Rada
Unii Europejskiej

Bruksela, 23 kwietnia 2021 r.
(OR. en)

8115/21

Międzyinstytucjonalny numer referencyjny:
2021/0106 (COD)

TELECOM 156
JAI 429
COPEN 191
CYBER 108
DATAPROTECT 103
EJUSTICE 41
COSI 69
IXIM 74
ENFOPOL 148
FREMP 103
RELEX 347
MI 271
COMPET 275
IA 60
CODEC 573

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	22 kwietnia 2021 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2021) 206 final
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY USTANAWIAJĄCEGO ZHARMONIZOWANE PRZEPISY DOTYCZĄCE SZTUCZNEJ INTELIGENCJI (AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI) I ZMIENIAJĄCE NIEKTÓRE AKTY USTAWODAWCZE UNII

Delegacje otrzymują w załączeniu dokument COM(2021) 206 final.

Zał.: COM(2021) 206 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 21.4.2021 r.
COM(2021) 206 final

2021/0106 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

USTANAWIAJĄCE ZHARMONIZOWANE PRZEPISY DOTYCZĄCE SZTUCZNEJ INTELIGENCJI (AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI) I ZMIENIAJĄCE NIEKTÓRE AKTY USTAWODAWCZE UNII

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

1.1. Przyczyny i cele wniosku

Niniejsze uzasadnienie towarzyszy wnioskowi dotyczącemu rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji). Sztuczna inteligencja (AI) to szybko rozwijająca się grupa technologii, które mogą przynosić wiele różnych korzyści społeczno-ekonomicznych we wszystkich branżach i obszarach działalności społecznej. Rozwiązania bazujące na sztucznej inteligencji umożliwiają lepsze prognozowanie, optymalizację operacji i przydzielania zasobów oraz personalizację świadczonych usług, dzięki czemu osiągane wyniki są korzystne z punktu widzenia kwestii społecznych i ochrony środowiska, a przedsiębiorstwa i europejska gospodarka zyskują kluczową przewagę konkurencyjną. Takie działania są szczególnie potrzebne w sektorach o dużym wpływie, w tym w obszarze zmiany klimatu oraz ochrony środowiska i zdrowia, w sektorze publicznym, w obszarze finansów, mobilności, spraw wewnętrznych i rolnictwie. Te same elementy i techniki, które przynoszą korzyści społeczno-ekonomiczne wynikające ze stosowania sztucznej inteligencji, jednocześnie wiążą się również jednak z nowymi rodzajami ryzyka lub niekorzystnymi konsekwencjami odczuwanymi przez osoby fizyczne lub społeczeństwo. W związku z tempem zachodzących zmian technologicznych i w świetle potencjalnych wyzwań UE dąży do wypracowania odpowiednio wyważonego podejścia. W interesie Unii leży utrzymanie wiodącej pozycji UE w zakresie technologii i zapewnienie, aby Europejczycy mogli korzystać z nowych technologii opracowanych i funkcjonujących zgodnie z unijnymi wartościami, prawami podstawowymi i zasadami.

Niniejszy wniosek służy realizacji politycznego zobowiązania podjętego przez przewodniczącą Ursulę von der Leyen – w wytycznych politycznych dla Komisji na lata 2019–2024 „Unia, która mierzy wyżej”[1] przewodnicząca ogłosiła, że Komisja zaproponuje przepisy w sprawie skoordynowanego europejskiego podejścia do społecznych i etycznych konsekwencji sztucznej inteligencji. W związku z tą zapowiedzią w dniu 19 lutego 2020 r. Komisja opublikowała białą księgę w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania[2]. W tej białej księdze określono warianty strategiczne dotyczące sposobów osiągnięcia podwójnego celu, jakim jest promowanie stosowania sztucznej inteligencji i zajęcie się zagrożeniami związanymi z niektórymi zastosowaniami tej nowej technologii. Niniejszy wniosek służy osiągnięciu tego drugiego celu na potrzeby budowania ekosystemu zaufania poprzez zaproponowanie ram prawnych dotyczących godnej zaufania sztucznej inteligencji. Niniejszy wniosek opiera się na unijnych wartościach i prawach podstawowych i ma przyczynić się do tego, by obywatele i inni użytkownicy obdarzyli zaufaniem i zaakceptowali rozwiązania oparte na sztucznej inteligencji, a przedsiębiorstwa chętniej opracowywały takie rozwiązania. Sztuczna inteligencja powinna działać na rzecz ludzi i społeczeństwa, a ostatecznym celem jest zwiększenie dobrostanu człowieka. Przepisy dotyczące sztucznej inteligencji, która jest dostępna na rynku Unii lub w inny sposób wpływa na obywateli Unii, powinny zatem być ukierunkowane na człowieka, aby ludzie mogli mieć pewność, że technologię tę wykorzystuje się w sposób bezpieczny i zgodny z prawem, w tym z poszanowaniem praw podstawowych. Po publikacji przedmiotowej białej księgi Komisja

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[2] Komisja Europejska „Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania”, COM(2020) 65 final, 2020 r.

rozpoczęła szeroko zakrojone konsultacje z zainteresowanymi stronami, w których udział wzięło duże grono zainteresowanych stron, a większość z nich poparła interwencję regulacyjną, aby zaradzić wyzwaniom i obawom związanym z rosnącym wykorzystaniem sztucznej inteligencji.

Niniejszy wniosek stanowi również odpowiedź na wyraźne apele ze strony Parlamentu Europejskiego (PE) i Rady Europejskiej, które wielokrotnie wzywały do podjęcia działań ustawodawczych w celu zapewnienia prawidłowego funkcjonowania rynku wewnętrznego systemów sztucznej inteligencji, na którym na szczeblu unijnym należycie uwzględnia się zarówno korzyści, jak i zagrożenia związane ze sztuczną inteligencją. Niniejszy wniosek służy realizacji celu, jakim jest osiągnięcie przez Unię pozycji światowego lidera, jeśli chodzi o rozwój bezpiecznej, wiarygodnej i etycznej sztucznej inteligencji, zgodnie z konkluzjami Rady Europejskiej[3], oraz zapewnia ochronę zasad etycznych, zgodnie z wyraźnym żądaniem Parlamentu Europejskiego[4].

W 2017 r. Rada Europejska wskazała na potrzebę „świadomości, że nowe trendy wymagają pilnej reakcji", co obejmuje „kwestie takie jak sztuczna inteligencja (...) przy zapewnieniu wysokiego poziomu ochrony danych, praw cyfrowych i standardów etycznych"[5]. W konkluzjach z 2019 r. na temat dokumentu pt. „Skoordynowany plan w sprawie rozwoju i wykorzystania sztucznej inteligencji opracowanej w Europie"[6] Rada podkreśliła również znaczenie zapewnienia pełnego poszanowania praw obywateli Unii i wezwała do zmiany istniejących odnośnych przepisów w celu ich dostosowania do nowych możliwości i wyzwań generowanych przez sztuczną inteligencję. Rada Europejska wezwała również do jasnego określenia zastosowań AI, które należy uznać za zastosowania wysokiego ryzyka[7].

W najnowszych konkluzjach z dnia 21 października 2020 r. wezwano również do sprostania wyzwaniom takim jak efekt czarnej skrzynki, złożoność, stronniczość, pewna nieprzewidywalność i częściowo autonomiczne zachowanie w przypadku niektórych systemów sztucznej inteligencji w celu zapewnienia ich zgodności z prawami podstawowymi i ułatwienia egzekwowania przepisów[8].

Parlament Europejski również prowadzi wiele prac w obszarze sztucznej inteligencji. W październiku 2020 r. przyjął szereg rezolucji związanych ze sztuczną inteligencją, w tym w sprawie aspektów etycznych[9], odpowiedzialności[10] i praw autorskich[11]. W 2021 r. w dalszej

---

3 Rada Europejska, Nadzwyczajne posiedzenie Rady Europejskiej (1 i 2 października 2020 r.) – Konkluzje, EUCO 13/20, 2020, s. 6.

4 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).

5 Rada Europejska, *Posiedzenie Rady Europejskiej (19 października 2017 r.) – Konkluzje* EUCO 14/17, 2017, s. 8.

6 Rada Unii Europejskiej, *Sztuczna inteligencja b) Konkluzje na temat skoordynowanego planu w sprawie sztucznej inteligencji – Przyjęcie* 6177/19, 2019.

7 Rada Europejska, *Nadzwyczajne posiedzenie Rady Europejskiej (1 i 2 października 2020 r.) – Konkluzje*, EUCO 13/20, 2020 r.

8 Rada Unii Europejskiej, *Konkluzje prezydencji – Karta praw podstawowych w kontekście sztucznej inteligencji i przemian cyfrowych*, 11481/20, 2020 r.

9 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).

10 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję, 2020/2014(INL).

11 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji, 2020/2015(INI).

kolejności przyjęto rezolucje w sprawie sztucznej inteligencji w sprawach karnych[12] i w sektorze edukacji i kultury oraz w sektorze audiowizualnym[13]. W rezolucji Parlamentu Europejskiego w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii zalecono w szczególności, aby Komisja zaproponowała działania ustawodawcze w celu wykorzystania możliwości i korzyści związanych ze sztuczną inteligencją, a jednocześnie w celu zapewnienia ochrony zasad etycznych. Rezolucja ta zawiera tekst wniosku ustawodawczego dotyczącego rozporządzenia w sprawie zasad etycznych dotyczących opracowywania, wdrażania i wykorzystywania sztucznej inteligencji, robotyki i powiązanych z nimi technologii. Zgodnie z zobowiązaniem politycznym podjętym przez przewodniczącą Ursulę von der Leyen w wytycznych politycznych w odniesieniu do rezolucji przyjmowanych przez Parlament Europejski na podstawie art. 225 TFUE w niniejszym wniosku uwzględniono wyżej wymienioną rezolucję Parlamentu Europejskiego z pełnym poszanowaniem zasady proporcjonalności, pomocniczości i lepszego stanowienia prawa.

W tym kontekście politycznym Komisja przedstawia proponowane ramy regulacyjne dotyczące sztucznej inteligencji, którym przyświecają następujące **cele szczegółowe**:

- zapewnienie, aby systemy sztucznej inteligencji wprowadzane do obrotu w Unii i znajdujące się w użyciu były bezpieczne i zgodne z obowiązującym prawem w obszarze praw podstawowych oraz z unijnymi wartościami;
- zapewnienie pewności prawa na potrzeby ułatwienia inwestycji i innowacji w dziedzinie sztucznej inteligencji;
- poprawa zarządzania i skuteczne egzekwowanie obowiązujących przepisów dotyczących praw podstawowych i wymogów bezpieczeństwa mających zastosowanie do systemów sztucznej inteligencji;
- ułatwienie rozwoju jednolitego rynku zgodnych z prawem, bezpiecznych i wiarygodnych zastosowań sztucznej inteligencji oraz zapobieganie fragmentacji rynku.

Aby osiągnąć te cele, we wniosku przedstawiono wyważone i proporcjonalne horyzontalne podejście regulacyjne do sztucznej inteligencji, które to podejście ogranicza się do minimalnych wymogów niezbędnych do zaradzenia ryzyku i problemom związanym ze sztuczną inteligencją bez nadmiernego ograniczania lub utrudniania rozwoju technologicznego lub powodowania w inny sposób nieproporcjonalnego zwiększenia kosztów wprowadzania do obrotu rozwiązań AI. We wniosku ustanowiono solidne i elastyczne ramy prawne. Z jednej strony proponowane ramy są kompleksowe i nie ulegają dezaktualizacji ze względu na określone w nich podstawowe warianty regulacyjne, w tym oparte na zasadach wymogi, które muszą spełniać systemy sztucznej inteligencji. Z drugiej strony we wniosku wprowadzono proporcjonalny system regulacyjny skoncentrowany wokół odpowiednio zdefiniowanego, opartego na analizie ryzyka podejścia regulacyjnego, w ramach którego nie tworzy się niepotrzebnych ograniczeń handlu, a interwencja regulacyjna jest dostosowana do konkretnych sytuacji, w których występują uzasadnione obawy lub w których można

[12] Projekt sprawozdania Parlamentu Europejskiego na temat sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych, 2020/2016(INI).

[13] Projekt sprawozdania Parlamentu Europejskiego w sprawie sztucznej inteligencji w sektorze edukacji i kultury oraz w sektorze audiowizualnym, 2020/2017(INI). W tym kontekście Komisja przyjęła „Plan działania w dziedzinie edukacji cyfrowej na lata 2021–2027. Nowe podejście do kształcenia i szkolenia w epoce cyfrowej", w którym przewidziano opracowanie wytycznych etycznych dotyczących sztucznej inteligencji i wykorzystania danych w kształceniu – komunikat Komisji COM(2020) 624 final.

przypuszczać, że takie obawy wystąpią w niedalekiej przyszłości. Jednocześnie przedmiotowe ramy prawne obejmują elastyczne mechanizmy, dzięki którym ramy te można dynamicznie dostosowywać stosownie do rozwoju technologii i pojawiających się nowych problematycznych sytuacji.

We wniosku określono zharmonizowane przepisy dotyczące opracowywania, wprowadzania do obrotu i wykorzystywania systemów sztucznej inteligencji w Unii zgodnie z proporcjonalnym podejściem opartym na analizie ryzyka. Wniosek zawiera jedną, nieulegającą dezaktualizacji definicję sztucznej inteligencji. We wniosku przewidziano zakaz stosowania niektórych szczególnie szkodliwych praktyk z wykorzystaniem AI, które są sprzeczne z unijnymi wartościami, oraz zaproponowano szczególne ograniczenia i zabezpieczenia w odniesieniu do określonych zastosowań systemów zdalnej identyfikacji biometrycznej do celów egzekwowania prawa. Określono w nim solidną metodykę w zakresie ryzyka na potrzeby zdefiniowania systemów sztucznej inteligencji wysokiego ryzyka, które stanowią znaczne zagrożenie dla zdrowia i bezpieczeństwa lub praw podstawowych człowieka. Zanim takie systemy sztucznej inteligencji będzie można wprowadzić do obrotu w Unii, będą one musiały spełnić szereg horyzontalnych obowiązkowych wymogów dotyczących wiarygodnej sztucznej inteligencji i zostać poddane procedurom oceny zgodności. Przewidywalne, proporcjonalne i jasne obowiązki nałożono również na dostawców i użytkowników takich systemów w celu zapewnienia bezpieczeństwa i poszanowania obowiązujących przepisów dotyczących ochrony praw podstawowych w całym cyklu życia systemów sztucznej inteligencji. W odniesieniu do niektórych szczególnych systemów sztucznej inteligencji proponuje się wyłącznie minimalne obowiązki dotyczące przejrzystości, w szczególności w przypadku stosowania chatbotów lub zmanipulowanych cyfrowo obrazów lub nagrań wideo (tzw. deepfake).

Proponowane przepisy będą egzekwowane za pomocą systemu zarządzania na szczeblu państw członkowskich opartego na już istniejących strukturach oraz mechanizmu współpracy na szczeblu unijnym, w którym to celu zostanie powołana Europejska Rada ds. Sztucznej Inteligencji. Ponadto proponuje się dodatkowe środki służące wsparciu innowacji, w tym w szczególności piaskownice regulacyjne w zakresie AI i inne środki ograniczające obciążenie regulacyjne i wspierające małe i średnie przedsiębiorstwa oraz przedsiębiorstwa typu start-up.

1.2. Spójność z przepisami obowiązującymi w tej dziedzinie polityki

Horyzontalny charakter niniejszego wniosku wymaga zapewnienia pełnej spójności z obowiązującymi przepisami Unii mającymi zastosowanie do sektorów, w których systemy sztucznej inteligencji wysokiego ryzyka już są stosowane lub prawdopodobnie będą stosowane w niedalekiej przyszłości.

Zapewniono również spójność z postanowieniami Karty praw podstawowych Unii Europejskiej i obowiązującym prawem wtórnym Unii dotyczącym ochrony danych, ochrony konsumentów, niedyskryminacji i równouprawnienia płci. Niniejszy wniosek nie narusza przepisów ogólnego rozporządzenia o ochronie danych (rozporządzenie (UE) 2016/679) ani przepisów dyrektywy w sprawie egzekwowania prawa (dyrektywa (UE) 2016/680) oraz uzupełnia przepisy tych aktów, wprowadzając zbiór zharmonizowanych przepisów mających zastosowanie do projektowania, opracowywania i stosowania określonych systemów sztucznej inteligencji wysokiego ryzyka oraz ograniczenia dotyczące określonych zastosowań systemów zdalnej identyfikacji biometrycznej. Ponadto niniejszy wniosek uzupełnia obowiązujące obecnie przepisy prawa Unii dotyczące niedyskryminacji o szczególne wymogi służące ograniczeniu do minimum ryzyka dyskryminacji algorytmicznej, w szczególności w zakresie projektowania i jakości zestawów danych wykorzystywanych do rozwoju

systemów sztucznej inteligencji, w połączeniu z obowiązkami w zakresie testowania, zarządzania ryzykiem, dokumentacji i nadzoru ze strony człowieka w całym cyklu życia systemów sztucznej inteligencji. Niniejszy wniosek pozostaje bez uszczerbku dla stosowania unijnego prawa konkurencji.

Jeżeli chodzi o systemy sztucznej inteligencji wysokiego ryzyka, które stanowią związane z bezpieczeństwem elementy produktów, niniejszy wniosek zostanie włączony do obowiązujących obecnie przepisów sektorowych dotyczących bezpieczeństwa w celu zapewnienia spójności, uniknięcia powielania i ograniczenia do minimum dodatkowych obciążeń. W szczególności, jeżeli chodzi o systemy sztucznej inteligencji wysokiego ryzyka związane z produktami wchodzącymi w zakres nowych ram prawnych (np. maszynami, wyrobami medycznymi, zabawkami), zgodność z wymogami określonymi w niniejszym wniosku w odniesieniu do systemów sztucznej inteligencji będzie sprawdzana w ramach obowiązujących procedur oceny zgodności określonych w odnośnych przepisach składających się na nowe ramy prawne. Jeżeli chodzi o zależności między wymogami, choć zagrożenia dla bezpieczeństwa stwarzane przez systemy sztucznej inteligencji mają być objęte wymogami określonymi w niniejszym wniosku, to jednak przepisy nowych ram prawnych służą zapewnieniu ogólnego bezpieczeństwa produktu końcowego, a zatem mogą zawierać szczególne wymogi dotyczące bezpiecznej integracji systemu sztucznej inteligencji z produktem końcowym. Podejście to zostało w pełni odzwierciedlone we wniosku dotyczącym rozporządzenia w sprawie maszyn, którego data przyjęcia pokrywa się z datą przyjęcia niniejszego wniosku. Niniejszy wniosek nie miałby bezpośredniego zastosowania do systemów sztucznej inteligencji wysokiego ryzyka związanych z produktami objętymi zakresem stosowania odpowiednich przepisów reprezentujących „stare podejście” (dotyczy to np. sektora lotnictwa, samochodów). Przyjmując odpowiednie przepisy wykonawcze lub delegowane na podstawie tych aktów, trzeba będzie jednak brać pod uwagę zasadnicze wymagania *ex ante* dotyczące systemów sztucznej inteligencji wysokiego ryzyka.

Jeżeli chodzi o systemy sztucznej inteligencji zapewniane lub wykorzystywane przez regulowane instytucje kredytowe, organy odpowiedzialne za nadzorowanie wykonania unijnych przepisów dotyczących usług finansowych należy wyznaczyć jako organy właściwe do spraw nadzoru zgodności z wymogami określonymi w niniejszym wniosku w celu zapewnienia spójnego egzekwowania obowiązków określonych w niniejszym wniosku i w unijnych przepisach dotyczących usług finansowych w przypadkach, w których systemy sztucznej inteligencji w określonym stopniu uregulowano w sposób dorozumiany w odniesieniu do systemu zarządzania wewnętrznego instytucji kredytowych. W celu dalszego zwiększenia spójności procedurę oceny zgodności i niektóre spośród spoczywających na dostawcach obowiązków proceduralnych określonych w niniejszym wniosku włączono do procedur określonych w dyrektywie 2013/36/UE w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego[14].

Niniejszy wniosek jest również spójny z mającymi zastosowanie przepisami Unii dotyczącymi usług, w tym usług pośrednictwa uregulowanych w dyrektywie 2000/31/WE

[14] Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE, tekst mający znaczenie dla EOG, Dz.U. L 176 z 27.6.2013, s. 338.

o handlu elektronicznym[15] i w przyjętym niedawno wniosku Komisji dotyczącym aktu o usługach cyfrowych[16].

W odniesieniu do systemów sztucznej inteligencji, które stanowią elementy wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości i są zarządzane przez Agencję Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), niniejszy wniosek nie będzie miał zastosowania do systemów sztucznej inteligencji, które wprowadzono do obrotu lub oddano do użytku przed upływem jednego roku od daty rozpoczęcia stosowania niniejszego rozporządzenia, chyba że na skutek zastąpienia lub zmiany takich aktów prawnych projekt lub przeznaczenie odnośnego systemu sztucznej inteligencji lub odnośnych systemów sztucznej inteligencji ulegną znacznym zmianom.

