadniczo obowiązki dystrybutorów są bardziej ograniczone niż obowiązki importerów, na których spoczywa ciężar pierwotnej weryfikacji spełnienia tego obowiązku. Wynika to z faktu, że relacja importera i dostawcy jest co do zasady bliższa niż relacja dystrybutora i dostawcy.

Inaczej wygląda sytuacja podmiotów stosujących systemy AI wysokiego ryzyka. Obowiązki nałożone na te podmioty nie mają zazwyczaj charakteru wtórnego wobec obowiązków dostawców. Są odrębnymi zadaniami, wynikającymi z chęci przeciwdziałania zagrożeniom, jakie niesie za sobą etap stosowania systemów AI wysokiego ryzyka. Prawodawca unijny przyjął – jak się wydaje, słusznie – że na

[44] Zob. pkt 102 i 103 Preambuły.

etapie tym może dojść do naruszeń w zakresie praw człowieka, mimo prawidłowego wywiązania się z obowiązków ukierunkowanych na minimalizowanie tych ryzyk na etapie tworzenia i dystrybuowania systemów AI wysokiego ryzyka. Podmioty stosujące mają bowiem niezwykle istotny wpływ na to, w jaki sposób ostatecznie systemy te będą stosowane, jak chronione będą dane, w jaki sposób wykorzystywane czy weryfikowane będą ich wyniki oraz procedura ich uzyskania.

Szczególną sytuacją jest ta, w której ingerencja w systemy AI powoduje, że na podmiot niebędący dostawcą nałożone zostają obowiązki zrównane z obowiązkami dostawców systemów AI wysokiego ryzyka. Jest tak dlatego, że systemy oparte na technologii sztucznej inteligencji są podatne na m.in. na zmiany ich przeznaczenia, w sposób niezależny od sposobów ich zaprojektowania oraz woli dostawców. Nie jest więc w takich przypadkach uzasadnione obciążanie dostawców odpowiedzialnością za zgodność ich funkcjonowania z wytycznymi rozporządzenia. Należy więc każdorazowo pamiętać, że zakres obowiązków importera, dystrybutora i podmiotu stosującego może ewoluować w zależności od okoliczności i zrównać z obowiązkami dostawców systemów AI wysokiego ryzyka.

BIBLIOGRAFIA

Edwards L., *The EU AI Act: A Summary of Its Significance and Scope*, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf.

Enqvist L., *'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?*, „Law, Innovation and Technology" 2023, nr 15 (2).

Fülöp T., Poindl P., *Art. 27*, w: *The EU Artificial Intelligence (AI) Act: A Commentary*, red. C.N. Pehlivan, N. Forgó, P. Valcke, Alphen aan den Rijn: Wolters Kluwer Law International, 2025.

Hewson K., *The Roles of the Provider and Deployer in AI Systems and Models*, https://www.stephensonharwood.com/insights/the-roles-of-the-provider-and-deployer-in-ai-systems-and-models.

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

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, nr 54.

Ministerstwo Pracy i i Polityki Społecznej, *Profilowanie pomocy dla osób bezrobotnych. Podręcznik dla pracowników powiatowych urzędów pracy*, 2014, https://panoptykon.org/sites/default/files/podrecznik_profilowania.pdf.

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.

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, nr 54 (2).

Riede L., Talhoff O., *Art. 23*, w: *The EU Artificial Intelligence (AI) Act: A Commentary*, C.N. Pehlivan, N. Forgó, P. Valcke, Alphen aan den Rijn: Wolters Kluwer Law International, 2025.

Riede L., Talhoff O., *Art. 24*, w: *The EU Artificial Intelligence (AI) Act: A Commentary*, C.N. Pehlivan, N. Forgó, P. Valcke, Alphen aan den Rijn: Wolters Kluwer Law International, 2025.

Riede L., Talhoff O., *Art. 25*, w: *The EU Artificial Intelligence (AI) Act: A Commentary*, C.N. Pehlivan, N. Forgó, P. Valcke, Alphen aan den Rijn: Wolters Kluwer Law International, 2025.

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

Weitkunat R., Bestle M., *Computerized Mackworth Vigilance Clock Test*, „Computer Methods and Programs in Biomedicine" 1990, nr 32 (2).

Cytuj jako:

Kiejnich-Kruk K., *Obowiązki importerów, dystrybutorów i podmiotów stosujących systemy AI wysokiego ryzyka na gruncie AI Act*, „Ius Novum" 2025, nr 4 (19), s. 129–149. DOI: 10.26399/iusnovum.v19.4.2025.40/k.kiejnich-kruk