1.3. Spójność z innymi politykami Unii

Niniejszy wniosek stanowi element większego kompleksowego pakietu środków służących rozwiązaniu problemów zaistniałych w związku z rozwojem i wykorzystywaniem sztucznej inteligencji, które to problemy przeanalizowano w białej księdze w sprawie sztucznej inteligencji. Tym samym zapewniono spójność i komplementarność z innymi realizowanymi lub planowanymi inicjatywami Komisji, które również mają na celu rozwiązanie tych problemów, w tym z inicjatywami służącymi przeglądowi przepisów sektorowych dotyczących produktów (np. dyrektywy w sprawie maszyn, dyrektywy w sprawie ogólnego bezpieczeństwa produktów) oraz inicjatywami, które dotyczą kwestii odpowiedzialności w zakresie nowych technologii, w tym systemów sztucznej inteligencji. Takie inicjatywy będą bazować na niniejszym wniosku oraz go uzupełniać, co służy zapewnieniu jasności prawa i ma sprzyjać rozwojowi ekosystemu zaufania do sztucznej inteligencji w Europie.

Niniejszy wniosek jest również spójny z ogólną strategią cyfrową Komisji, ponieważ stanowi wkład w promowanie technologii przynoszącej korzyści ludziom, czyli jednego z trzech głównych filarów kierunków i celów polityki ogłoszonych w komunikacie pt. „Kształtowanie cyfrowej przyszłości Europy”[17]. We wniosku określono spójne, skuteczne i proporcjonalne ramy w celu zapewnienia, aby sztuczną inteligencję opracowywano z poszanowaniem praw ludzi i w sposób zwiększający zaufanie obywateli do tej technologii, tak aby budować Europę na miarę ery cyfrowej i aby kolejne dziesięć lat można było nazwać **cyfrową dekadą**[18].

Ponadto promowanie innowacji opartych na AI ściśle wiąże się z **aktem w sprawie zarządzania danymi**[19]**, dyrektywą w sprawie otwartych danych**[20] oraz innymi inicjatywami stanowiącymi element **europejskiej strategii w zakresie danych**[21], dzięki

---

15 Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz.U. L 178 z 17.7.2000, s. 1.

16 Zob. wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniającego dyrektywę 2000/31/WE, COM(2020) 825 final.

17 Komunikat Komisji pt. „Kształtowanie cyfrowej przyszłości Europy”, COM(2020) 67 final.

18 Cyfrowy Kompas na 2030 r.: europejska wizja cyfrowej dekady.

19 Wniosek dotyczący rozporządzenia w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) COM(2020) 767.

20 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, PE/28/2019/REV/1, Dz.U. L 172 z 26.6.2019, s. 56.

21 Komunikat Komisji pt. „Europejska strategia w zakresie danych”, COM(2020) 66 final.

którym zostaną ustanowione godne zaufania mechanizmy i usługi w zakresie ponownego wykorzystania, udostępniania i gromadzenia danych kluczowych dla rozwoju wysokiej jakości modeli AI opartych na danych.

Niniejszy wniosek przyczyni się również do znacznego umocnienia roli Unii w kształtowaniu światowych norm i standardów oraz promowaniu wiarygodnej sztucznej inteligencji zgodnej z unijnymi wartościami i interesami. Wniosek stanowi solidną podstawę umożliwiającą Unii podjęcie dalszej współpracy w sprawach związanych ze sztuczną inteligencją z partnerami zewnętrznymi, w tym z państwami trzecimi, oraz na forach międzynarodowych.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

2.1. Podstawa prawna

Podstawę prawną niniejszego wniosku stanowi przede wszystkim art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), w którym przewidziano przyjęcie środków mających na celu zapewnienie ustanowienia i funkcjonowania rynku wewnętrznego.

Niniejszy wniosek stanowi główny element unijnej strategii jednolitego rynku cyfrowego. Głównym celem niniejszego wniosku jest zapewnienie należytego funkcjonowania rynku wewnętrznego poprzez określenie zharmonizowanych przepisów dotyczących w szczególności opracowywania, wprowadzania do obrotu w Unii i wykorzystywania produktów i usług opartych na wykorzystaniu technologii AI lub stanowiących samodzielne systemy sztucznej inteligencji. Niektóre państwa członkowskie rozważają już wprowadzenie przepisów krajowych w celu zapewnienia, aby sztuczna inteligencja była bezpieczna oraz rozwijana i stosowana w sposób zgodny z obowiązkami wynikającymi z praw podstawowych. Takie nieskoordynowane działania prawdopodobnie doprowadzą jednak do powstania dwóch zasadniczych problemów: (i) fragmentacji rynku wewnętrznego pod względem podstawowych elementów, co dotyczy w szczególności wymogów odnoszących się do produktów i usług wykorzystujących AI, wprowadzania do obrotu takich produktów i usług, ich stosowania, odpowiedzialności za nie oraz ich nadzorowania przez organy publiczne, oraz (ii) znacznego spadku pewności prawa – zarówno z punktu widzenia dostawców, jak i użytkowników systemów sztucznej inteligencji – co do tego, w jaki sposób dotychczasowe i nowe przepisy będą miały zastosowanie do takich systemów w Unii. Ze względu na intensywny obrót produktami i usługami ponad granicami najlepszym sposobem na rozwiązanie tego problemu jest przyjęcie unijnego prawodawstwa harmonizującego.

We wniosku określono wspólne obowiązkowe wymogi mające zastosowanie do projektowania i opracowywania określonych systemów sztucznej inteligencji przed ich wprowadzeniem do obrotu, a dalsze funkcjonowanie tych wymogów zostanie zapewnione w oparciu o zharmonizowane normy techniczne. We wniosku uwzględniono również sytuację po wprowadzeniu systemów sztucznej inteligencji do obrotu, harmonizując sposób prowadzenia kontroli *ex post*.

Ponadto, mając na uwadze, że niniejszy wniosek zawiera określone przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w szczególności ograniczenia wykorzystywania systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa, podstawą niniejszego rozporządzenia w zakresie takich przepisów szczegółowych powinien być art. 16 TFUE.

2.2. Pomocniczość (w przypadku kompetencji niewyłącznych)

Charakter sztucznej inteligencji, która często opiera się na dużych i zróżnicowanych zbiorach danych i którą można wbudować do każdego produktu lub usługi będących przedmiotem

swobodnego obrotu na rynku wewnętrznym, sprawia, że państwa członkowskie nie są w stanie samodzielnie osiągnąć celów niniejszego wniosku. Ponadto powstająca mozaika potencjalnie rozbieżnych przepisów krajowych utrudni płynny obrót produktami i usługami związanymi z systemami sztucznej inteligencji w całej UE i będzie nieskuteczna w zapewnianiu bezpieczeństwa i ochrony praw podstawowych oraz wartości unijnych w poszczególnych państwach członkowskich. Podejście krajowe do rozwiązywania tych problemów spowoduje jedynie dodatkowy brak pewności prawa i powstanie dodatkowych barier, a także spowolni wprowadzanie AI na rynek.

Cele niniejszego wniosku można lepiej zrealizować na poziomie Unii, aby uniknąć dalszej fragmentacji jednolitego rynku na potencjalnie sprzeczne ramy krajowe uniemożliwiające swobodny obrót towarów i usług z wbudowaną technologią AI. Solidne europejskie ramy regulacyjne w zakresie wiarygodnej sztucznej inteligencji zapewnią również równe warunki działania oraz ochronę wszystkich obywateli, wzmacniając jednocześnie konkurencyjność i bazę przemysłową Europy w dziedzinie sztucznej inteligencji. Co więcej, jedynie wspólne działanie na szczeblu UE umożliwi ochronę suwerenności cyfrowej Unii oraz wykorzystanie unijnych narzędzi i uprawnień regulacyjnych w celu kształtowania globalnych zasad i norm.

2.3. Proporcjonalność

Wniosek opiera się na istniejących ramach prawnych oraz jest proporcjonalny i niezbędny do osiągnięcia zakładanych w nim celów, ponieważ zastosowano w nim podejście oparte na analizie ryzyka, a obciążenia regulacyjne nakłada się tylko w przypadku, gdy system sztucznej inteligencji może stwarzać wysokie ryzyko dla praw podstawowych i bezpieczeństwa. W przypadku innych systemów sztucznej inteligencji, nieobarczonych wysokim ryzykiem, wprowadzono jedynie bardzo ograniczone obowiązki w zakresie przejrzystości, na przykład w zakresie dostarczania informacji w celu zasygnalizowania wykorzystania systemu sztucznej inteligencji, w przypadku gdy ma miejsce interakcja tego systemu z człowiekiem. W przypadku systemów sztucznej inteligencji wysokiego ryzyka wymogi dotyczące danych wysokiej jakości, dokumentacji i identyfikowalności, przejrzystości, nadzoru ze strony człowieka, dokładności i solidności są absolutnie niezbędne, aby złagodzić stwarzane przez AI ryzyko dla praw podstawowych i bezpieczeństwa, którego nie obejmują istniejące ramy prawne. Normy zharmonizowane oraz towarzyszące im wytyczne i narzędzia zapewniające przestrzeganie przepisów pomogą dostawcom i użytkownikom w spełnieniu wymogów określonych we wniosku oraz zminimalizują ich koszty. Koszty ponoszone przez podmioty gospodarcze są proporcjonalne do realizowanych celów oraz korzyści gospodarczych i korzyści pod względem reputacji, jakich podmioty gospodarcze mogą oczekiwać od niniejszego wniosku.

2.4. Wybór instrumentu

Wybór rozporządzenia jako instrumentu prawnego jest uzasadniony potrzebą jednolitego stosowania nowych przepisów, takich jak definicja sztucznej inteligencji, zakaz określonych szkodliwych praktyk opartych na sztucznej inteligencji oraz klasyfikacja określonych systemów sztucznej inteligencji. Rozporządzenie, jako instrument, który zgodnie z art. 288 TFUE ma bezpośrednie zastosowanie, ograniczy rozdrobnienie prawne i ułatwi rozwój jednolitego rynku zgodnych z prawem, bezpiecznych i wiarygodnych systemów sztucznej inteligencji. Cel ten zostanie osiągnięty w szczególności poprzez wprowadzenie zharmonizowanego zestawu podstawowych wymogów w odniesieniu do systemów sztucznej inteligencji sklasyfikowanych jako systemy wysokiego ryzyka oraz obowiązków dostawców i użytkowników tych systemów, co poprawi ochronę praw podstawowych i zapewni pewność prawa zarówno podmiotom gospodarczym, jak i konsumentom.

Jednocześnie przepisy rozporządzenia nie są nadmiernie nakazowe i pozostawiają przestrzeń na różne wielowymiarowe działania państw członkowskich w odniesieniu do elementów, które nie podważają celów inicjatywy, w szczególności jeśli chodzi o wewnętrzną organizację systemu nadzoru rynku oraz wprowadzanie środków mających wspierać innowacyjność.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

3.1. Konsultacje z zainteresowanymi stronami

Niniejszy wniosek jest wynikiem szeroko zakrojonych konsultacji ze wszystkimi głównymi zainteresowanymi stronami, w których to konsultacjach zastosowano ogólne zasady i minimalne normy w zakresie konsultacji Komisji z zainteresowanymi stronami.

W dniu 19 lutego 2020 r. wraz z publikacją białej księgi w sprawie sztucznej inteligencji rozpoczęto **internetowe konsultacje publiczne**, które trwały do dnia 14 czerwca 2020 r. Celem tych konsultacji było zebranie poglądów i opinii na temat białej księgi. Były one skierowane do wszystkich zainteresowanych stron z sektora publicznego i prywatnego, w tym rządów, władz lokalnych, organizacji komercyjnych i niekomercyjnych, partnerów społecznych, ekspertów, środowiska akademickiego i obywateli. Po przeanalizowaniu wszystkich otrzymanych odpowiedzi Komisja opublikowała na swojej stronie internetowej podsumowanie wyników oraz poszczególne odpowiedzi[22].

Łącznie otrzymano 1215 odpowiedzi, z czego: 352 od przedsiębiorstw lub organizacji/stowarzyszeń biznesowych, 406 od osób fizycznych (z czego 92 % od osób fizycznych z UE), 152 w imieniu instytucji naukowych/badawczych oraz 73 od organów publicznych. Społeczeństwo obywatelskie reprezentowało 160 respondentów (w tym 9 organizacji konsumenckich, 129 organizacji pozarządowych i 22 związki zawodowe), 72 respondentów wypowiedziało się jako „inni”. Spośród 352 przedstawicieli biznesu i przemysłu 222 stanowiły przedsiębiorstwa i przedstawiciele przedsiębiorstw, z czego 41,5 % to mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa. Resztę stanowiły stowarzyszenia przedsiębiorców. Ogółem 84 % odpowiedzi udzielonych przez przedstawicieli biznesu i przemysłu pochodziło z UE-27. W zależności od pytania od 81 do 598 respondentów skorzystało z opcji dowolnego tekstu w celu wprowadzenia uwag. Za pośrednictwem strony internetowej EU Survey przedłożono ponad 450 stanowisk – były one albo dołączone do odpowiedzi na pytania zawarte w kwestionariuszu (ponad 400), albo stanowiły samodzielne opinie (ponad 50).

Zasadniczo zainteresowane strony są zgodne co do konieczności podjęcia działania. Znaczna większość zainteresowanych stron zgadza się, że istnieje luka prawna lub że konieczne jest wprowadzenie nowych przepisów. Szereg zainteresowanych stron ostrzega jednak Komisję, aby unikała powielania przepisów, sprzecznych obowiązków i nadmiernej regulacji. W wielu uwagach podkreślono znaczenie proporcjonalnych ram regulacyjnych, które byłyby neutralne pod względem technologicznym.

Zainteresowane strony w większości domagały się wąskiej, jasnej i precyzyjnej definicji sztucznej inteligencji. Zainteresowane strony podkreśliły również, że oprócz wyjaśnienia terminu „sztuczna inteligencja”, ważne jest zdefiniowanie „ryzyka”, „wysokiego ryzyka”, „niskiego ryzyka”, „zdalnej identyfikacji biometrycznej” oraz „szkody”.

[22] Wszystkie wyniki konsultacji można znaleźć tutaj.

Większość respondentów jednoznacznie opowiada się za podejściem opartym na analizie ryzyka. Uznano, że zastosowanie ram opartych na analizie ryzyka jest lepszym rozwiązaniem niż ogólne uregulowanie wszystkich systemów sztucznej inteligencji. Rodzaje ryzyka i zagrożeń powinny być ustalane na podstawie indywidualnego podejścia do każdego sektora i każdego przypadku. Ryzyko należy również kalkulować, biorąc pod uwagę wpływ na prawa i bezpieczeństwo.

Piaskownice regulacyjne mogłyby być bardzo przydatne w promowaniu AI i niektóre zainteresowane strony przyjmują je z zadowoleniem, zwłaszcza stowarzyszenia przedsiębiorców.

Spośród osób, które wyraziły swoją opinię na temat modeli egzekwowania przepisów, ponad 50 %, zwłaszcza przedstawicieli stowarzyszeń przedsiębiorców, opowiedziało się za połączeniem dokonywanej *ex ante* samooceny ryzyka i egzekwowania *ex post* w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka.

3.2. Gromadzenie i wykorzystanie wiedzy eksperckiej

Wniosek opiera się na dwuletniej analizie i dużym zaangażowaniu zainteresowanych stron, w tym środowisk akademickich, przedsiębiorstw, partnerów społecznych, organizacji pozarządowych, państw członkowskich i obywateli. Prace przygotowawcze rozpoczęły się w 2018 r. od powołania **grupy ekspertów wysokiego szczebla ds. AI** o pluralistycznym i szerokim składzie, w której zasiada 52 znanych ekspertów, których zadaniem jest doradzanie Komisji w kwestiach realizacji strategii Komisji w sprawie sztucznej inteligencji. W kwietniu 2019 r. Komisja poparła[23] kluczowe wymogi określone w wytycznych w zakresie etyki dotyczących godnej zaufania sztucznej inteligencji[24] opracowanych przez grupę ekspertów wysokiego szczebla ds. AI, które zmieniono w celu uwzględnienia ponad 500 uwag otrzymanych od zainteresowanych stron. W kluczowych wymogach odzwierciedlono powszechnie stosowane i wspólne podejście, o czym świadczy duża liczba kodeksów i zasad etycznych opracowanych przez wiele organizacji prywatnych i publicznych w Europie i poza nią, zgodnie z którym w rozwijaniu i wykorzystywaniu AI należy kierować się pewnymi podstawowymi zasadami opartymi na wartościach. Dzięki liście kontrolnej dla godnej zaufania sztucznej inteligencji (ALTAI)[25] wprowadzono te wymagania w życie w ramach procesu pilotażowego z udziałem ponad 350 organizacji.

Ponadto powołano **sojusz na rzecz sztucznej inteligencji**[26] jako platformę, na której około 4 000 zainteresowanych stron będzie mogło prowadzić dyskusje na temat technologicznych i społecznych konsekwencji sztucznej inteligencji, których zwieńczeniem będzie coroczne zgromadzenie poświęcone sztucznej inteligencji.

W **białej księdze** w sprawie sztucznej inteligencji jeszcze bardziej rozwinięto to pluralistyczne podejście, co zachęciło ponad 1 250 zainteresowanych stron do zgłoszenia uwag, w tym ponad 450 dodatkowych stanowisk. W związku z tym Komisja opublikowała

---

23 Komisja Europejska, *Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka*, COM(2019) 168.

24 Grupa ekspertów wysokiego szczebla ds. AI, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, 2019 r.

25 Grupa ekspertów wysokiego szczebla ds. AI, *Lista kontrolna dla godnej zaufania sztucznej inteligencji (ALTAI) do celów samooceny*, 2020 r.

26 Sojusz na rzecz sztucznej inteligencji to wielostronne forum, które uruchomiono w czerwcu 2018 r., sojusz na rzecz AI https://ec.europa.eu/digital-single-market/en/european-ai-alliance

wstępną ocenę skutków, w odpowiedzi na którą przesłano z kolei ponad 130 uwag[27]. **Zorganizowano również dodatkowe warsztaty i wydarzenia** dla zainteresowanych stron, których wyniki wykorzystano w analizie zawartej w ocenie skutków oraz przy wyborze wariantów strategicznych na potrzeby niniejszego wniosku[28]. Zamówiono również **badanie zewnętrzne**, które stanowi część oceny skutków.

3.3. Ocena skutków

Zgodnie ze swoją strategią „lepszego stanowienia prawa" Komisja przeprowadziła ocenę skutków w odniesieniu do niniejszego wniosku, która została zbadana przez działającą przy Komisji Radę ds. Kontroli Regulacyjnej. W dniu 16 grudnia 2020 r. odbyło się spotkanie z Radą ds. Kontroli Regulacyjnej, po którym Rada wydała negatywną opinię. Po wprowadzeniu istotnych zmian w ocenie skutków w celu uwzględnienia uwag oraz po ponownym przedłożeniu oceny skutków w dniu 21 marca 2021 r. Rada ds. Kontroli Regulacyjnej wydała pozytywną opinię. Opinie Rady ds. Kontroli Regulacyjnej, zalecenia oraz wyjaśnienie sposobu ich uwzględnienia przedstawiono w załączniku 1 do oceny skutków.

Komisja zbadała różne warianty strategiczne, aby osiągnąć ogólny cel niniejszego wniosku polegający na **zapewnieniu prawidłowego funkcjonowania jednolitego rynku** przez stworzenie warunków sprzyjających rozwijaniu i wykorzystywaniu w Unii wiarygodnej sztucznej inteligencji.

Oceniono cztery warianty strategiczne zakładające różny stopień interwencji regulacyjnej:

- **wariant 1**: instrument legislacyjny UE ustanawiający dobrowolny system etykietowania;
- **wariant 2**: podejście sektorowe ad hoc;
- **wariant 3**: horyzontalny instrument legislacyjny UE uwzględniający proporcjonalne podejście oparte na analizie ryzyka;
- **wariant 3+**: horyzontalny instrument legislacyjny UE uwzględniający proporcjonalne podejście oparte na analizie ryzyka + kodeksy postępowania dotyczące systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem;
- **wariant 4**: horyzontalny instrument legislacyjny UE ustanawiający obowiązkowe wymogi dotyczące wszystkich systemów sztucznej inteligencji, niezależnie od ryzyka, jakie stwarzają.

Zgodnie z przyjętą przez Komisję metodyką każdy wariant strategiczny oceniono pod kątem skutków gospodarczych i społecznych, ze szczególnym uwzględnieniem skutków dla praw podstawowych. Preferowanym wariantem jest wariant 3+, czyli ramy regulacyjne dotyczące wyłącznie systemów sztucznej inteligencji wysokiego ryzyka, przewidujące jednocześnie możliwość przyjęcia kodeksu postępowania, do którego mogliby się dobrowolnie stosować wszyscy dostawcy systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem. Wymogi – obowiązkowe dla systemów sztucznej inteligencji wysokiego ryzyka – będą dotyczyć danych, dokumentacji i identyfikowalności, dostarczania informacji i przejrzystości, nadzoru ze strony człowieka oraz solidności i dokładności. Przedsiębiorstwa, które zechcą

---

[27] Komisja Europejska, *Wstępna ocena skutków w sprawie wniosku dotyczącego aktu prawnego Parlamentu Europejskiego i Rady ustanawiającego wymogi dotyczące sztucznej inteligencji.*

[28] Szczegółowe informacje na temat wszystkich przeprowadzonych konsultacji znajdują się w załączniku 2 do oceny skutków.

wprowadzić kodeksy postępowania w odniesieniu do innych systemów sztucznej inteligencji, robiłyby to dobrowolnie.

Uznano, iż preferowany wariant będzie odpowiedni, aby w najbardziej skuteczny sposób przyczynić się do osiągnięcia celów niniejszego wniosku. Wymagając od twórców i użytkowników AI ograniczonego, ale skutecznego zestawu działań, preferowany wariant ogranicza ryzyko naruszenia praw podstawowych i bezpieczeństwa ludzi oraz sprzyja skutecznemu nadzorowi i egzekwowaniu poprzez ukierunkowanie wymogów wyłącznie na systemy, w przypadku których istnieje wysokie ryzyko wystąpienia takich naruszeń. W rezultacie wariant ten pozwala utrzymać koszty przestrzegania przepisów na minimalnym poziomie, dzięki czemu można będzie uniknąć niepotrzebnego spowolnienia absorpcji ze względu na wyższe ceny i koszty przestrzegania przepisów. Aby zaradzić ewentualnym niekorzystnym skutkom dla MŚP, wariant ten obejmuje szereg przepisów mających na celu ułatwienie przestrzegania przez nie przepisów i obniżenie ponoszonych przez nie kosztów, w tym utworzenie piaskownic regulacyjnych oraz obowiązek uwzględniania interesów MŚP przy ustalaniu opłat związanych z oceną zgodności.

Preferowany wariant zwiększy zaufanie ludzi do AI, przedsiębiorstwa zyskają pewność prawa, a państwa członkowskie nie będą miały powodu do podejmowania jednostronnych działań, które mogłyby doprowadzić do fragmentacji jednolitego rynku. W wyniku większego popytu wynikającego z większego zaufania, większej dostępności ofert dzięki pewności prawa oraz braku przeszkód w transgranicznym przepływie systemów sztucznej inteligencji jednolity rynek AI powinien dynamicznie rozwinąć się. Unia Europejska będzie nadal rozwijać szybko rosnący ekosystem sztucznej inteligencji, obejmujący innowacyjne usługi i produkty z wbudowaną technologią sztucznej inteligencji lub samodzielne systemy sztucznej inteligencji, co doprowadzi do zwiększenia autonomii cyfrowej.

Przedsiębiorstwa lub organy publiczne, które opracowują lub wykorzystują zastosowania AI stanowiące wysokie ryzyko dla bezpieczeństwa lub praw podstawowych obywateli, musiałyby spełnić szczególne wymogi i obowiązki. Spełnienie tych wymogów oznaczałoby konieczność poniesienia do 2025 r. kosztów w wysokości około 6 000 EUR do 7 000 EUR w przypadku udostępnienia systemu sztucznej inteligencji wysokiego ryzyka o wartości około 170 000 EUR. W przypadku użytkowników AI dochodziłby jeszcze roczny koszt czasu poświęconego na zapewnienie nadzoru ze strony człowieka, gdy jest to właściwe, w zależności od przypadku użycia. Koszt ten oszacowano na około 5 000 EUR do 8 000 EUR rocznie. Koszty weryfikacji mogłyby wynieść od 3 000 EUR do 7 500 EUR w przypadku dostawców AI wysokiego ryzyka. W odniesieniu do przedsiębiorstw lub organów publicznych, które opracowują lub wykorzystują AI w ramach zastosowania niesklasyfikowanego jako zastosowanie wysokiego ryzyka, obowiązek informacyjny miałby zastosowanie w minimalnym zakresie. Mogłyby one jednak zdecydować się dołączyć do innych i wspólnie przyjąć kodeks postępowania, zobowiązując się do przestrzegania odpowiednich wymogów, co dałoby pewność, że ich systemy sztucznej inteligencji są wiarygodne. W takim przypadku koszty byłyby co najwyżej równe kosztom ponoszonym w przypadku systemów sztucznej inteligencji wysokiego ryzyka, choć najprawdopodobniej byłyby niższe.

Wpływ wariantów strategicznych na różne kategorie zainteresowanych stron (podmioty gospodarcze/przedsiębiorstwa; jednostki oceniające zgodność, organy normalizacyjne i inne podmioty publiczne; osoby fizyczne/obywateli; naukowców) wyjaśniono szczegółowo w załączniku 3 do oceny skutków uzupełniającej niniejszy wniosek.

3.4. Sprawność regulacyjna i uproszczenie

W niniejszym wniosku ustanawia się obowiązki, które będą miały zastosowanie do dostawców i użytkowników systemów sztucznej inteligencji wysokiego ryzyka. W przypadku dostawców, którzy opracowują i wprowadzają takie systemy na rynek unijny, stworzy to pewność prawa i zapewni brak przeszkód w transgranicznym świadczeniu usług i oferowaniu produktów związanych z AI. W przypadku przedsiębiorstw korzystających z AI pozwoli to zwiększyć zaufanie wśród ich klientów. W przypadku krajowych administracji publicznych pozwoli to zbudować zaufanie społeczeństwa do wykorzystywania sztucznej inteligencji i wzmocni mechanizmy egzekwowania prawa (poprzez wprowadzenie europejskiego mechanizmu koordynacji, zapewnienie odpowiedniego potencjału i ułatwienie kontroli systemów sztucznej inteligencji dzięki wprowadzeniu nowych wymogów w zakresie dokumentacji, identyfikowalności i przejrzystości). Ponadto w ramach tych zostaną uwzględnione szczególne środki wspierające innowacyjność, w tym piaskownice regulacyjne oraz szczególne środki mające wspierać drobnych użytkowników i dostawców systemów sztucznej inteligencji wysokiego ryzyka w przestrzeganiu nowych przepisów.

Wniosek ma również na celu wzmocnienie konkurencyjności i bazy przemysłowej Europy w dziedzinie sztucznej inteligencji. Zapewniono w nim pełną spójność z istniejącymi sektorowymi przepisami Unii mającymi zastosowanie do systemów sztucznej inteligencji (np. dotyczących produktów i usług), co zapewni większą jasność i uprości egzekwowanie nowych przepisów.

3.5. Prawa podstawowe

Wykorzystywanie sztucznej inteligencji wraz z jej szczególnymi cechami (np. efekt czarnej skrzynki, złożoność, zależność od danych, autonomiczne zachowanie) może mieć negatywny wpływ na szereg praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej („Karta"). Niniejszy wniosek ma na celu zapewnienie wysokiego poziomu ochrony tych praw podstawowych i zmierza do uwzględnienia różnych źródeł ryzyka poprzez jasno określone podejście oparte na analizie ryzyka. Dzięki zestawowi wymogów dotyczących wiarygodnej sztucznej inteligencji oraz proporcjonalnym obowiązkom nałożonym na wszystkich uczestników łańcucha wartości wniosek wzmocni i będzie promował ochronę praw chronionych Kartą, do których zaliczają się: prawo do godności człowieka (art. 1), poszanowanie życia prywatnego i ochrona danych osobowych (art. 7 i 8), niedyskryminacja (art. 21) oraz równość kobiet i mężczyzn (art. 23). Ma on na celu zapobieganie ograniczaniu prawa do wolności wypowiedzi (art. 11) i wolności zgromadzania się (art. 12), zapewnienie ochrony prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawa do obrony i domniemania niewinności (art. 47 i 48), jak również ogólnej zasady dobrej administracji. Ponadto, w razie potrzeby w określonych dziedzinach, wniosek będzie miał pozytywny wpływ na prawa wielu szczególnych grup, takie jak prawa pracowników do należytych i sprawiedliwych warunków pracy (art. 31), wysoki poziom ochrony konsumentów (art. 28), prawa dziecka (art. 24) oraz integracja osób niepełnosprawnych (art. 26). Istotne jest również prawo do wysokiego poziomu ochrony środowiska i poprawa jego jakości (art. 37), w tym w odniesieniu do zdrowia i bezpieczeństwa ludzi. Obowiązki w zakresie testowania *ex ante*, zarządzania ryzykiem i nadzoru ze strony człowieka ułatwią również poszanowanie innych praw podstawowych poprzez zminimalizowanie ryzyka błędnych lub stronniczych decyzji podejmowanych przy wsparciu AI w obszarach krytycznych, takich jak kształcenie i szkolenie, zatrudnienie, ważne usługi, egzekwowanie prawa i sądownictwo. W przypadku gdyby nadal dochodziło do naruszeń praw podstawowych, skuteczne dochodzenie roszczeń przez osoby poszkodowane będzie możliwe dzięki zapewnieniu przejrzystości i identyfikowalności systemów sztucznej inteligencji w połączeniu z solidnymi kontrolami *ex post*.

W niniejszym wniosku nałożono pewne ograniczenia na wolność prowadzenia działalności gospodarczej (art. 16) oraz wolność sztuki i nauki (art. 13) w celu zapewnienia zgodności z nadrzędnym interesem publicznym, przejawiającym się w takich dziedzinach jak zdrowie, bezpieczeństwo, ochrona konsumentów i ochrona innych praw podstawowych („odpowiedzialne innowacje") w przypadku opracowywania i stosowania technologii sztucznej inteligencji wysokiego ryzyka. Ograniczenia te są proporcjonalne i zawężone do minimum niezbędnego, aby zapobiegać poważnym zagrożeniom dla bezpieczeństwa i prawdopodobnym naruszeniom praw podstawowych oraz łagodzić ich skutki.

Zwiększone obowiązki w zakresie przejrzystości nie będą miały również nieproporcjonalnego wpływu na prawo do ochrony własności intelektualnej (art. 17 ust. 2), ponieważ wymagane informacje będą ograniczone jedynie do niezbędnego minimum, tak aby osoby fizyczne mogły korzystać z prawa do skutecznego środka odwoławczego oraz aby zapewnić niezbędną przejrzystość wobec organów nadzoru i organów egzekwowania prawa, zgodnie z ich kompetencjami. Każde ujawnienie informacji będzie odbywało się zgodnie z odpowiednimi przepisami mającymi zastosowanie do danej dziedziny, w tym z dyrektywą (UE) 2016/943 w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem. W przypadku gdy organy publiczne i jednostki notyfikowane będą musiały uzyskać dostęp do informacji poufnych lub kodu źródłowego w celu zbadania zgodności z istotnymi zobowiązaniami, będą podlegać wiążącemu obowiązkowi zachowania poufności.

4. WPŁYW NA BUDŻET

Państwa członkowskie będą musiały wyznaczyć organy nadzorcze odpowiedzialne za wdrażanie wymogów legislacyjnych. Ich funkcja nadzorcza mogłaby być realizowana w oparciu o istniejące struktury, na przykład jednostki oceniające zgodność lub struktury nadzoru rynku, ale będzie wymagać odpowiedniej wiedzy specjalistycznej w zakresie technologii oraz odpowiednich zasobów ludzkich i finansowych. W zależności od istniejącej wcześniej struktury w każdym państwie członkowskim może to być od 1 do 25 ekwiwalentów pełnego czasu pracy na państwo członkowskie.

Szczegółowy przegląd odnośnych kosztów znajduje się w ocenie skutków finansowych regulacji dołączonej do niniejszego wniosku.

5. ELEMENTY FAKULTATYWNE

5.1. Plany wdrożenia i monitorowanie, ocena i sprawozdania

Zapewnienie solidnego mechanizmu monitorowania i oceny ma zasadnicze znaczenie dla zapewnienia skuteczności wniosku w osiąganiu jego celów szczegółowych. Komisja będzie odpowiedzialna za monitorowanie skutków wniosku. Ustanowi ona system rejestracji samodzielnych zastosowań sztucznej inteligencji wysokiego ryzyka w publicznej ogólnounijnej bazie danych. Rejestracja ta pozwoli również właściwym organom, użytkownikom i innym zainteresowanym osobom sprawdzić, czy dany system sztucznej inteligencji wysokiego ryzyka spełnia wymogi określone we wniosku, oraz umożliwi sprawowanie zwiększonego nadzoru nad systemami sztucznej inteligencji stwarzającymi wysokie ryzyko dla praw podstawowych. Tę bazę danych będą zasilać dostawcy AI, którzy będą zobowiązani do przekazywania istotnych informacji na temat swoich systemów oraz oceny zgodności przeprowadzonej w odniesieniu do tych systemów.

Ponadto dostawcy AI będą zobowiązani do informowania właściwych organów krajowych o poważnych incydentach lub przypadkach nieprawidłowego działania stanowiących

naruszenie obowiązków w zakresie praw podstawowych, gdy tylko się o nich dowiedzą, a także o wszelkich przypadkach wycofania systemów sztucznej inteligencji od użytkowników lub wycofania ich z rynku. Po każdym takim zdarzeniu właściwe organy krajowe przeprowadzą dochodzenie w sprawie incydentu lub nieprawidłowego działania, będą gromadzić wszystkie niezbędne informacje i będą je regularnie przekazywać Komisji wraz z odpowiednimi metadanymi. Uzupełnienie tych informacji na temat incydentów stanowić będzie kompleksowa analiza ogólnego rynku AI przeprowadzona przez Komisję.

Komisja opublikuje sprawozdanie, w którym oceni ramy w zakresie AI będące przedmiotem niniejszego wniosku i dokona ich przeglądu po upływie pięciu lat od daty rozpoczęcia ich stosowania.

5.2. Szczegółowe objaśnienia poszczególnych przepisów wniosku

5.2.1. ZAKRES I DEFINICJE (TYTUŁ I)

W **tytule I** określono przedmiot rozporządzenia i zakres stosowania nowych przepisów obejmujących wprowadzanie do obrotu, oddawanie do użytku i wykorzystywanie systemów sztucznej inteligencji. Przedstawiono w nim również definicje stosowane w całym akcie. Definicję systemu sztucznej inteligencji sformułowano w ramach prawnych w taki sposób, aby w możliwie największym stopniu była neutralna pod względem technologicznym i nie ulegała dezaktualizacji, biorąc pod uwagę szybki rozwój technologiczny i rozwój sytuacji rynkowej w dziedzinie AI. W celu zapewnienia niezbędnej pewności prawa uzupełnieniem tytułu I jest załącznik I zawierający szczegółowy wykaz podejść i technik na potrzeby rozwoju AI, które mają być dostosowywane przez Komisję w świetle postępu technologicznego. Wyraźnie określono również kluczowych uczestników w łańcuchu wartości sztucznej inteligencji, takich jak dostawcy i użytkownicy systemów sztucznej inteligencji, przy czym aby zapewnić równe warunki działania, zaliczono do nich zarówno podmioty publiczne, jak i prywatne.

5.2.2. ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI (TYTUŁ II)

W **tytule II** ustanowiono wykaz zakazanych praktyk w zakresie sztucznej inteligencji. W rozporządzeniu zastosowano podejście oparte na analizie ryzyka, wprowadzając rozróżnienie między zastosowaniami AI, które stwarzają (i) niedopuszczalne ryzyko, (ii) wysokie ryzyko oraz (iii) niskie lub minimalne ryzyko. Przedstawiony w tytule II wykaz zakazanych praktyk obejmuje wszystkie systemy sztucznej inteligencji, których wykorzystywanie uznaje się za niedopuszczalne ze względu na ich sprzeczność z wartościami Unii, na przykład ze względu na fakt, że naruszają one prawa podstawowe. Zakazy obejmują praktyki, które wykazują znaczny potencjał manipulowania ludźmi, oparte na technikach podprogowych działających na ich podświadomość lub wykorzystujące słabości określonych słabszych grup, takich jak dzieci lub osoby z niepełnosprawnościami, aby istotnie wypaczyć ich zachowania w sposób, który może spowodować u nich lub u innej osoby szkodę psychiczną lub fizyczną. Inne praktyki polegające na manipulacji lub wykorzystywaniu osób dorosłych, których stosowanie może być ułatwione przez systemy sztucznej inteligencji, mogłyby zostać objęte obowiązującymi przepisami dotyczącymi ochrony danych, ochrony konsumentów i usług cyfrowych zapewniającymi, aby osoby fizyczne były odpowiednio informowane i mogły swobodnie zdecydować o niepodleganiu profilowaniu lub innym praktykom mogącym wpływać na ich zachowanie. We wniosku zakazuje się również organom publicznym stosowania do celów ogólnych opartych na sztucznej inteligencji systemów punktowej oceny zachowań społecznych . Ponadto zakazuje się również wykorzystywania systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa, chyba że mają zastosowanie niektóre ograniczone wyjątki.

5.2.3. SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA (TYTUŁ III)

W **tytule III** zawarto przepisy szczegółowe dotyczące systemów sztucznej inteligencji, które stwarzają wysokie ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych osób fizycznych. Zgodnie z podejściem opartym na analizie ryzyka te systemy sztucznej inteligencji wysokiego ryzyka dopuszcza się do obrotu na rynku europejskim pod warunkiem spełnienia określonych wymogów obowiązkowych i przeprowadzenia oceny zgodności *ex ante*. Klasyfikacja systemu sztucznej inteligencji jako systemu wysokiego ryzyka opiera się na przeznaczeniu systemu AI, zgodnie z obowiązującymi przepisami dotyczącymi bezpieczeństwa produktów. Dlatego też klasyfikacja jako system sztucznej inteligencji wysokiego ryzyka zależy nie tylko od funkcji pełnionej przez system sztucznej inteligencji, ale także od konkretnego celu i trybu jego wykorzystania.

W tytule III rozdział 1 określono zasady klasyfikacji i wskazano dwie główne kategorie systemów sztucznej inteligencji wysokiego ryzyka:

- systemy sztucznej inteligencji przeznaczone do wykorzystywania jako związane z bezpieczeństwem elementy produktów podlegających ocenie zgodności *ex ante* przeprowadzanej przez osoby trzecie;
- inne samodzielne systemy sztucznej inteligencji mające wpływ głównie na prawa podstawowe, które wyraźnie wymieniono w załączniku III.

Zawarty w załączniku III wykaz systemów sztucznej inteligencji wysokiego ryzyka zawiera ograniczoną liczbę systemów sztucznej inteligencji, w przypadku których ryzyko już się urzeczywistniło lub może się urzeczywistnić w najbliższej przyszłości. Aby zapewnić możliwość dostosowania rozporządzenia do pojawiających się sposobów wykorzystania i zastosowań AI, Komisja może rozszerzyć wykaz systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych w pewnych z góry określonych obszarach, stosując zestaw kryteriów i metodykę oceny ryzyka.

W rozdziale 2 przedstawiono prawne wymogi, jakie systemy sztucznej inteligencji wysokiego ryzyka muszą spełniać, a dotyczące danych i zarządzania danymi, dokumentacji i rejestrowania zdarzeń, przejrzystości i dostarczania informacji użytkownikom, nadzoru ze strony człowieka, solidności, dokładności i bezpieczeństwa. Proponowane minimalne wymogi są już codziennością dla wielu działających z należytą starannością podmiotów gospodarczych i są wynikiem dwóch lat prac przygotowawczych opartych na wytycznych w zakresie etyki opracowanych przez grupę ekspertów wysokiego szczebla ds. AI[29], pilotażowo realizowanych przez ponad 350 organizacji[30]. Są one również w dużej mierze spójne z innymi międzynarodowymi zaleceniami i zasadami, co gwarantuje, że proponowane ramy w zakresie AI są zgodne z ramami przyjętymi przez międzynarodowych partnerów handlowych UE. Konkretne rozwiązania techniczne mające na celu osiągnięcie zgodności z tymi wymogami mogą zostać określone w formie norm lub innych specyfikacji technicznych lub opracowane w inny sposób zgodnie z ogólną wiedzą techniczną lub naukową, według uznania dostawcy systemu sztucznej inteligencji. Ta elastyczność jest szczególnie ważna, ponieważ umożliwia dostawcom systemów sztucznej inteligencji wybór sposobu spełnienia obowiązujących ich wymagań, przy uwzględnieniu stanu techniki oraz postępu technologicznego i naukowego w tej dziedzinie.

---

[29] Grupa ekspertów wysokiego szczebla ds. AI, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, 2019 r.

[30] Zostały one również zatwierdzone przez Komisję w komunikacie z 2019 r. w sprawie ukierunkowanego na człowieka podejścia do AI.

W rozdziale 3 nałożono na dostawców systemów sztucznej inteligencji wysokiego ryzyka jasno określony zestaw obowiązków horyzontalnych. Proporcjonalne obowiązki nałożono również na użytkowników i innych uczestników łańcucha wartości AI (np. importerów, dystrybutorów, autoryzowanych przedstawicieli).

W rozdziale 4 określono ramy dla jednostek notyfikowanych, które mają być zaangażowane w procedury oceny zgodności jako niezależne osoby trzecie, natomiast w rozdziale 5 szczegółowo wyjaśniono procedury oceny zgodności, które należy stosować w przypadku każdego rodzaju systemu sztucznej inteligencji wysokiego ryzyka. Podejście oparte na ocenie zgodności ma na celu zminimalizowanie obciążenia podmiotów gospodarczych oraz jednostek notyfikowanych, których zdolności muszą być z czasem stopniowo zwiększane. Systemy sztucznej inteligencji, które mają być wykorzystywane jako związane z bezpieczeństwem elementy produktów podlegających przepisom nowych ram prawnych (np. maszyn, zabawek, wyrobów medycznych itp.), będą podlegać tym samym mechanizmom zapewnienia zgodności i egzekwowania przepisów w trybie *ex ante* i *ex post*, co produkty, których są elementem. Kluczowa różnica polega na tym, że mechanizmy *ex ante* i *ex post* zapewnią zgodność nie tylko z wymogami określonymi w przepisach sektorowych, ale także z wymogami określonymi w niniejszym rozporządzeniu.

W odniesieniu do samodzielnych systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III, ustanowiony zostanie nowy system zapewnienia zgodności i egzekwowania przepisów. Jest to zgodne z modelem przewidzianym w nowych ramach prawnych, który – z wyjątkiem systemów zdalnej identyfikacji biometrycznej, które podlegałyby ocenie zgodności przeprowadzanej przez osobę trzecią – zakłada weryfikacje przeprowadzane przez dostawców w ramach ich systemów kontroli wewnętrznej. Kompleksowa ocena zgodności *ex ante* przeprowadzana w ramach kontroli wewnętrznych, połączona z rygorystycznym egzekwowaniem *ex post*, mogłaby być skutecznym i uzasadnionym rozwiązaniem w przypadku tych systemów, biorąc pod uwagę wczesny etap interwencji regulacyjnej oraz fakt, że sektor AI charakteryzuje się dużą innowacyjnością, a wiedza ekspercka potrzebna do jego kontrolowania jest dopiero gromadzona. Ocena w ramach kontroli wewnętrznych w przypadku „samodzielnych" systemów sztucznej inteligencji wysokiego ryzyka wymagałaby stosowania kompleksowego, skutecznego i odpowiednio udokumentowanego procesu zapewnienia zgodności *ex ante* ze wszystkimi wymogami rozporządzenia oraz zgodności z solidnymi systemami zarządzania jakością i ryzykiem oraz monitorowania po wprowadzeniu do obrotu. Po przeprowadzeniu przez dostawcę odpowiedniej oceny zgodności powinien on zarejestrować te samodzielne systemy sztucznej inteligencji wysokiego ryzyka w unijnej bazie danych, która będzie zarządzana przez Komisję w celu zwiększenia publicznej przejrzystości i kontroli oraz wzmocnienia nadzoru *ex post* sprawowanego przez właściwe organy. Natomiast w celu zachowania spójności z obowiązującymi przepisami dotyczącymi bezpieczeństwa produktów oceny zgodności systemów sztucznej inteligencji, które stanowią związane z bezpieczeństwem elementy produktów, będą przeprowadzane w ramach systemu obejmującego procedury oceny zgodności przeprowadzanej przez osobę trzecią, które już ustanowiono na podstawie odpowiednich przepisów sektorowych dotyczących bezpieczeństwa produktów. Nowe ponowne oceny zgodności *ex ante* będą potrzebne w przypadku istotnych zmian wprowadzanych w systemach sztucznej inteligencji (a zwłaszcza zmian, które wykraczają poza to, co zostało wstępnie ustalone przez dostawcę w jego dokumentacji technicznej i zweryfikowane w momencie przeprowadzania oceny zgodności *ex ante*).

5.2.4. OBOWIĄZKI W ZAKRESIE PRZEJRZYSTOŚCI W ODNIESIENIU DO OKREŚLONYCH SYSTEMÓW SZTUCZNEJ INTELIGENCJI (TYTUŁ IV)

Tytuł IV dotyczy określonych systemów sztucznej inteligencji i ma na celu uwzględnienie szczególnego ryzyka manipulacji, jakie one stwarzają. Obowiązki w zakresie przejrzystości będą miały zastosowanie do systemów, które (i) wchodzą w interakcję z człowiekiem, (ii) są wykorzystywane do wykrywania emocji lub określania powiązań z kategoriami (społecznymi) na podstawie danych biometrycznych lub (iii) generują treści lub manipulują nimi (technologia deepfake). Gdy osoby fizyczne wchodzą w interakcję się z systemem sztucznej inteligencji lub gdy ich emocje lub cechy charakterystyczne są rozpoznawane za pomocą środków zautomatyzowanych, konieczne jest poinformowanie ich o tym fakcie. Jeżeli system sztucznej inteligencji jest wykorzystywany do generowania obrazów, dźwięków lub treści wideo, które w znacznym stopniu przypominają autentyczne treści, lub do manipulowania takimi obrazami, dźwiękami lub treściami wideo, powinien istnieć obowiązek ujawniania, że dane treści wygenerowano za pomocą środków zautomatyzowanych, z zastrzeżeniem sytuacji wyjątkowych dotyczących zgodnych z prawem celów (egzekwowanie prawa, wolność wypowiedzi). Pozwala to tym osobom na dokonywanie świadomych wyborów lub na wycofanie się z danej sytuacji.

5.2.5. ŚRODKI WSPIERAJĄCE INNOWACYJNOŚĆ (TYTUŁ V)

Tytuł V przyczynia się do realizacji celu polegającego na utworzeniu ram prawnych, które sprzyjają innowacyjności, nie ulegają dezaktualizacji i są odporne na zakłócenia. W tym celu zachęca się w nim właściwe organy krajowe do tworzenia piaskownic regulacyjnych i ustanawia się podstawowe ramy w zakresie zarządzania, nadzoru i odpowiedzialności. Piaskownice regulacyjne w zakresie AI tworzą kontrolowane środowisko do testowania innowacyjnych technologii przez ograniczony czas na podstawie planu testów uzgodnionego z właściwymi organami. Tytuł V zawiera również środki mające na celu zmniejszenie obciążeń regulacyjnych dla MŚP i przedsiębiorstw typu start-up.

5.2.6. ZARZĄDZANIE I WDRAŻANIE (TYTUŁY VI, VII I VII)

W **tytule VI** ustanawia się systemy zarządzania na szczeblu unijnym i krajowym. Na szczeblu unijnym we wniosku powołano Europejską Radę ds. Sztucznej Inteligencji (zwaną dalej „Radą”), w skład której wchodzą przedstawiciele państw członkowskich i Komisji. Rada będzie ułatwiać sprawne, skuteczne i zharmonizowane wdrażanie niniejszego rozporządzenia, przyczyniając się do skutecznej współpracy krajowych organów nadzorczych i Komisji oraz służąc Komisji radą i wiedzą fachową. Będzie ona również gromadzić najlepsze praktyki i udostępniać je państwom członkowskim.

Na szczeblu krajowym państwa członkowskie będą musiały wyznaczyć co najmniej jeden właściwy organ krajowy, a spośród tych organów – krajowy organ nadzorczy, do celów sprawowania nadzoru nad stosowaniem i wdrażaniem rozporządzenia. Europejski Inspektor Ochrony Danych będzie występował w charakterze właściwego organu w zakresie nadzoru nad instytucjami, agencjami i jednostkami organizacyjnymi Unii, w przypadku gdy te wchodzą w zakres niniejszego rozporządzenia.

Tytuł VII ma na celu ułatwienie prac Komisji i organów krajowych w zakresie monitorowania poprzez utworzenie ogólnounijnej bazy danych gromadzącej informacje o samodzielnych systemach sztucznej inteligencji wysokiego ryzyka mających wpływ głównie na prawa podstawowe. Obsługą bazy danych zajmie się Komisja, a umieszczane w niej dane będą pochodzić od dostawców systemów sztucznej inteligencji, którzy będą zobowiązani do zarejestrowania swoich systemów przed wprowadzeniem ich na rynek lub oddaniem do użytku w inny sposób.

W **tytule VIII** określono obowiązki dostawców systemów sztucznej inteligencji w zakresie monitorowania i zgłaszania zdarzeń, a dokładniej obowiązki w zakresie monitorowania systemu po jego wprowadzeniu do obrotu oraz zgłaszania incydentów i przypadków nieprawidłowego działania związanych ze sztuczną inteligencją i prowadzenia dochodzeń w tych sprawach. Organy nadzoru rynku będą również kontrolować rynek i sprawdzać zgodność z obowiązkami i wymogami dotyczącymi wszystkich systemów sztucznej inteligencji wysokiego ryzyka już wprowadzonych do obrotu. Organy nadzoru rynku będą posiadały wszystkie uprawnienia wynikające z rozporządzenia (UE) 2019/1020 w sprawie nadzoru rynku. Egzekwowanie prawa *ex post* powinno zapewnić, aby po wprowadzeniu systemu sztucznej inteligencji do obrotu organy publiczne dysponowały uprawnieniami i zasobami umożliwiającymi interwencję w przypadku, gdy systemy sztucznej inteligencji generują nieoczekiwane ryzyko, które wymaga szybkiego działania. Będą one również monitorować spełnianie przez podmioty gospodarcze ich odpowiednich obowiązków wynikających z rozporządzenia. We wniosku nie przewidziano automatycznego tworzenia żadnych dodatkowych organów lub władz na poziomie państw członkowskich. Państwa członkowskie mogą zatem wyznaczyć istniejące organy sektorowe (i korzystać z ich wiedzy specjalistycznej), którym mogą powierzyć również uprawnienia w zakresie monitorowania i egzekwowania przepisów rozporządzenia.

Wszystko to pozostaje bez uszczerbku dla istniejącego systemu i podziału uprawnień w zakresie egzekwowania *ex post* obowiązków dotyczących praw podstawowych w państwach członkowskich. Jeżeli jest to niezbędne do wykonywania ich mandatu, istniejące organy nadzoru i egzekwowania prawa będą również uprawnione do żądania dostępu do wszelkiej dokumentacji prowadzonej na podstawie niniejszego rozporządzenia oraz, w razie potrzeby, do kierowania do organów nadzoru rynku wniosków o zorganizowanie testów systemu sztucznej inteligencji wysokiego ryzyka za pomocą środków technicznych.

5.2.7. KODEKSY POSTĘPOWANIA (TYTUŁ IX)

W **tytule IX** ustanowiono ramy dotyczące tworzenia kodeksów postępowania, które mają na celu zachęcenie dostawców systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem do dobrowolnego stosowania się do obowiązkowych wymogów mających zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka (określonych w tytule III). Dostawcy systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem mogą samodzielnie tworzyć i wdrażać kodeksy postępowania. Kodeksy te mogą również obejmować dobrowolne zobowiązania dotyczące na przykład zrównoważenia środowiskowego, dostępności systemu dla osób z niepełnosprawnościami, udziału zainteresowanych stron w projektowaniu i rozwijaniu systemów sztucznej inteligencji oraz zróżnicowanego pod wieloma względami składu zespołów programistycznych.

5.2.8. PRZEPISY KOŃCOWE (TYTUŁY X, XI I XII)

W **tytule X** podkreślono zobowiązanie wszystkich stron do przestrzegania poufności informacji i danych oraz określono zasady wymiany informacji uzyskanych podczas wdrażania rozporządzenia. W tytule X uwzględniono również środki zapewniające skuteczne wdrożenie rozporządzenia poprzez skuteczne, proporcjonalne i odstraszające kary za naruszenie przepisów.

W **tytule XI** określono zasady wykonywania przekazanych uprawnień i uprawnień wykonawczych. We wniosku upoważnia się Komisję do przyjęcia, w stosownych przypadkach, aktów wykonawczych w celu zapewnienia jednolitego stosowania rozporządzenia lub aktów delegowanych w celu aktualizacji lub uzupełnienia wykazów zawartych w załącznikach I–VII.

W **tytule XII** zobowiązano Komisję do przeprowadzania regularnej oceny potrzeby aktualizacji załącznika III oraz do przygotowywania regularnych sprawozdań z oceny i przeglądu rozporządzenia. Określono w nim również przepisy końcowe, w tym zróżnicowany okres przejściowy w odniesieniu do początkowej daty rozpoczęcia stosowania rozporządzenia, aby ułatwić wszystkim zainteresowanym stronom jego sprawne wdrożenie.

2021/0106 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

USTANAWIAJĄCE ZHARMONIZOWANE PRZEPISY DOTYCZĄCE SZTUCZNEJ INTELIGENCJI (AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI) I ZMIENIAJĄCE NIEKTÓRE AKTY USTAWODAWCZE UNII

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 i 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[31],

uwzględniając opinię Komitetu Regionów[32],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania sztucznej inteligencji zgodnie z wartościami Unii. Niniejsze rozporządzenie służy realizacji szeregu nadrzędnych celów interesu publicznego, takich jak wysoki poziom ochrony zdrowia, bezpieczeństwa i praw podstawowych, oraz zapewnia swobodny przepływ transgraniczny towarów i usług opartych na sztucznej inteligencji, uniemożliwiając tym samym państwom członkowskim nakładanie ograniczeń w zakresie opracowywania, wprowadzania do obrotu i wykorzystywania systemów sztucznej inteligencji, chyba że wyraźnie zezwolono na to w niniejszym rozporządzeniu.

(2) Systemy sztucznej inteligencji mogą być łatwo wdrażane w wielu sektorach gospodarki i obszarach życia społecznego, w tym w wymiarze transgranicznym, i mogą być przedmiotem obrotu w całej Unii. Niektóre państwa członkowskie rozważały już przyjęcie przepisów krajowych w celu zapewnienia, aby sztuczna inteligencja była bezpieczna oraz rozwijana i wykorzystywana w sposób zgodny z obowiązkami wynikającymi z praw podstawowych. Zróżnicowane przepisy krajowe mogą prowadzić do rozdrobnienia rynku wewnętrznego i zmniejszenia pewności prawa dla operatorów, którzy opracowują lub wykorzystują systemy sztucznej inteligencji. Należy zatem zapewnić spójny i wysoki poziom ochrony w całej Unii, zapobiegając jednocześnie rozbieżnościom utrudniającym swobodny obrót systemami sztucznej inteligencji oraz powiązanymi produktami i usługami na rynku wewnętrznym poprzez ustanowienie jednolitych obowiązków dla operatorów

[31] Dz.U. C […] z […], s. […].
[32] Dz.U. C […] z […], s. […].

i zagwarantowanie jednolitej ochrony nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym, w oparciu o art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). W zakresie, w jakim niniejsze rozporządzenie zawiera określone przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w odniesieniu do ograniczenia wykorzystywania systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa, podstawą niniejszego rozporządzenia w zakresie takich przepisów szczegółowych powinien być art. 16 TFUE. W świetle tych przepisów szczegółowych i odwołania się do art. 16 TFUE należy skonsultować się z Europejską Radą Ochrony Danych.

(3) Sztuczna inteligencja to szybko rozwijająca się grupa technologii, które mogą przyczyniać się do wielu różnych korzyści społeczno-ekonomicznych we wszystkich gałęziach przemysłu i obszarach działalności społecznej. Rozwiązania bazujące na sztucznej inteligencji umożliwiają lepsze prognozowanie, optymalizację operacji i przydzielania zasobów oraz personalizację rozwiązań cyfrowych dostępnych dla osób fizycznych i organizacji, mają potencjał, aby zapewnić przedsiębiorstwom kluczową przewagę konkurencyjną i wspierać wyniki korzystne z punktu widzenia kwestii społecznych i ochrony środowiska, na przykład w zakresie opieki zdrowotnej, rolnictwa, kształcenia i szkolenia, zarządzania infrastrukturą, energetyki, transportu i logistyki, usług publicznych, bezpieczeństwa, wymiaru sprawiedliwości, zasobooszczędności i efektywności energetycznej oraz łagodzenia zmiany klimatu i przystosowywania się do niej.

(4) Jednocześnie sztuczna inteligencja może być źródłem ryzyka i szkody dla interesu publicznego i przywilejów chronionych prawem Unii, w zależności od okoliczności dotyczących jej konkretnego zastosowania i wykorzystania. Szkody te mogą być materialne lub niematerialne.

(5) Unijne ramy prawne określające zharmonizowane przepisy dotyczące sztucznej inteligencji są zatem niezbędne do wspierania rozwoju, wykorzystywania i upowszechniania sztucznej inteligencji na rynku wewnętrznym, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony interesów publicznych, takich jak zdrowie i bezpieczeństwo oraz ochrona praw podstawowych, uznanych i chronionych przez prawo Unii. Aby osiągnąć ten cel, należy ustanowić przepisy regulujące wprowadzanie do obrotu i oddawanie do użytku niektórych systemów sztucznej inteligencji, zapewniając w ten sposób sprawne funkcjonowanie rynku wewnętrznego i umożliwiając swobodny obrót tymi systemami zgodnie z zasadą swobodnego przepływu towarów i usług. Ustanawiając te zasady, niniejsze rozporządzenie wspiera realizację celu, jakim jest osiągnięcie przez Unię pozycji światowego lidera, jeśli chodzi o rozwój bezpiecznej, wiarygodnej i etycznej sztucznej inteligencji, zgodnie z konkluzjami Rady Europejskiej[33], oraz zapewnia ochronę zasad etycznych, zgodnie z wyraźnym żądaniem Parlamentu Europejskiego[34].

(6) Pojęcie systemu sztucznej inteligencji powinno być jasno zdefiniowane w celu zapewnienia pewności prawa, przy jednoczesnym zapewnieniu elastyczności umożliwiającej dostosowanie się do przyszłego rozwoju technologicznego. Podstawę

---

33 Rada Europejska, Nadzwyczajne posiedzenie Rady Europejskiej (1 i 2 października 2020 r.) – Konkluzje., EUCO 13/20, 2020, s. 6.

34 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).

tej definicji powinny stanowić kluczowe cechy funkcjonalne oprogramowania, w szczególności zdolność, przy danym zestawie celów określonych przez człowieka, do generowania wyników takich jak treści, prognozy, zalecenia lub decyzje wpływające na środowisko, z którym system wchodzi w interakcję, czy to w wymiarze fizycznym, czy cyfrowym. Systemy sztucznej inteligencji mogą być zaprojektowane tak, aby działały na różnym poziomie autonomii i mogły być wykorzystywane jako samodzielne rozwiązania lub jako element produktu, niezależnie od tego, czy system jest fizycznie zintegrowany z produktem (wbudowany), czy też służy realizacji funkcji produktu, choć nie jest z nim zintegrowany (niewbudowany). Definicję systemu sztucznej inteligencji powinien uzupełniać wykaz konkretnych technik i podejść stosowanych przy jego opracowywaniu, który to wykaz powinien być aktualizowany w świetle rozwoju sytuacji rynkowej i postępu technologicznego w drodze aktów delegowanych przyjmowanych przez Komisję w celu zmiany tego wykazu.

(7) Pojęcie danych biometrycznych stosowane w niniejszym rozporządzeniu jest zgodne z pojęciem danych biometrycznych zdefiniowanym w art. 4 pkt 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[35], art. 3 pkt 18 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[36] oraz art. 3 pkt 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 i powinno być interpretowane w sposób spójny z tym pojęciem[37].

(8) Pojęcie systemu zdalnej identyfikacji biometrycznej stosowane w niniejszym rozporządzeniu należy zdefiniować funkcjonalnie jako system sztucznej inteligencji służący do identyfikacji osób fizycznych na odległość poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, bez wcześniejszej wiedzy o tym, czy dana osoba będzie w niej figurować i może zatem zostać zidentyfikowana, niezależnie od konkretnej technologii oraz konkretnych procesów lub rodzajów wykorzystywanych danych biometrycznych. Należy dokonać rozróżnienia między systemami zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” a systemami zdalnej identyfikacji biometrycznej „post factum”, biorąc pod uwagę ich różne cechy i sposoby stosowania, a także różne związane z nimi zagrożenia. W przypadku systemów działających „w czasie rzeczywistym” pobranie danych biometrycznych, porównanie i identyfikacja następują natychmiast, niemal natychmiast lub w każdym razie bez znacznego opóźnienia. W związku z tym nie powinno być możliwości obchodzenia przepisów niniejszego rozporządzenia dotyczących stosowania przedmiotowych systemów sztucznej inteligencji „w czasie rzeczywistym” poprzez wprowadzenie niewielkich opóźnień. Systemy identyfikacji „w czasie rzeczywistym” obejmują wykorzystanie materiału

---

35 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

36 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

37 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (dyrektywa w sprawie egzekwowania prawa) (Dz.U. L 119 z 4.5.2016, s. 89).

rejestrowanego „na żywo” lub „w czasie zbliżonym do rzeczywistego”, takiego jak materiał wideo generowany przez kamerę lub inne urządzenie o podobnej funkcjonalności. Natomiast w przypadku systemów identyfikacji „post factum” dane biometryczne zostały już pobrane, a porównanie i identyfikacja następują ze znacznym opóźnieniem. Dotyczy to materiałów, takich jak zdjęcia lub nagrania wideo generowane przez kamery telewizji przemysłowej lub urządzenia prywatne, których rejestracji dokonano, zanim użyto systemu w stosunku do danej osoby fizycznej.

(9) Do celów niniejszego rozporządzenia pojęcie przestrzeni publicznej należy rozumieć jako odnoszące się do każdego miejsca fizycznego, które jest dostępne dla ogółu osób, niezależnie od tego, czy dane miejsce jest własnością prywatną czy publiczną. Pojęcie to nie obejmuje zatem miejsc, które mają charakter prywatny i zazwyczaj nie są ogólnodostępne dla osób trzecich, w tym organów ścigania, chyba że osoby te wyraźnie zaproszono lub upoważniono do wejścia na dany teren; do takich miejsc zalicza się domy, prywatne kluby, biura, magazyny i fabryki. Przestrzenie internetowe również nie są objęte niniejszym rozporządzeniem, ponieważ nie są to przestrzenie fizyczne. Sam fakt, że mogą obowiązywać jednak pewne warunki dostępu do danej przestrzeni, takie jak bilety wstępu lub ograniczenia wiekowe, nie oznacza, że przestrzeń ta nie jest dostępna publicznie w rozumieniu niniejszego rozporządzenia. W związku z tym oprócz przestrzeni publicznych, takich jak ulice, odpowiednie części budynków rządowych i większość infrastruktury transportowej, publicznie dostępne są zazwyczaj również przestrzenie takie jak kina, teatry, sklepy i centra handlowe. To, czy dana przestrzeń jest dostępna publicznie, powinno być jednak ustalane indywidualnie w każdym przypadku, z uwzględnieniem specyfiki danej sytuacji.

(10) W celu zapewnienia równych szans oraz skutecznej ochrony praw i wolności osób fizycznych w całej Unii przepisy ustanowione niniejszym rozporządzeniem powinny mieć zastosowanie do dostawców systemów sztucznej inteligencji w sposób niedyskryminacyjny, niezależnie od tego, czy mają oni siedzibę w Unii, czy w państwie trzecim, oraz do użytkowników systemów sztucznej inteligencji mających siedzibę w Unii.

(11) Ze względu na swój cyfrowy charakter niektóre systemy sztucznej inteligencji powinny zostać objęte zakresem niniejszego rozporządzenia, nawet jeśli nie są wprowadzane do obrotu, oddawane do użytku ani wykorzystywane w Unii. Dotyczy to na przykład operatora mającego siedzibę w Unii, który zleca określone usługi operatorowi mającemu siedzibę poza Unią w związku z operacjami, które mają być wykonywane przez system sztucznej inteligencji, który zostałby zakwalifikowany jako system wysokiego ryzyka, a których skutki byłyby odczuwalne przez osoby fizyczne zlokalizowane w Unii. W takich okolicznościach system sztucznej inteligencji wykorzystywany przez operatora spoza Unii mógłby przetwarzać dane, które legalnie zgromadzono w Unii i przekazano poza Unię, oraz przekazywać zlecającemu operatorowi z Unii wynik przetwarzania tych danych, natomiast sam system sztucznej inteligencji nie byłby przedmiotem wprowadzenia do obrotu lub oddania do użytku w Unii ani nie byłby w Unii wykorzystywany. Aby zapobiec obchodzeniu przepisów niniejszego rozporządzenia oraz zapewnić skuteczną ochronę osób fizycznych znajdujących się w Unii, niniejsze rozporządzenie powinno mieć również zastosowanie do dostawców i użytkowników systemów sztucznej inteligencji, którzy mają siedzibę w państwie trzecim, w zakresie, w jakim wyniki działania tych systemów są wykorzystywane w Unii. Aby uwzględnić jednak istniejące ustalenia i szczególne potrzeby w zakresie współpracy z partnerami zagranicznymi, z którymi wymienia się informacje i dowody, niniejsze rozporządzenie nie powinno mieć

zastosowania do organów publicznych państwa trzeciego i organizacji międzynarodowych działających w ramach zawartych na szczeblu krajowym lub europejskim umów międzynarodowych o współpracy organów ścigania i wymiarów sprawiedliwości z Unią lub jej państwami członkowskimi. Takie umowy zostały zawarte dwustronnie między państwami członkowskimi a państwami trzecimi lub między Unią Europejską, Europolem i innymi agencjami UE a państwami trzecimi i organizacjami międzynarodowymi.

(12) Niniejsze rozporządzenie powinno mieć również zastosowanie do instytucji, urzędów, organów i agencji Unii, gdy działają one jako dostawca lub użytkownik systemu sztucznej inteligencji. Systemy sztucznej inteligencji opracowywane lub wykorzystywane wyłącznie do celów wojskowych powinny zostać wyłączone z zakresu stosowania niniejszego rozporządzenia, jeżeli takie wykorzystanie wchodzi w zakres wyłącznych kompetencji wspólnej polityki zagranicznej i bezpieczeństwa regulowanej na mocy tytułu V Traktatu o Unii Europejskiej (TUE). Niniejsze rozporządzenie nie powinno naruszać przepisów dotyczących odpowiedzialności usługodawców będących pośrednikami, określonych w dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady [zmienionej aktem prawnym o usługach cyfrowych].

(13) W celu zapewnienia spójnego i wysokiego poziomu ochrony interesów publicznych w dziedzinie zdrowia, bezpieczeństwa i praw podstawowych należy ustanowić wspólne standardy normatywne dla wszystkich systemów sztucznej inteligencji wysokiego ryzyka. Standardy te powinny być zgodne z Kartą praw podstawowych Unii Europejskiej („Karta") oraz powinny być niedyskryminacyjne i zgodne z międzynarodowymi zobowiązaniami handlowymi Unii.

(14) Aby wprowadzić proporcjonalny i skuteczny zestaw wiążących zasad dotyczących systemów sztucznej inteligencji, należy zastosować jasno określone podejście oparte na analizie ryzyka. Takie podejście powinno polegać na dostosowywaniu rodzaju i treści takich zasad do intensywności i zakresu zagrożeń, jakie mogą powodować systemy sztucznej inteligencji. Konieczne jest zatem wprowadzenie zakazu stosowania niektórych praktyk z zakresu sztucznej inteligencji, określenie wymogów w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka i obowiązków spoczywających na odpowiednich operatorach oraz określenie obowiązków w zakresie przejrzystości w odniesieniu do niektórych systemów sztucznej inteligencji.

(15) Oprócz wielu korzystnych zastosowań sztucznej inteligencji technologia ta może być również niewłaściwie wykorzystywana i może dostarczać nowych i potężnych narzędzi do praktyk manipulacji, wykorzystywania i kontroli społecznej. Takie praktyki są szczególnie szkodliwe i powinny być zakazane, ponieważ są sprzeczne z unijnymi wartościami poszanowania godności ludzkiej, wolności, równości, demokracji i praworządności oraz z prawami podstawowymi Unii, w tym z prawem do niedyskryminacji, ochrony danych i prywatności oraz z prawami dziecka.

(16) Należy zakazać wprowadzania do obrotu, oddawania do użytku lub wykorzystywania niektórych systemów sztucznej inteligencji mających na celu zniekształcenie ludzkiego zachowania, co w rezultacie może prowadzić do wystąpienia szkód fizycznych lub psychicznych. Takie systemy sztucznej inteligencji wykorzystują mechanizmy podprogowe, których osoby fizyczne nie są w stanie dostrzec, lub wykorzystują słabości dzieci i innych osób ze względu na ich wiek, niepełnosprawność fizyczną lub umysłową. Czynią to z zamiarem istotnego zniekształcenia zachowania danej osoby i w sposób, który powoduje lub może

powodować szkodę dla tej lub innej osoby. Istnienia takiego zamiaru nie można zakładać wówczas, gdy zniekształcenie ludzkiego zachowania wynika z czynników zewnętrznych w stosunku do systemu sztucznej inteligencji, które pozostają poza kontrolą dostawcy lub użytkownika. Zakaz ten nie powinien hamować badań prowadzonych w uzasadnionych celach w odniesieniu do takich systemów sztucznej inteligencji, jeżeli badania te nie prowadzą do takiego wykorzystania systemu sztucznej inteligencji w relacjach człowiek-maszyna, które naraża osoby fizyczne na szkodę, a przy tym są prowadzone zgodnie z uznanymi normami etycznymi dotyczącymi badań naukowych.

(17) Systemy sztucznej inteligencji, które umożliwiają prowadzenie przez organy publiczne lub w ich imieniu oceny punktowej zachowań społecznych osób fizycznych do celów ogólnych, mogą prowadzić do dyskryminacyjnych wyników i wykluczenia pewnych grup. Mogą one naruszać prawo do godności i niedyskryminacji oraz wartości, jakimi są równość i sprawiedliwość. Takie systemy sztucznej inteligencji oceniają lub klasyfikują wiarygodność osób fizycznych na podstawie ich zachowań społecznych w wielu kontekstach lub na podstawie znanych lub przewidywanych cech osobistych lub cech osobowości. Ocena społeczna wystawiona przez takie systemy sztucznej inteligencji może prowadzić do krzywdzącego lub niekorzystnego traktowania osób fizycznych lub całych ich grup w kontekstach społecznych, które nie są związane z kontekstem, w którym pierwotnie wygenerowano lub zgromadzono dane, lub do krzywdzącego traktowania, które jest nieproporcjonalne lub nieuzasadnione w stosunku do wagi ich zachowań społecznych. Takie systemy sztucznej inteligencji należy zatem zakazać.

(18) Wykorzystanie systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa uważa się za szczególnie ingerujące w prawa i wolności zainteresowanych osób w zakresie, ponieważ może wpływać na życie prywatne dużej części społeczeństwa, wywoływać poczucie stałego nadzoru i pośrednio zniechęcać do korzystania z wolności zgromadzeń i innych praw podstawowych. Ponadto bezpośredniość oddziaływania i ograniczone możliwości późniejszej kontroli lub korekty wykorzystania takich systemów działających „w czasie rzeczywistym" niosą ze sobą zwiększone ryzyko dla praw i wolności osób, których dotyczą działania organów ścigania.

(19) Wykorzystanie tych systemów do celów egzekwowania prawa powinno zatem być zabronione, z wyjątkiem zamkniętej listy trzech wąsko zdefiniowanych sytuacji, w których wykorzystanie jest absolutnie konieczne do realizacji istotnego interesu publicznego, którego waga przeważa nad ryzykiem. Sytuacje te obejmują poszukiwanie potencjalnych ofiar przestępstw, w tym zaginionych dzieci; zapobieganie niektórym zagrożeniom życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu; oraz wykrywanie, lokalizowanie, identyfikowanie lub ściganie sprawców przestępstw lub podejrzanych o popełnienie przestępstw, o których mowa w decyzji ramowej Rady 2002/584/WSiSW[38], jeżeli przestępstwa te podlegają w danym państwie członkowskim karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, i zostały

[38] Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).

zdefiniowane w prawie danego państwa członkowskiego. Taki próg kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności zgodnie z prawem krajowym pozwala zapewnić, aby przestępstwo było na tyle poważne, by potencjalnie uzasadniać wykorzystanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym". Ponadto spośród 32 przestępstw wymienionych w decyzji ramowej Rady 2002/584/WSiSW niektóre mogą w praktyce mieć większe znaczenie niż inne, ponieważ można przewidzieć, że korzystanie ze zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" będzie w bardzo różnym stopniu konieczne i proporcjonalne do praktycznych celów wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy poszczególnych wymienionych przestępstw lub podejrzanego o popełnienie tych przestępstw, przy uwzględnieniu prawdopodobnych różnic w odniesieniu do powagi, prawdopodobieństwa i skali szkody lub ewentualnych negatywnych konsekwencji.

(20) W celu zapewnienia, aby systemy te były wykorzystywane w sposób odpowiedzialny i proporcjonalny, należy również zastrzec, że w każdej z tych trzech wąsko zdefiniowanych sytuacji z zamkniętej listy należy uwzględniać pewne elementy, w szczególności charakter sytuacji, która skutkowała złożeniem wniosku, wpływ korzystania z takich systemów na prawa i wolności wszystkich zainteresowanych osób, a także zabezpieczenia i warunki przewidziane w związku z korzystaniem z takich systemów. Ponadto wykorzystanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa powinno podlegać odpowiednim ograniczeniom w czasie i przestrzeni, z uwzględnieniem w szczególności dowodów lub wskazówek dotyczących zagrożeń, ofiar lub sprawcy. Referencyjna baza danych osób powinna być odpowiednia dla każdego przypadku użycia w każdej z trzech wyżej wymienionych sytuacji.

(21) Każde użycie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa powinno podlegać wyraźnemu i szczegółowemu zezwoleniu wydanemu przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego. Takie zezwolenie należy zasadniczo uzyskać przed rozpoczęciem korzystania z systemu, z wyjątkiem należycie uzasadnionych sytuacji nagłych, to znaczy sytuacji, w których potrzeba skorzystania z danego systemu jest na tyle duża, że uzyskanie zezwolenia przed rozpoczęciem korzystania jest faktycznie i obiektywnie niemożliwe. W takich sytuacjach nagłych wykorzystanie powinno być ograniczone do absolutnie niezbędnego minimum i powinno podlegać odpowiednim zabezpieczeniom i warunkom określonym w prawie krajowym i sprecyzowanym w kontekście każdego przypadku pilnego użycia przez sam organ ścigania. Ponadto organ ścigania powinien w takich sytuacjach dążyć do jak najszybszego uzyskania zezwolenia, podając jednocześnie powody, dla których nie mógł wystąpić o nie wcześniej.

(22) Ponadto należy zapewnić, w wyczerpujących ramach określonych w niniejszym rozporządzeniu, aby takie wykorzystanie na terytorium państwa członkowskiego zgodnie z niniejszym rozporządzeniem było możliwe tylko wówczas gdy – i w zakresie, w jakim – dane państwo członkowskie postanowiło wyraźnie przewidzieć możliwość zezwolenia na takie wykorzystanie w swoich szczegółowych przepisach prawa krajowego. W związku z tym państwa członkowskie mogą na mocy niniejszego rozporządzenia w ogóle nie przewidywać takiej możliwości lub przewidzieć ją jedynie w odniesieniu do niektórych celów mogących uzasadniać dozwolone wykorzystanie, określonych w niniejszym rozporządzeniu.

(23) Wykorzystanie systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa nieuchronnie wiąże się z przetwarzaniem danych biometrycznych. Przepisy niniejszego rozporządzenia zakazujące, z zastrzeżeniem pewnych wyjątków, takiego wykorzystywania, a których podstawę stanowi art. 16 TFUE, powinny mieć zastosowanie jako *lex specialis* w odniesieniu do przepisów dotyczących przetwarzania danych biometrycznych zawartych w art. 10 dyrektywy (UE) 2016/680, regulując tym samym w sposób wyczerpujący takie wykorzystywanie i przetwarzanie wspomnianych danych biometrycznych. W związku z tym takie wykorzystywanie i przetwarzanie powinno być możliwe wyłącznie w zakresie, w jakim jest zgodne z ramami określonymi w niniejszym rozporządzeniu, przy czym stosowanie takich systemów i przetwarzanie odnośnych danych przez właściwe organy – gdy działają w celu egzekwowania prawa – w oparciu o przesłanki wymienione w art. 10 dyrektywy (UE) 2016/680 może mieć miejsce wyłącznie w granicach nakreślonych przez te ramy. W tym kontekście niniejsze rozporządzenie nie ma na celu zapewnienia podstawy prawnej do przetwarzania danych osobowych na podstawie art. 8 dyrektywy (UE) 2016/680. Wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów innych niż egzekwowanie prawa, w tym przez właściwe organy, nie powinno być jednak objęte szczegółowymi ramami dotyczącymi takiego wykorzystywania do celów egzekwowania prawa, określonymi w niniejszym rozporządzeniu. Takie wykorzystywanie do celów innych niż egzekwowanie prawa nie powinno zatem podlegać wymogowi uzyskania zezwolenia na mocy niniejszego rozporządzenia i obowiązujących szczegółowych przepisów prawa krajowego, które mogą stanowić podstawę jego wykonania.

(24) Wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane ze stosowaniem systemów sztucznej inteligencji do identyfikacji biometrycznej, inne niż w związku z wykorzystywaniem systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa zgodnie z przepisami niniejszego rozporządzenia, w tym w przypadku gdy systemy te są stosowane przez właściwe organy w przestrzeni publicznej do celów innych niż egzekwowanie prawa, powinno nadal spełniać wszystkie wymogi wynikające, stosownie do przypadku, z art. 9 ust. 1 rozporządzenia (UE) 2016/679, art. 10 ust. 1 rozporządzenia (UE) 2018/1725 oraz art. 10 dyrektywy (UE) 2016/680.

(25) Zgodnie z art. 6a Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i TFUE, Irlandia nie jest związana przepisami określonymi w art. 5 ust. 1 lit. d) oraz art. 5 ust. 2 i 3 niniejszego rozporządzenia przyjętymi na podstawie art. 16 TFUE, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdziały 4 lub 5 TFUE, jeśli Irlandia nie jest związana przepisami Unii w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy przestrzegać przepisów ustanowionych na podstawie art. 16 TFUE.

(26) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i TFUE, Dania nie jest związana przepisami określonymi w art. 5 ust. 1 lit. d) oraz art. 5 ust. 2 i 3 niniejszego rozporządzenia przyjętymi na podstawie art. 16 TFUE, które dotyczą przetwarzania danych osobowych przez państwa członkowskie

w wykonywaniu działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdziały 4 lub 5 TFUE, ani przepisy te nie mają do niej zastosowania.

(27) Systemy sztucznej inteligencji wysokiego ryzyka powinny być wprowadzane do obrotu w Unii lub oddawane do użytku wyłącznie wówczas, gdy spełniają określone obowiązkowe wymogi. Wymogi te powinny zapewniać, aby systemy sztucznej inteligencji wysokiego ryzyka dostępne w Unii lub takie, których wyniki działania są w inny sposób wykorzystywane w Unii, nie stwarzały niedopuszczalnego ryzyka dla istotnych interesów publicznych Unii uznanych w prawie Unii i przez nie chronionych. Klasyfikację systemów sztucznej inteligencji jako systemów wysokiego ryzyka należy ograniczyć do tych systemów, które mają znaczący szkodliwy wpływ na zdrowie, bezpieczeństwo i prawa podstawowe osób w Unii, przy czym takie ograniczenie powinno minimalizować wszelkie potencjalne przeszkody w handlu międzynarodowym, o ile występują.

(28) Systemy sztucznej inteligencji mogą wywoływać szkodliwe skutki dla zdrowia i bezpieczeństwa osób, w szczególności w przypadku, gdy takie systemy funkcjonują jako elementy produktów. Zgodnie z celami określonymi w unijnym prawodawstwie harmonizacyjnym, polegającymi na ułatwieniu swobodnego przepływu produktów na rynku wewnętrznym oraz zapewnieniu, aby na rynek trafiały wyłącznie produkty bezpieczne i spełniające pozostałe wymogi, istotne jest odpowiednie zapobieganie i ograniczanie zagrożeń dla bezpieczeństwa, które mogą być powodowane przez produkt jako całość ze względu na jego elementy cyfrowe, w tym systemy sztucznej inteligencji. Na przykład coraz bardziej autonomiczne roboty, zarówno w kontekście działalności produkcyjnej, jak i świadczenia pomocy oraz opieki osobistej, powinny być w stanie bezpiecznie funkcjonować i wykonywać swoje funkcje w złożonych środowiskach. Podobnie w sektorze opieki zdrowotnej, w którym chodzi o szczególnie wysoką stawkę, jaką jest życie i zdrowie, coraz bardziej zaawansowane systemy diagnostyczne i systemy wspomagające decyzje podejmowane przez człowieka powinny być niezawodne i dokładne. Przy klasyfikowaniu systemu sztucznej inteligencji jako systemu wysokiego ryzyka zasadnicze znaczenie ma skala szkodliwego wpływu wywieranego przez system sztucznej inteligencji na prawa podstawowe chronione na mocy Karty. Do praw tych należą: prawo do godności człowieka, poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji, wolność zgromadzania się i stowarzyszania się oraz niedyskryminacja, ochrona konsumentów, prawa pracownicze, prawa osób niepełnosprawnych, prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawo do obrony i domniemania niewinności, prawo do dobrej administracji. Oprócz tych praw należy podkreślić, że dzieciom przysługują szczególne prawa zapisane w art. 24 Karty praw podstawowych UE oraz w Konwencji o prawach dziecka (szerzej rozwinięte w komentarzu ogólnym nr 25 do Konwencji ONZ o prawach dziecka w odniesieniu do środowiska cyfrowego), które wymagają uwzględnienia słabości dzieci oraz zapewnienia im takiej ochrony i opieki, jaka jest konieczna dla ich dobra. Podstawowe prawo do wysokiego poziomu ochrony środowiska zapisane w Karcie i wdrażane w strategiach politycznych Unii również należy uwzględnić w ocenie powagi szkody, jaką może spowodować system sztucznej inteligencji, w tym w odniesieniu do zdrowia i bezpieczeństwa osób.

(29) Jeżeli chodzi o systemy sztucznej inteligencji wysokiego ryzyka, które są związanymi z bezpieczeństwem elementami produktów lub systemów objętych zakresem

rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008[39], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 167/2013[40], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013[41], dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE[42], dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/797[43], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858[44], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139[45] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2144[46] lub które same są takimi produktami lub systemami, wskazane jest wprowadzenie zmian do tych aktów w celu zapewnienia, aby przyjmując wszelkie stosowne przyszłe akty delegowane lub wykonawcze na podstawie wspomnianych aktów, Komisja uwzględniła – w oparciu o techniczną i regulacyjną charakterystykę każdego sektora oraz bez ingerowania w istniejące mechanizmy i organy zarządzania, oceny zgodności i egzekwowania ustanowione w tych aktach – obowiązkowe wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka określone w niniejszym rozporządzeniu.

(30) W przypadku systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami produktów lub które same są produktami objętymi zakresem stosowania niektórych przepisów unijnego prawodawstwa harmonizacyjnego, systemy te należy klasyfikować jako systemy wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, jeżeli dany produkt jest poddawany

---

39 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz.U. L 97 z 9.4.2008, s. 72).

40 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 167/2013 z dnia 5 lutego 2013 r. w sprawie homologacji i nadzoru rynku pojazdów rolniczych i leśnych (Dz.U. L 60 z 2.3.2013, s. 1).

41 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 168/2013 z dnia 15 stycznia 2013 r. w sprawie homologacji i nadzoru rynku pojazdów dwu- lub trzykołowych oraz czterokołowców (Dz.U. L 60 z 2.3.2013, s. 52).

42 Dyrektywa Parlamentu Europejskiego i Rady 2014/90/UE z dnia 23 lipca 2014 r. w sprawie wyposażenia morskiego i uchylająca dyrektywę Rady 96/98/WE (Dz.U. L 257 z 28.8.2014, s. 146).

43 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/797 z dnia 11 maja 2016 r. w sprawie interoperacyjności systemu kolei w Unii Europejskiej (Dz.U. L 138 z 26.5.2016, s. 44).

44 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 z dnia 30 maja 2018 r. w sprawie homologacji i nadzoru rynku pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, zmieniające rozporządzenie (WE) nr 715/2007 i (WE) nr 595/2009 oraz uchylające dyrektywę 2007/46/WE (Dz.U. L 151 z 14.6.2018, s. 1).

45 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz.U. L 212 z 22.8.2018, s. 1).

46 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2144 z dnia 27 listopada 2019 r. w sprawie wymogów dotyczących homologacji typu pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, w odniesieniu do ich ogólnego bezpieczeństwa oraz ochrony osób znajdujących się w pojeździe i niechronionych uczestników ruchu drogowego, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 oraz uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 78/2009, (WE) nr 79/2009 i (WE) nr 661/2009 oraz rozporządzenia Komisji (WE) nr 631/2009, (UE) nr 406/2010, (UE) nr 672/2010, (UE) nr 1003/2010, (UE) nr 1005/2010, (UE) nr 1008/2010, (UE) nr 1009/2010, (UE) nr 19/2011, (UE) nr 109/2011, (UE) nr 458/2011, (UE) nr 65/2012, (UE) nr 130/2012, (UE) nr 347/2012, (UE) nr 351/2012, (UE) nr 1230/2012 i (UE) 2015/166 (Dz.U. L 325 z 16.12.2019, s. 1).

procedurze oceny zgodności przez jednostkę oceniającą zgodność będącą osobą trzecią na podstawie tych stosownych przepisów unijnego prawodawstwa harmonizacyjnego. W szczególności produktami takimi są maszyny, zabawki, dźwigi, urządzenia i systemy ochronne przeznaczone do użytku w atmosferze potencjalnie wybuchowej, urządzenia radiowe, urządzenia ciśnieniowe, wyposażenie rekreacyjnych jednostek pływających, urządzenia kolei linowych, urządzenia spalające paliwa gazowe, wyroby medyczne oraz wyroby medyczne do diagnostyki *in vitro*.

(31) Klasyfikacja systemu sztucznej inteligencji jako systemu wysokiego ryzyka na podstawie niniejszego rozporządzenia nie powinna koniecznie oznaczać, że produkt, którego związanym z bezpieczeństwem elementem jest system sztucznej inteligencji, lub sam system sztucznej inteligencji jako produkt uznaje się za produkt „wysokiego ryzyka" zgodnie z kryteriami ustanowionymi w stosownym unijnym prawodawstwie harmonizacyjnym, które ma zastosowanie do tego produktu. Ma to miejsce w szczególności w przypadku rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745[47] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746[48], w których ocenę zgodności przeprowadzaną przez osobę trzecią przewidziano dla produktów średniego i wysokiego ryzyka.

(32) Jeżeli chodzi o samodzielne systemy sztucznej inteligencji, tj. systemy sztucznej inteligencji wysokiego ryzyka inne niż te, które są związanymi z bezpieczeństwem elementami produktów lub które same są produktami, należy je klasyfikować jako systemy wysokiego ryzyka, jeżeli w związku z ich przeznaczeniem stwarzają one wysokie ryzyko powstania szkody dla zdrowia i bezpieczeństwa lub praw podstawowych osób, biorąc pod uwagę zarówno skalę potencjalnych szkód, jak i prawdopodobieństwo ich wystąpienia, oraz jeżeli są one wykorzystywane w szeregu ściśle określonych z góry obszarów wskazanych w rozporządzeniu. Identyfikacja tych systemów opiera się na tej samej metodyce i tych samych kryteriach, które przewidziano także dla wszelkich przyszłych zmian w wykazie systemów sztucznej inteligencji wysokiego ryzyka.

(33) Techniczne niedokładności systemów sztucznej inteligencji przeznaczonych do zdalnej identyfikacji biometrycznej osób fizycznych mogą prowadzić do nieobiektywnych wyników i wywoływać skutki w postaci dyskryminacji. Jest to szczególnie istotne, jeżeli chodzi o wiek, pochodzenie etniczne, płeć lub niepełnosprawność. W związku z tym systemy zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" i „post factum" należy klasyfikować jako systemy wysokiego ryzyka. Ze względu na zagrożenia, które stwarzają, oba rodzaje systemów zdalnej identyfikacji biometrycznej powinny podlegać szczególnym wymogom dotyczącym funkcji rejestracji zdarzeń i nadzoru ze strony człowieka.

(34) W odniesieniu do zarządzania infrastrukturą krytyczną i jej funkcjonowania wskazane jest klasyfikowanie jako systemy wysokiego ryzyka systemów sztucznej inteligencji, które mają być użytkowane jako związane z bezpieczeństwem elementy procesów zarządzania i obsługi ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło

---

47 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. L 117 z 5.5.2017, s. 1).

48 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.U. L 117 z 5.5.2017, s. 176).

i energię elektryczną, ponieważ ich awaria lub nieprawidłowe działanie mogą stanowić zagrożenie dla życia i zdrowia osób na dużą skalę i prowadzić do znacznych zakłóceń w zwykłym prowadzeniu działalności społecznej i gospodarczej.

(35) Systemy sztucznej inteligencji wykorzystywane w obszarze kształcenia lub szkolenia zawodowego, w szczególności przy podejmowaniu decyzji o dostępie do instytucji kształcenia i szkolenia zawodowego lub nadawaniu osobom przydziału do tych instytucji lub też do oceniania osób na testach w ramach kształcenia lub jako warunek dopuszczenia do kształcenia, należy uznać za systemy wysokiego ryzyka, ponieważ mogą one decydować o przebiegu kształcenia i kariery zawodowej danej osoby, a tym samym wpływać na jej zdolność do zapewnienia sobie źródła utrzymania. Takie systemy, jeżeli są niewłaściwie zaprojektowane i nieodpowiednio stosowane, mogą naruszać prawo do nauki i odbywania szkoleń, a także prawo do niedyskryminacji i mogą utrwalać historyczne wzorce dyskryminacji.

(36) Systemy sztucznej inteligencji wykorzystywane w obszarze zatrudnienia, zarządzania pracownikami i dostępu do samozatrudnienia, w szczególności do rekrutacji i wyboru kandydatów, do podejmowania decyzji o awansie i rozwiązaniu stosunku pracy oraz do przydzielania zadań, monitorowania lub oceny osób pozostających w umownych stosunkach pracy, należy również klasyfikować jako systemy wysokiego ryzyka, ponieważ systemy te mogą w znacznym stopniu wpływać na przyszłe perspektywy zawodowe i źródła utrzymania tych osób. Odnośne umowne stosunki pracy powinny obejmować pracowników i osoby pracujące za pośrednictwem platform internetowych, o których mowa w programie prac Komisji na 2021 r. Co do zasady osób takich nie należy uznawać za użytkowników w rozumieniu niniejszego rozporządzenia. W całym procesie rekrutacji oraz w ramach oceny, awansu lub retencji osób pozostających w umownych stosunkach pracy systemy takie mogą utrwalać historyczne wzorce dyskryminacji, na przykład wobec kobiet, niektórych grup wiekowych, osób z niepełnosprawnościami lub osób o określonym pochodzeniu rasowym lub etnicznym bądź określonej orientacji seksualnej. Systemy sztucznej inteligencji wykorzystywane do monitorowania wydajności i zachowania tych osób mogą wpływać również na ich prawo do ochrony danych i prywatności.

(37) Innym obszarem, w którym stosowanie systemów sztucznej inteligencji zasługuje na szczególną uwagę, jest dostęp do niektórych podstawowych usług i świadczeń prywatnych i publicznych niezbędnych ludziom do pełnego uczestnictwa w życiu społecznym lub do poprawy poziomu życia oraz korzystanie z tych usług i świadczeń. W szczególności systemy sztucznej inteligencji wykorzystywane do przeprowadzania punktowej oceny kredytowej lub oceny zdolności kredytowej osób fizycznych należy klasyfikować jako systemy wysokiego ryzyka, ponieważ decydują one o dostępie tych osób do zasobów finansowych lub podstawowych usług, takich jak mieszkalnictwo, energia elektryczna i usługi telekomunikacyjne. Systemy sztucznej inteligencji wykorzystywane w tym celu mogą prowadzić do dyskryminacji osób lub grup i utrwalać historyczne wzorce dyskryminacji, na przykład ze względu na pochodzenie rasowe lub etniczne, niepełnosprawność, wiek, orientację seksualną, lub powodować powstawanie dyskryminujących skutków w nowej postaci. Biorąc pod uwagę bardzo ograniczoną skalę skutków i dostępność na rynku alternatywnych rozwiązań, wskazane jest wyłączenie systemów sztucznej inteligencji stosowanych do oceny zdolności kredytowej i punktowej oceny kredytowej, w przypadku gdy są one oddawane do użytku przez drobnych dostawców na ich własny użytek. Osoby fizyczne ubiegające się o świadczenia i usługi w ramach pomocy publicznej zapewniane przez organy publiczne lub korzystające z takich świadczeń i usług są

zazwyczaj zależne od tych świadczeń i usług oraz znajdują się w słabszym położeniu względem odpowiedzialnych organów. Jeżeli systemy sztucznej inteligencji są wykorzystywane do ustalenia, czy organy powinny odmówić takich świadczeń i usług, ograniczyć je, cofnąć lub odzyskać, mogą one mieć znaczący wpływ na źródła utrzymania osób i mogą naruszać ich prawa podstawowe, takie jak prawo do ochrony socjalnej, niedyskryminacji, godności człowieka lub skutecznego środka prawnego. W związku z tym systemy te należy klasyfikować jako systemy wysokiego ryzyka. Niniejsze rozporządzenie nie powinno jednak utrudniać rozwoju i stosowania innowacyjnych rozwiązań w administracji publicznej, która może odnieść korzyści z powszechniejszego wykorzystywania spełniających odnośne wymogi i bezpiecznych systemów sztucznej inteligencji, pod warunkiem że systemy te nie stwarzają wysokiego ryzyka dla osób prawnych i fizycznych. Ponadto systemy sztucznej inteligencji wykorzystywane do wysyłania służb pierwszej pomocy w sytuacjach nadzwyczajnych lub ustalania priorytetów w ich wysyłaniu również należy klasyfikować jako systemy wysokiego ryzyka, ponieważ służą one do podejmowania decyzji o krytycznym znaczeniu dla życia i zdrowia osób oraz ich mienia.

(38) Działania organów ścigania związane z niektórymi zastosowaniami systemów sztucznej inteligencji charakteryzują się znacznym brakiem równowagi sił i mogą prowadzić do objęcia osoby fizycznej niejawnym nadzorem, do jej aresztowania lub pozbawienia wolności, jak również do zaistnienia innych niekorzystnych skutków dla praw podstawowych gwarantowanych w Karcie. W szczególności jeżeli system sztucznej inteligencji nie jest trenowany z wykorzystaniem danych wysokiej jakości, nie spełnia odpowiednich wymogów pod względem dokładności lub solidności lub nie został odpowiednio zaprojektowany i przetestowany przed wprowadzeniem do obrotu lub oddaniem do użytku w inny sposób, może on wskazywać osoby w sposób dyskryminacyjny lub w inny nieprawidłowy lub niesprawiedliwy sposób. Ponadto korzystanie z istotnych procesowych praw podstawowych, takich jak prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, jak również prawo do obrony i domniemania niewinności, może być utrudnione, w szczególności w przypadku gdy takie systemy sztucznej inteligencji nie są w wystarczającym stopniu przejrzyste, wyjaśnialne i udokumentowane. W związku z tym szereg systemów sztucznej inteligencji przeznaczonych do stosowania w kontekście egzekwowania prawa, w którym dokładność, wiarygodność i przejrzystość są szczególnie ważne dla uniknięcia szkodliwych skutków, zachowania zaufania publicznego oraz zapewnienia odpowiedzialności i skutecznego dochodzenia roszczeń, należy klasyfikować jako systemy wysokiego ryzyka. Ze względu na charakter przedmiotowych działań i związane z nimi ryzyko do systemów sztucznej inteligencji wysokiego ryzyka należy zaliczyć w szczególności systemy sztucznej inteligencji przeznaczone do stosowania przez organy ścigania do przeprowadzenia indywidualnej oceny ryzyka, jako poligrafy i podobne narzędzia lub do wykrywania stanu emocjonalnego osoby fizycznej, do wykrywania treści typu „deepfake”, do oceny wiarygodności dowodów w postępowaniu karnym, do przewidywania wystąpienia lub ponownego wystąpienia faktycznego lub potencjalnego przestępstwa na podstawie profilowania osób fizycznych lub oceny cech osobowości i charakterystyki lub wcześniejszego zachowania przestępnego osób fizycznych lub grup, do profilowania w trakcie wykrywania przestępstw, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania, jak również do analizy przestępczości osób fizycznych. Systemów sztucznej inteligencji specjalnie przeznaczonych do stosowania w postępowaniach administracyjnych prowadzonych przez organy podatkowe i celne nie należy uznawać za systemy sztucznej inteligencji wysokiego ryzyka wykorzystywane przez organy

ścigania do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

(39) Systemy sztucznej inteligencji wykorzystywane w zarządzaniu migracją, azylem i kontrolą graniczną mają wpływ na osoby, które często znajdują się w szczególnie trudnej sytuacji i które są zależne od rezultatów działań właściwych organów publicznych. Dokładność, niedyskryminujący charakter i przejrzystość systemów sztucznej inteligencji wykorzystywanych w tych kontekstach są zatem szczególnie istotne w celu zapewnienia poszanowania praw podstawowych zainteresowanych osób, w szczególności ich prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji. Za systemy wysokiego ryzyka należy zatem uznać systemy sztucznej inteligencji przeznaczone do wykorzystywania przez właściwe organy publiczne odpowiedzialne za wykonywanie zadań w dziedzinach zarządzania migracją, azylem i kontrolą graniczną jako poligrafy i podobne narzędzia lub do wykrywania stanu emocjonalnego osoby fizycznej; w celu oceny niektórych zagrożeń stwarzanych przez osoby fizyczne wjeżdżające na terytorium państwa członkowskiego lub ubiegające się o wizę lub azyl; w celu weryfikacji autentyczności odpowiednich dokumentów osób fizycznych; w celu udzielenia pomocy właściwym organom publicznym przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do celu, jakim jest ustalenie kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu. Systemy sztucznej inteligencji w obszarze zarządzania migracją, azylem i kontrolą graniczną objęte niniejszym rozporządzeniem powinny być zgodne z odpowiednimi wymogami proceduralnymi określonymi w dyrektywie Parlamentu Europejskiego i Rady 2013/32/UE[49], rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 810/2009[50] i innych właściwych przepisach.

(40) Niektóre systemy sztucznej inteligencji przeznaczone na potrzeby sprawowania wymiaru sprawiedliwości i procesów demokratycznych należy sklasyfikować jako systemy wysokiego ryzyka, biorąc pod uwagę ich potencjalnie istotny wpływ na demokrację, praworządność, wolności osobiste, a także prawo do skutecznego środka odwoławczego i do rzetelnego procesu sądowego. W szczególności, aby wyeliminować potencjalne ryzyko tendencyjności, efektu czarnej skrzynki i błędów, jako systemy wysokiego ryzyka należy kwalifikować systemy sztucznej inteligencji, które mają za zadanie pomóc organom sądowym w badaniu i interpretacji faktów i przepisów oraz w stosowaniu tych przepisów do konkretnego stanu faktycznego. Taka kwalifikacja nie powinna jednak rozciągać się na systemy sztucznej inteligencji przeznaczone do czysto pomocniczych czynności administracyjnych, które nie mają wpływu na faktyczne sprawowanie wymiaru sprawiedliwości w poszczególnych przypadkach, takich jak anonimizacja lub pseudonimizacja orzeczeń sądowych, dokumentów lub danych, komunikacja między członkami personelu, zadania administracyjne lub przydział zasobów.

(41) Faktu, że dany system sztucznej inteligencji został sklasyfikowany jako system wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, nie należy interpretować

---

[49] Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (Dz.U. L 180 z 29.6.2013, s. 60).

[50] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz.U. L 243 z 15.9.2009, s. 1).

jako wskazującego na to, że korzystanie z tego systemu jest siłą rzeczy zgodne z prawem na gruncie innych aktów prawa Unii lub prawa krajowego zgodnego z prawem Unii, na przykład w zakresie ochrony danych osobowych, stosowania poligrafów i podobnych narzędzi lub innych systemów służących wykrywaniu stanu emocjonalnego osób fizycznych. Każde takie wykorzystanie należy kontynuować wyłącznie w sposób zgodny z mającymi zastosowanie wymogami wynikającymi z Karty oraz z mającymi zastosowanie aktami prawa wtórnego Unii i prawa krajowego. Niniejszego rozporządzenia nie należy rozumieć jako ustanawiającego podstawę prawną przetwarzania danych osobowych, w tym w stosownych przypadkach szczególnych kategorii danych osobowych.

(42) Aby ograniczyć ryzyko dla użytkowników i zainteresowanych osób stwarzane przez systemy sztucznej inteligencji wysokiego ryzyka wprowadzone do obrotu lub w inny sposób oddawane do użytku na rynku unijnym, należy wprowadzić pewne obowiązkowe wymogi, z uwzględnieniem docelowego zastosowania systemu oraz zgodnie z systemem zarządzania ryzykiem, który ma zostać ustanowiony przez dostawcę.

(43) Systemy sztucznej inteligencji wysokiego ryzyka powinny podlegać wymogom dotyczącym jakości wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji użytkownikom, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Wymogi te są konieczne, aby skutecznie ograniczyć zagrożenia dla zdrowia, bezpieczeństwa i praw podstawowych, w stosownych przypadkach w świetle przeznaczenia systemu, gdy nie są racjonalnie dostępne inne środki, które powodowałyby mniejsze ograniczenia w handlu, co pozwala uniknąć nieuzasadnionych ograniczeń w handlu.

(44) Wysoka jakość danych ma zasadnicze znaczenie dla skuteczności działania wielu systemów sztucznej inteligencji, w szczególności w przypadku stosowania technik obejmujących trenowanie modeli, w celu zapewnienia, aby system sztucznej inteligencji wysokiego ryzyka działał zgodnie z przeznaczeniem i bezpiecznie oraz aby nie stał się źródłem zakazanej przez prawo Unii dyskryminacji. Wysokiej jakości zbiory danych treningowych, walidacyjnych i testowych wymagają wdrożenia odpowiednich praktyk w zakresie zarządzania danymi. Zbiory danych treningowych, walidacyjnych i testowych powinny być wystarczająco adekwatne, reprezentatywne i wolne od błędów oraz kompletne z punktu widzenia przeznaczenia systemu. Powinny one również charakteryzować się odpowiednimi właściwościami statystycznymi, w tym w odniesieniu do osób lub grup osób, wobec których system sztucznej inteligencji wysokiego ryzyka ma być wykorzystywany. W szczególności zbiory danych treningowych, walidacyjnych i testowych powinny uwzględniać – w zakresie wymaganym w świetle ich przeznaczenia – cechy, właściwości lub elementy, które są specyficzne dla określonego kontekstu geograficznego, behawioralnego lub funkcjonalnego lub okoliczności, w których system sztucznej inteligencji ma być wykorzystywany. Aby chronić prawa innych osób przed dyskryminacją, która może wynikać z tendencyjności systemów sztucznej inteligencji, dostawcy powinni mieć możliwość przetwarzania również szczególnych kategorii danych osobowych przez wzgląd na istotny interes publiczny w celu zapewnienia monitorowania, wykrywania i eliminowania tendencyjności w systemach sztucznej inteligencji wysokiego ryzyka.

(45) W celu opracowania systemów sztucznej inteligencji wysokiego ryzyka niektóre podmioty, takie jak dostawcy, jednostki notyfikowane i inne odpowiednie podmioty,

w tym ośrodki innowacji cyfrowych, ośrodki testowo-doświadczalne i naukowcy, powinny mieć możliwość uzyskania dostępu do wysokiej jakości zbiorów danych i korzystania z nich w swoich odpowiednich obszarach działalności związanych z niniejszym rozporządzeniem. Wspólne europejskie przestrzenie danych ustanowione przez Komisję oraz ułatwienie wymiany danych między przedsiębiorstwami i udostępniania danych administracji publicznej w interesie publicznym będą miały zasadnicze znaczenie dla zapewnienia zaufanego, odpowiedzialnego i niedyskryminacyjnego dostępu do danych wysokiej jakości na potrzeby trenowania, walidacji i testowania systemów sztucznej inteligencji. Na przykład w dziedzinie zdrowia europejska przestrzeń danych dotyczących zdrowia ułatwi niedyskryminacyjny dostęp do danych dotyczących zdrowia oraz trenowanie algorytmów sztucznej inteligencji na tych zbiorach danych w sposób bezpieczny, terminowy, przejrzysty, wiarygodny i zapewniający ochronę prywatności oraz przy odpowiednim zarządzaniu instytucjonalnym. Odpowiednie właściwe organy, w tym organy sektorowe, zapewniające dostęp do danych lub wspierające taki dostęp, mogą również wspierać dostarczanie wysokiej jakości danych na potrzeby trenowania, walidacji i testowania systemów sztucznej inteligencji.

(46) Dysponowanie informacjami na temat tego, w jaki sposób opracowano systemy sztucznej inteligencji wysokiego ryzyka i jak działają one w całym cyklu życia, ma zasadnicze znaczenie dla weryfikacji zgodności z wymogami określonymi w niniejszym rozporządzeniu. Wymaga to prowadzenia rejestrów zdarzeń oraz zapewnienia dostępności dokumentacji technicznej zawierającej informacje niezbędne do oceny zgodności systemu sztucznej inteligencji z odpowiednimi wymogami. Informacje takie powinny obejmować ogólne właściwości, możliwości i ograniczenia systemu, algorytmy, dane, procesy związane z trenowaniem, testowaniem i walidacją, a także dokumentację dotyczącą odpowiedniego systemu zarządzania ryzykiem. Dokumentacja techniczna powinna podlegać aktualizacji.

(47) Aby zapobiec efektowi czarnej skrzynki, który może sprawić, że niektóre systemy sztucznej inteligencji staną się niezrozumiałe lub zbyt skomplikowane dla osób fizycznych, od systemów sztucznej inteligencji wysokiego ryzyka należy wymagać zapewnienia określonego stopnia przejrzystości. Użytkownicy powinni być w stanie interpretować wyniki działania systemu i odpowiednio z nich korzystać. W związku z tym do systemów sztucznej inteligencji wysokiego ryzyka należy dołączać odpowiednią dokumentację i instrukcję obsługi, a w stosownych przypadkach systemy te powinny zawierać zwięzłe i jasne informacje, w tym informacje dotyczące ewentualnego zagrożenia dla praw podstawowych oraz dyskryminacji.

(48) Systemy sztucznej inteligencji wysokiego ryzyka należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie. W tym celu przed wprowadzeniem systemu do obrotu lub jego oddaniem do użytku dostawca systemu powinien określić odpowiednie środki związane z nadzorem ze strony człowieka. W szczególności, w stosownych przypadkach, takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka–operatora systemu, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru ze strony człowieka, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji.

(49) Systemy sztucznej inteligencji wysokiego ryzyka powinny działać w sposób spójny w całym cyklu życia i charakteryzować się odpowiednim poziomem dokładności, solidności i cyberbezpieczeństwa zgodnie z powszechnie uznawanym stanem wiedzy.

O poziomie dokładności i wskaźnikach dokładności należy informować użytkowników.

(50) Kluczowym wymogiem dotyczącym systemów sztucznej inteligencji wysokiego ryzyka jest solidność techniczna. Systemy te powinny być odporne na zagrożenia związane z ograniczeniami systemu (np. błędami, usterkami, niespójnościami, nieprzewidzianymi sytuacjami), jak również na szkodliwe działania, które mogą naruszyć bezpieczeństwo systemu sztucznej inteligencji i prowadzić do szkodliwych lub innych niepożądanych zachowań. Brak ochrony przed tymi zagrożeniami może mieć konsekwencje dla bezpieczeństwa lub negatywnie wpłynąć na prawa podstawowe, na przykład z powodu błędnych decyzji bądź nieprawidłowych lub tendencyjnych wyników działania generowanych przez system sztucznej inteligencji.

(51) Cyberbezpieczeństwo odgrywa kluczową rolę w zapewnianiu odporności systemów sztucznej inteligencji na próby modyfikacji ich zastosowania, zachowania, skuteczności działania lub obejścia ich zabezpieczeń przez działające w złej wierze osoby trzecie wykorzystujące podatności systemu. Cyberataki na systemy sztucznej inteligencji mogą polegać na wykorzystaniu konkretnych zasobów, takich jak zbiory danych treningowych (np. „data poisoning") lub trenowane modele (np. ataki polegające na wprowadzeniu do modelu złośliwych danych w celu spowodowania niezamierzonego działania systemu), lub wykorzystaniu podatności w zasobach cyfrowych systemu sztucznej inteligencji lub w infrastrukturze ICT, na której opiera się dany system. Aby zapewnić poziom cyberbezpieczeństwa odpowiedni do ryzyka, dostawcy systemów sztucznej inteligencji wysokiego ryzyka powinni zatem wdrożyć odpowiednie środki, uwzględniając również w stosownych przypadkach infrastrukturę ICT, na której opiera się dany system.

(52) W ramach unijnego prawodawstwa harmonizacyjnego przepisy mające zastosowanie do wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka należy ustanowić zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008[51] ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku produktów, decyzją Parlamentu Europejskiego i Rady nr 768/2008/WE[52] w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/1020[53] w sprawie nadzoru rynku i zgodności produktów („nowe ramy prawne").

(53) Należy zapewnić, aby odpowiedzialność za wprowadzenie do obrotu lub oddanie do użytku systemu sztucznej inteligencji wysokiego ryzyka brała na siebie konkretna osoba fizyczna lub prawna określona jako dostawca, niezależnie od tego, czy ta osoba fizyczna lub prawna jest osobą, która zaprojektowała lub opracowała ten system.

---

[51] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

[52] Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz.U. L 218 z 13.8.2008, s. 82).

[53] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (tekst mający znaczenie dla EOG) (Dz.U. L 169 z 25.6.2019, s. 1).

(54) Dostawca powinien ustanowić skuteczny system zarządzania jakością, zapewnić przeprowadzenie wymaganej procedury oceny zgodności, sporządzić odpowiednią dokumentację i ustanowić solidny system monitorowania po wprowadzeniu do obrotu. Organy publiczne, które oddają do użytku systemy sztucznej inteligencji wysokiego ryzyka na własny użytek, mogą przyjąć i wdrożyć zasady dotyczące systemu zarządzania jakością w ramach systemu zarządzania jakością przyjętego, stosownie do przypadku, na szczeblu krajowym lub regionalnym, z uwzględnieniem specyfiki sektora oraz kompetencji i organizacji danego organu publicznego.

(55) W przypadku gdy system sztucznej inteligencji wysokiego ryzyka będący związanym z bezpieczeństwem elementem produktu, który jest objęty właściwymi przepisami sektorowymi nowych ram prawnych, nie jest wprowadzany do obrotu ani oddawany do użytku niezależnie od produktu, producent produktu końcowego, w rozumieniu właściwych przepisów nowych ram prawnych, powinien przestrzegać obowiązków dostawcy określonych w niniejszym rozporządzeniu, a w szczególności powinien zapewnić zgodność systemu sztucznej inteligencji wbudowanego w produkt końcowy z wymogami niniejszego rozporządzenia.

(56) W celu umożliwienia egzekwowania niniejszego rozporządzenia i stworzenia równych warunków działania dla operatorów, a także biorąc pod uwagę różnorakie formy udostępniania produktów cyfrowych, należy zapewnić, aby osoba mająca siedzibę w Unii zawsze była w stanie przekazać organom wszystkie niezbędne informacje dotyczące zgodności systemu sztucznej inteligencji z przepisami. W związku z tym w przypadku, gdy nie ma możliwości zidentyfikowania importera, dostawcy mający siedzibę poza terytorium Unii są zobowiązani wyznaczyć – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego siedzibę w Unii przed udostępnieniem swoich systemów sztucznej inteligencji w Unii.

(57) Zgodnie z zasadami nowych ram prawnych należy określić szczegółowe obowiązki odpowiednich operatorów, takich jak importerzy i dystrybutorzy, aby zagwarantować pewność prawa i ułatwić tym podmiotom przestrzeganie przepisów.

(58) Ze względu na naturę systemów sztucznej inteligencji oraz zagrożenia dla bezpieczeństwa i praw podstawowych, jakie mogą wiązać się z ich wykorzystywaniem, w tym uwzględniając potrzebę zapewnienia właściwego monitorowania skuteczności działania systemu sztucznej inteligencji w warunkach rzeczywistych, należy określić szczególne obowiązki użytkowników. Użytkownicy powinni w szczególności korzystać z systemów sztucznej inteligencji wysokiego ryzyka zgodnie z instrukcjami obsługi, a w stosownych przypadkach należy przewidzieć określone inne obowiązki w odniesieniu do monitorowania funkcjonowania systemów sztucznej inteligencji oraz rejestrowania zdarzeń.

(59) Należy przewidzieć, że za użytkownika systemu sztucznej inteligencji uznaje się osobę fizyczną lub prawną, organ publiczny, agencję lub inny organ, które odpowiadają za eksploatację systemu sztucznej inteligencji, chyba że system jest wykorzystywany w ramach osobistej działalności pozazawodowej.

(60) Ponieważ łańcuch wartości sztucznej inteligencji jest złożony, odpowiednie osoby trzecie – w szczególności zajmujące się sprzedażą i dostarczaniem oprogramowania, narzędzi i elementów oprogramowania, wcześniej wytrenowanych modeli i danych lub dostawcy usług sieciowych – powinny współpracować, w stosownych przypadkach, z dostawcami i użytkownikami, aby umożliwić im wypełnianie obowiązków wynikających z niniejszego rozporządzenia, oraz z właściwymi organami ustanowionymi na podstawie niniejszego rozporządzenia.

(61) Kluczową rolę w dostarczaniu dostawcom rozwiązań technicznych w celu zapewnienia zgodności z niniejszym rozporządzeniem powinna odgrywać normalizacja. Zgodność z normami zharmonizowanymi określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1025/2012[54] powinna stanowić dla dostawców sposób wykazania zgodności z wymogami niniejszego rozporządzenia. Komisja może jednak przyjąć wspólne specyfikacje techniczne w obszarach, w których nie istnieją normy zharmonizowane lub w których są one niewystarczające.

(62) Aby zapewnić wysoki poziom wiarygodności systemów sztucznej inteligencji wysokiego ryzyka, takie systemy powinny podlegać ocenie zgodności przed wprowadzeniem ich do obrotu lub oddaniem do użytku.

(63) Aby zminimalizować obciążenie dla operatorów i uniknąć ewentualnego powielania działań, zgodność systemów sztucznej inteligencji wysokiego ryzyka, które wchodzą w zakres obowiązującego unijnego prawodawstwa harmonizacyjnego zgodnie z podejściem opartym na nowych ramach prawnych, z wymogami niniejszego rozporządzenia należy oceniać w ramach oceny zgodności przewidzianej już w tym prawodawstwie. Stosowanie wymogów niniejszego rozporządzenia nie powinno zatem wpływać na szczególną logikę, metodykę lub ogólną strukturę oceny zgodności określone w odpowiednim szczegółowym prawodawstwie opartym na nowych ramach prawnych. Podejście to znajduje pełne odzwierciedlenie w zależnościach między niniejszym rozporządzeniem a [rozporządzeniem w sprawie maszyn]. Chociaż w wymogach niniejszego rozporządzenia uwzględniono zagrożenia dla bezpieczeństwa związane z systemami sztucznej inteligencji zapewniającymi funkcje bezpieczeństwa w maszynach, określone wymogi szczegółowe zawarte w [rozporządzeniu w sprawie maszyn] zapewnią bezpieczną integrację systemu sztucznej inteligencji z całą maszyną w sposób, który nie zagraża bezpieczeństwu maszyny jako całości. W [rozporządzeniu w sprawie maszyn] zawarto tę samą definicję systemu sztucznej inteligencji co w niniejszym rozporządzeniu.

(64) Biorąc pod uwagę większe doświadczenie zawodowych podmiotów, które zajmują się certyfikacją przed wprowadzeniem do obrotu w dziedzinie bezpieczeństwa produktów, oraz odmienny charakter odnośnego ryzyka, zakres stosowania oceny zgodności przeprowadzanej przez osobę trzecią należy ograniczyć, przynajmniej na początkowym etapie stosowania niniejszego rozporządzenia, w przypadku systemów sztucznej inteligencji wysokiego ryzyka innych niż systemy powiązane z produktami. Dlatego też ocenę zgodności takich systemów powinien zasadniczo przeprowadzać dostawca na swoją własną odpowiedzialność, przy czym jedynym wyjątkiem są systemy sztucznej inteligencji przeznaczone do zdalnej identyfikacji biometrycznej osób, w przypadku których to systemów w ocenie zgodności należy przewidzieć zaangażowanie jednostki notyfikowanej w zakresie, w jakim nie jest to zabronione.

(65) Do celów oceny zgodności systemów sztucznej inteligencji przeznaczonych do zdalnej identyfikacji biometrycznej osób przeprowadzanej przez osobę trzecią właściwe organy krajowe powinny wyznaczyć na podstawie niniejszego rozporządzenia

---

[54] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

jednostki notyfikowane, pod warunkiem że spełniają one szereg wymogów, w szczególności dotyczących niezależności, kompetencji i braku konfliktu interesów.

(66) Zgodnie z powszechnie przyjętym pojęciem istotnej zmiany w odniesieniu do produktów objętych unijnym prawodawstwem harmonizacyjnym system sztucznej inteligencji należy poddawać nowej ocenie zgodności w przypadku każdej zmiany, która może mieć wpływ na zgodność systemu z niniejszym rozporządzeniem, lub w przypadku zmiany przeznaczenia systemu. Ponadto w przypadku systemów sztucznej inteligencji, które nadal „uczą się" po wprowadzeniu ich do obrotu lub po oddaniu ich do użytku (tj. automatycznie dostosowują sposób, w jaki wykonują swoje funkcje), należy ustanowić przepisy, zgodnie z którymi zmiany algorytmu i jego funkcjonowania, które zostały z góry zaplanowane przez dostawcę i które oceniono w chwili przeprowadzania oceny zgodności, nie powinny być uznawane za istotne zmiany.

(67) Systemy sztucznej inteligencji wysokiego ryzyka powinny posiadać oznakowanie CE świadczące o ich zgodności z niniejszym rozporządzeniem, aby umożliwić ich swobodny przepływ na rynku wewnętrznym. Państwa członkowskie nie powinny stwarzać nieuzasadnionych przeszkód dla wprowadzania do obrotu lub oddawania do użytku systemów sztucznej inteligencji wysokiego ryzyka zgodnych z wymogami określonymi w niniejszym rozporządzeniu i posiadających oznakowanie CE.

(68) W pewnych warunkach szybka dostępność innowacyjnych technologii może być kluczowa dla zdrowia i bezpieczeństwa osób oraz dla całego społeczeństwa. Jest zatem właściwe, aby w przypadku wystąpienia nadzwyczajnych względów dotyczących bezpieczeństwa publicznego lub ochrony zdrowia i życia osób fizycznych oraz ochrony własności przemysłowej i handlowej państwa członkowskie mogły zezwolić na wprowadzenie do obrotu lub oddanie do użytku systemów sztucznej inteligencji, których nie poddano ocenie zgodności.

(69) Aby ułatwić pracę Komisji i państw członkowskich w dziedzinie sztucznej inteligencji, jak również zwiększyć przejrzystość wobec ogółu społeczeństwa, dostawców systemów sztucznej inteligencji wysokiego ryzyka innych niż systemy powiązane z produktami objętymi zakresem odpowiedniego istniejącego unijnego prawodawstwa harmonizacyjnego należy zobowiązać do rejestracji swoich systemów sztucznej inteligencji wysokiego ryzyka w unijnej bazie danych, którą utworzy i którą zarządzać będzie Komisja. Komisja powinna być administratorem tej bazy danych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725[55]. W celu zapewnienia pełnej funkcjonalności tej bazy danych po jej wdrożeniu procedura ustanawiania bazy danych powinna obejmować opracowanie przez Komisję specyfikacji funkcjonalnych oraz sprawozdanie z niezależnego audytu.

(70) Niektóre systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi lub tworzenia treści mogą stwarzać szczególne ryzyko podawania się za inną osobę lub świadomego wprowadzania w błąd, niezależnie od tego, czy kwalifikują się jako systemy wysokiego ryzyka, czy też nie. W pewnych okolicznościach korzystanie z tych systemów powinno zatem podlegać szczególnym obowiązkom w zakresie przejrzystości bez uszczerbku dla wymogów i obowiązków

[55] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

określonych dla systemów sztucznej inteligencji wysokiego ryzyka. Osoby fizyczne powinno się w szczególności informować, że prowadzą interakcję z systemem sztucznej inteligencji, chyba że okoliczności i kontekst korzystania z systemu jednoznacznie na to wskazują. Osoby fizyczne należy ponadto informować, gdy mają kontakt z systemem rozpoznawania emocji lub systemem kategoryzacji biometrycznej. Tego rodzaju informacje i powiadomienia należy przekazywać w formatach dostępnych dla osób z niepełnosprawnościami. Ponadto użytkownicy, którzy wykorzystują system sztucznej inteligencji do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi w sposób sprawiający, że zaczynają one łudząco przypominać istniejące osoby, miejsca lub zdarzenia, przez co dana osoba mogłaby niesłusznie uznać je za autentyczne, powinny ujawnić, że dane treści zostały sztucznie stworzone lub zmanipulowane poprzez odpowiednie oznakowanie wyniku działania sztucznej inteligencji i ujawnienie, że źródłem danych treści jest system sztucznej inteligencji.

(71) Sztuczna inteligencja jest szybko rozwijającą się grupą technologii, wymagającą nowatorskich form nadzoru regulacyjnego oraz bezpiecznej przestrzeni do eksperymentów, przy jednoczesnym zapewnieniu odpowiedzialnej innowacji oraz uwzględnieniu odpowiednich zabezpieczeń i środków zmniejszających ryzyko. Aby zapewnić ramy prawne przyjazne innowacjom, nieulegające dezaktualizacji i odporne na zakłócenia, należy zachęcić właściwe organy krajowe z co najmniej jednego państwa członkowskiego do ustanowienia piaskownic regulacyjnych w zakresie sztucznej inteligencji, aby ułatwić rozwijanie i testowanie innowacyjnych systemów sztucznej inteligencji pod ścisłym nadzorem regulacyjnym przed ich wprowadzeniem do obrotu lub oddaniem do użytku w inny sposób.

(72) Piaskownice regulacyjne powinny mieć na celu: wspieranie innowacji w zakresie sztucznej inteligencji poprzez ustanowienie kontrolowanego środowiska do eksperymentów i testów na etapie rozwoju i przed wprowadzeniem do obrotu, z myślą o zapewnieniu zgodności innowacyjnych systemów sztucznej inteligencji z niniejszym rozporządzeniem oraz z innymi odnośnymi przepisami Unii i państw członkowskich; zwiększenie pewności prawa dla innowatorów, a także usprawnienie nadzoru ze strony właściwych organów oraz podnoszenie poziomu ich wiedzy na temat możliwości, pojawiających się rodzajów ryzyka oraz skutków związanych z wykorzystywaniem sztucznej inteligencji, a także przyspieszenie dostępu do rynków, w tym poprzez usuwanie barier dla małych i średnich przedsiębiorstw (MŚP) i przedsiębiorstw typu start-up. Aby zapewnić wdrożenie w całej Unii oraz korzyści skali, należy ustanowić wspólne przepisy regulujące uruchamianie piaskownic regulacyjnych oraz ramy współpracy między odpowiednimi organami uczestniczącymi w nadzorze nad piaskownicami regulacyjnymi. Niniejsze rozporządzenie powinno zapewnić podstawę prawną do wykorzystywania danych osobowych zebranych w innych celach do opracowywania, w ramach piaskownicy regulacyjnej w zakresie sztucznej inteligencji, określonych systemów sztucznej inteligencji w interesie publicznym zgodnie z art. 6 ust. 4 rozporządzenia (UE) 2016/679 i art. 6 rozporządzenia (UE) 2018/1725 i nie naruszając przepisów art. 4 ust. 2 dyrektywy (UE) 2016/680. Uczestnicy korzystający z piaskownicy regulacyjnej powinni zapewnić odpowiednie zabezpieczenia i współpracować z właściwymi organami, w tym przestrzegać wytycznych tych organów, a także podejmować w dobrej wierze bezzwłoczne działania w celu ograniczenia wszelkiego rodzaju wysokiego ryzyka dla bezpieczeństwa i praw podstawowych, jakie może powstać w trakcie opracowywania produktów oraz prowadzenia eksperymentów w ramach piaskownicy regulacyjnej. Przy podejmowaniu przez właściwe organy decyzji o ewentualnym nałożeniu

administracyjnej kary pieniężnej na podstawie art. 83 ust. 2 rozporządzenia 2016/679 oraz art. 57 dyrektywy 2016/680 należy uwzględnić postępowanie uczestników korzystających z piaskownicy regulacyjnej.

(73) W celu promowania i ochrony innowacji ważne jest szczególne uwzględnienie interesów drobnych dostawców i użytkowników systemów sztucznej inteligencji. W tym celu państwa członkowskie powinny opracować inicjatywy skierowane do tych operatorów, w tym inicjatywy służące podnoszeniu świadomości i przekazywaniu informacji. Ponadto przy ustalaniu przez jednostki notyfikowane wysokości opłat z tytułu oceny zgodności należy uwzględnić szczególne interesy i potrzeby drobnych dostawców. Koszty tłumaczeń związane z prowadzeniem obowiązkowej dokumentacji i komunikacji z organami mogą stanowić istotny koszt dla dostawców i innych operatorów, zwłaszcza tych działających na mniejszą skalę. Państwa członkowskie powinny w miarę możliwości zapewnić, aby jednym z języków wskazanych i zaakceptowanych przez nie do celów dokumentacji sporządzanej przez odpowiednich dostawców oraz komunikacji z operatorami był język powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych.

(74) Aby zminimalizować zagrożenia dla wdrożenia wynikające z braku wiedzy o rynku i jego znajomości, a także aby ułatwić dostawcom i jednostkom notyfikowanym wykonywanie obowiązków ustanowionych w niniejszym rozporządzeniu, platforma „Sztuczna inteligencja na żądanie", europejskie ośrodki innowacji cyfrowych oraz ośrodki testowo-doświadczalne ustanowione przez Komisję i państwa członkowskie na szczeblu krajowym lub unijnym powinny w miarę możliwości przyczynić się do wdrożenia niniejszego rozporządzenia. W ramach przypisanych zadań i obszarów kompetencji mogą one w szczególności zapewniać wsparcie techniczne i naukowe dostawcom oraz jednostkom notyfikowanym.

(75) Komisja powinna w miarę możliwości ułatwiać dostęp do ośrodków testowo-doświadczalnych podmiotom, grupom lub laboratoriom ustanowionym lub akredytowanym na podstawie odpowiedniego unijnego prawodawstwa harmonizacyjnego, wykonującym zadania w kontekście oceny zgodności produktów lub wyrobów objętych tym unijnym prawodawstwem harmonizacyjnym. Dotyczy to w szczególności paneli ekspertów, laboratoriów eksperckich oraz laboratoriów referencyjnych w dziedzinie wyrobów medycznych w rozumieniu rozporządzenia (UE) 2017/745 oraz rozporządzenia (UE) 2017/746.

(76) Aby ułatwić sprawne, skuteczne i zharmonizowane wdrożenie niniejszego rozporządzenia, należy ustanowić Europejską Radę ds. Sztucznej Inteligencji. Rada powinna odpowiadać za szereg zadań doradczych, w tym wydawanie opinii lub zaleceń oraz udzielanie porad lub wskazówek w dziedzinach związanych z wdrażaniem niniejszego rozporządzenia, także w sprawie specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w niniejszym rozporządzeniu, jak również za udzielanie porad i wsparcia Komisji w konkretnych kwestiach związanych ze sztuczną inteligencją.

(77) Państwa członkowskie odgrywają kluczową rolę w stosowaniu i egzekwowaniu niniejszego rozporządzenia. W tym zakresie każde państwo członkowskie powinno wyznaczyć co najmniej jeden właściwy organ krajowy do celów sprawowania nadzoru nad stosowaniem i wdrażaniem niniejszego rozporządzenia. Aby zwiększyć efektywność organizacyjną po stronie państw członkowskich oraz ustanowić oficjalny punkt kontaktowy dla społeczeństwa oraz innych partnerów na szczeblu państw

członkowskich i na szczeblu unijnym, w każdym państwie członkowskim należy wyznaczyć jeden organ krajowy jako krajowy organ nadzorczy.

(78) W celu zapewnienia, aby dostawcy systemów sztucznej inteligencji wysokiego ryzyka mogli wykorzystywać doświadczenia związane ze stosowaniem systemów sztucznej inteligencji wysokiego ryzyka do ulepszenia swoich systemów oraz procesu projektowania i rozwoju lub byli w stanie odpowiednio szybko podejmować wszelkie możliwe działania naprawcze, każdy dostawca powinien wdrożyć system monitorowania po wprowadzeniu do obrotu. System ten ma również zasadnicze znaczenie dla zapewnienia skuteczniejszego i terminowego przeciwdziałania możliwym zagrożeniom związanym z systemami sztucznej inteligencji, które nadal „uczą się" po wprowadzeniu do obrotu lub oddaniu do użytku. W tym kontekście dostawcy powinni być również zobowiązani do posiadania systemu zgłaszania właściwym organom wszelkich poważnych incydentów lub wszelkich naruszeń prawa krajowego i prawa Unii chroniącego prawa podstawowe, zaistniałych w związku ze stosowaniem ich systemów sztucznej inteligencji.

(79) Aby zapewnić odpowiednie i skuteczne egzekwowanie wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, które należy do unijnego prawodawstwa harmonizacyjnego, system nadzoru rynku i zgodności produktów ustanowiony rozporządzeniem (UE) 2019/1020 powinien mieć zastosowanie w całości. Jeżeli jest to niezbędne do wykonywania ich uprawnień, krajowe organy publiczne lub podmioty prawa publicznego, które nadzorują stosowanie prawa Unii chroniącego prawa podstawowe, w tym organy ds. równości, powinny również mieć dostęp do wszelkiej dokumentacji sporządzonej na podstawie niniejszego rozporządzenia.

(80) Przepisy Unii dotyczące usług finansowych obejmują zasady i wymogi dotyczące zarządzania wewnętrznego i zarządzania ryzykiem, które mają zastosowanie do objętych regulacją instytucji finansowych podczas świadczenia tych usług, w tym wówczas, gdy korzystają one z systemów sztucznej inteligencji. Aby zapewnić spójne stosowanie i egzekwowanie obowiązków ustanowionych w niniejszym rozporządzeniu oraz odpowiednich zasad i wymogów ustanowionych w przepisach Unii dotyczących usług finansowych, organy odpowiedzialne za nadzór nad przepisami dotyczącymi usług finansowych i ich egzekwowanie, w tym w stosownych przypadkach Europejski Bank Centralny, należy wyznaczyć jako właściwe organy do celów nadzoru nad wdrażaniem niniejszego rozporządzenia, w tym do celów działań związanych z nadzorem rynku, w odniesieniu do systemów sztucznej inteligencji dostarczanych lub wykorzystywanych przez objęte regulacją i nadzorem instytucje finansowe. Aby dodatkowo zwiększyć spójność między niniejszym rozporządzeniem a przepisami mającymi zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE[56], procedurę oceny zgodności oraz niektóre obowiązki proceduralne dostawców związane z zarządzaniem ryzykiem, monitorowaniem po wprowadzeniu do obrotu oraz dokumentowaniem należy również włączyć do istniejących obowiązków i procedur przewidzianych w dyrektywie 2013/36/UE. Aby uniknąć nakładania się przepisów, należy również przewidzieć ograniczone odstępstwa dotyczące systemu zarządzania jakością dostawców oraz obowiązku monitorowania nałożonego na użytkowników systemów

[56] Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim mają one zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy 2013/36/UE.

(81) Opracowywanie systemów sztucznej inteligencji innych niż systemy sztucznej inteligencji wysokiego ryzyka z uwzględnieniem wymogów niniejszego rozporządzenia może doprowadzić do szerszego upowszechnienia wiarygodnej sztucznej inteligencji w Unii. Dostawców systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem należy zachęcać do opracowywania kodeksów postępowania mających na celu wspieranie dobrowolnego stosowania obowiązkowych wymogów mających zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka. Dostawców należy również zachęcać do dobrowolnego stosowania dodatkowych wymogów związanych na przykład ze zrównoważeniem środowiskowym, z dostępnością dla osób z niepełnosprawnościami, udziałem zainteresowanych stron w projektowaniu i rozwoju systemów sztucznej inteligencji oraz różnorodnością zespołów programistycznych. Komisja może opracowywać inicjatywy, w tym o charakterze sektorowym, aby ułatwiać zmniejszenie barier technicznych utrudniających transgraniczną wymianę danych na potrzeby rozwoju sztucznej inteligencji, w tym w zakresie infrastruktury dostępu do danych oraz interoperacyjności semantycznej i technicznej różnych rodzajów danych.

(82) Istotne jest, aby systemy sztucznej inteligencji związane z produktami, które nie są systemami wysokiego ryzyka w rozumieniu niniejszego rozporządzenia, a zatem nie muszą spełniać ustanowionych w nim wymogów, były mimo to bezpieczne w chwili wprowadzenia ich do obrotu lub oddawania ich do użytku. Aby przyczynić się do osiągnięcia tego celu, dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady[57] miałaby zastosowanie jako „bezpiecznik".

(83) W celu zapewnienia opartej na zaufaniu i konstruktywnej współpracy właściwych organów na szczeblu unijnym i krajowym wszystkie strony zaangażowane w stosowanie niniejszego rozporządzenia powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań.

(84) Państwa członkowskie powinny wprowadzić wszelkie niezbędne środki, aby zapewnić wdrożenie przepisów niniejszego rozporządzenia, w tym poprzez ustanowienie skutecznych, proporcjonalnych i odstraszających kar za ich naruszenie. W przypadku niektórych szczególnych naruszeń państwa członkowskie powinny uwzględnić marginesy i kryteria określone w niniejszym rozporządzeniu. Europejski Inspektor Ochrony Danych powinien mieć uprawnienia do nakładania grzywien na instytucje, organy i jednostki organizacyjne Unii objęte zakresem stosowania niniejszego rozporządzenia.

(85) Aby zapewnić możliwość dostosowania w razie potrzeby ram regulacyjnych, należy powierzyć Komisji uprawnienia do przyjmowania aktów na podstawie art. 290 TFUE w celu zmiany technik i podejść, o których mowa w załączniku I, do definiowania systemów sztucznej inteligencji, zmiany unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II, systemów sztucznej inteligencji wysokiego ryzyka wymienionych w załączniku III, przepisów dotyczących dokumentacji technicznej wymienionych w załączniku IV, treści deklaracji zgodności UE zawartej w załączniku V, przepisów dotyczących procedur oceny zgodności zawartych w załącznikach VI i VII oraz przepisów określających systemy sztucznej inteligencji wysokiego ryzyka, do

[57] Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.U. L 11 z 15.1.2002, s. 4).

których powinna mieć zastosowanie procedura oceny zgodności oparta na ocenie systemu zarządzania jakością oraz ocenie dokumentacji technicznej. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[58]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(86) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[59].

(87) Ponieważ cel niniejszego rozporządzenia nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary lub skutki działań możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(88) Niniejsze rozporządzenie powinno mieć zastosowanie od dnia … [*Urząd Publikacji – proszę wstawić datę wskazaną w art. 85*]. Infrastruktura związana z zarządzaniem i systemem oceny zgodności powinna być jednak gotowa do działania przed tą datą, w związku z czym przepisy dotyczące jednostek notyfikowanych oraz struktury zarządzania powinny mieć zastosowanie od dnia … [*Urząd Publikacji – proszę wstawić datę – trzy miesiące od daty wejścia w życie niniejszego rozporządzenia*]. Ponadto państwa członkowskie powinny ustanowić i zgłosić Komisji przepisy dotyczące kar, w tym administracyjnych kar pieniężnych, oraz zapewnić ich właściwe i skuteczne wdrożenie przed datą rozpoczęcia stosowania niniejszego rozporządzenia. Przepisy dotyczące kar powinny mieć zatem zastosowanie od dnia … [*Urząd Publikacji – proszę wstawić datę – dwanaście miesięcy od daty wejścia w życie niniejszego rozporządzenia*].

(89) Zgodnie z art. 42 ust. 2 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych i z Europejską Radą Ochrony Danych, które zakończyły się wydaniem opinii w dniu […] r.,

---

[58] Dz.U. L 123 z 12.5.2016, s. 1.

[59] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

TYTUŁ I

PRZEPISY OGÓLNE

Artykuł 1
Przedmiot

W niniejszym rozporządzeniu ustanawia się:

a) zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w Unii;

b) zakazy dotyczące określonych praktyk w zakresie sztucznej inteligencji;

c) szczególne wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka oraz obowiązki spoczywające na podmiotach będących operatorami takich systemów;

d) zharmonizowane przepisy dotyczące przejrzystości w przypadku systemów sztucznej inteligencji przeznaczonych do wchodzenia w interakcję z osobami fizycznymi, systemów rozpoznawania emocji oraz systemów kategoryzacji biometrycznej, a także systemów sztucznej inteligencji wykorzystywanych do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi;

e) przepisy dotyczące monitorowania po wprowadzeniu do obrotu i nadzoru rynku.

Artykuł 2
Zakres

1. Niniejsze rozporządzenie ma zastosowanie do:

a) dostawców wprowadzających do obrotu lub oddających do użytku systemy sztucznej inteligencji w Unii, niezależnie od tego, czy dostawcy ci mają siedzibę w Unii czy w państwie trzecim;

b) użytkowników systemów sztucznej inteligencji, którzy znajdują się w Unii;

c) dostawców i użytkowników systemów sztucznej inteligencji, którzy znajdują się w państwie trzecim, jeżeli wyniki działania systemu są wykorzystywane w Unii.

2. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, które stanowią związane z bezpieczeństwem elementy produktów lub systemów objętych zakresem stosowania poniższych aktów lub które same są takimi produktami lub systemami, zastosowanie ma wyłącznie art. 84 niniejszego rozporządzenia:

a) rozporządzenie (WE) 300/2008;

b) rozporządzenie (UE) nr 167/2013;

c) rozporządzenie (UE) nr 168/2013;

d) dyrektywa 2014/90/UE;

e) dyrektywa (UE) 2016/797;

f) rozporządzenie (UE) 2018/858;

g) rozporządzenie (UE) 2018/1139;

h) rozporządzenie (UE) 2019/2144.

3. Niniejsze rozporządzenie nie ma zastosowania do systemów sztucznej inteligencji opracowanych lub wykorzystywanych wyłącznie do celów wojskowych.

4. Niniejsze rozporządzenie nie ma zastosowania do organów publicznych w państwie trzecim ani do organizacji międzynarodowych objętych zakresem stosowania niniejszego rozporządzenia na podstawie ust. 1, jeżeli te organy lub organizacje wykorzystują systemy sztucznej inteligencji w ramach umów międzynarodowych w sprawie egzekwowania prawa i współpracy sądowej zawartych z Unią lub z jednym państwem członkowskim bądź ich większą liczbą.

5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania przepisów dotyczących odpowiedzialności usługodawców będących pośrednikami ustanowionych w rozdziale II sekcja IV dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady[60] [*które zostaną zastąpione odpowiednimi przepisami aktu prawnego o usługach cyfrowych*].

Artykuł 3
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „system sztucznej inteligencji” oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję;

2) „dostawca” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które opracowują system sztucznej inteligencji lub zlecają jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku pod własną nazwą handlową lub własnym znakiem towarowym – odpłatnie lub nieodpłatnie;

3) „drobny dostawca” oznacza dostawcę będącego mikroprzedsiębiorstwem lub małym przedsiębiorstwem w rozumieniu zalecenia Komisji 2003/361/WE[61];

4) „użytkownik” oznacza osobą fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które korzystają z systemu sztucznej inteligencji pod swoją kontrolą, z wyjątkiem sytuacji, gdy system sztucznej inteligencji jest wykorzystywany w ramach osobistej działalności pozazawodowej;

5) „upoważniony przedstawiciel” oznacza dowolną osobę fizyczną lub prawną mającą siedzibę w Unii, która otrzymała pisemne pełnomocnictwo od dostawcy systemu

[60] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. L 178 z 17.7.2000, s. 1).

[61] Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

sztucznej inteligencji do realizacji w jego imieniu obowiązków i procedur ustanowionych w niniejszym rozporządzeniu;

6) „importer” oznacza dowolną osobę fizyczną lub prawną mającą siedzibę w Unii, która wprowadza do obrotu lub oddaje do użytku system sztucznej inteligencji opatrzony nazwą handlową lub znakiem towarowym osoby fizycznej lub prawnej mającej siedzibę poza granicami Unii;

7) „dystrybutor” oznacza dowolną osobę fizyczną lub prawną w łańcuchu dostaw, inną niż dostawca lub importer, która udostępnia system sztucznej inteligencji na rynku unijnym bez zmiany jego właściwości;

8) „operator” oznacza dostawcę, użytkownika, upoważnionego przedstawiciela, importera i dystrybutora;

9) „wprowadzenie do obrotu” oznacza udostępnienie systemu sztucznej inteligencji na rynku unijnym po raz pierwszy;

10) „udostępnianie na rynku” oznacza wszelkie dostarczanie systemu sztucznej inteligencji w celu jego dystrybucji lub wykorzystania na rynku unijnym w ramach działalności handlowej, odpłatnie lub nieodpłatnie;

11) „oddanie do użytku” oznacza dostarczenie systemu sztucznej inteligencji do pierwszego użycia bezpośrednio użytkownikowi lub do użytku własnego na rynku unijnym zgodnie z jego przeznaczeniem;

12) „przeznaczenie” oznacza zastosowanie, do jakiego system sztucznej inteligencji został przeznaczony przez jego dostawcę, w tym określony kontekst i warunki wykorzystywania, określone w informacjach dostarczonych przez dostawcę w instrukcji obsługi, materiałach promocyjnych lub sprzedażowych i oświadczeniach, jak również w dokumentacji technicznej;

13) „dające się racjonalnie przewidzieć niewłaściwe wykorzystanie” oznacza wykorzystanie systemu sztucznej inteligencji w sposób niezgodny z jego przeznaczeniem, które może wynikać z dającego się racjonalnie przewidzieć zachowania człowieka lub interakcji z innymi systemami;

14) „związany z bezpieczeństwem element produktu lub systemu” oznacza element produktu lub systemu, który spełnia funkcję bezpieczeństwa w przypadku tego produktu lub systemu lub którego awaria bądź nieprawidłowe działanie zagrażają zdrowiu i bezpieczeństwu osób lub mienia;

15) „instrukcja obsługi” oznacza informacje podane przez dostawcę w celu poinformowania użytkownika w szczególności o przeznaczeniu i właściwym użytkowaniu systemu sztucznej inteligencji, w tym informacje o szczególnym kontekście geograficznym, behawioralnym lub funkcjonalnym, w którym ma być wykorzystywany system sztucznej inteligencji wysokiego ryzyka;

16) „wycofanie systemu sztucznej inteligencji od użytkowników” oznacza dowolny środek mający na celu doprowadzenie do zwrotu dostawcy systemu sztucznej inteligencji udostępnionego użytkownikom;

17) „wycofanie systemu sztucznej inteligencji z rynku” oznacza dowolny środek mający na celu zapobieżenie dystrybucji, prezentowaniu i oferowaniu systemu sztucznej inteligencji;

18) „skuteczność działania systemu sztucznej inteligencji” oznacza zdolność systemu sztucznej inteligencji do funkcjonowania zgodnie ze swoim przeznaczeniem;

19) „organ notyfikujący” oznacza organ krajowy, który odpowiada za opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz za ich monitorowanie;

20) „ocena zgodności” oznacza proces weryfikacji, czy spełniono wymogi określone w tytule III rozdział 2 niniejszego rozporządzenia w odniesieniu do systemu sztucznej inteligencji;

21) „jednostka oceniająca zgodność” oznacza jednostkę, która wykonuje czynności z zakresu oceny zgodności przeprowadzanej przez osobę trzecią, w tym badanie, certyfikację i inspekcję;

22) „jednostka notyfikowana” oznacza jednostkę oceniającą zgodność wyznaczoną zgodnie z niniejszym rozporządzeniem i innym stosownym unijnym prawodawstwem harmonizacyjnym;

23) „istotna zmiana” oznacza zmianę w systemie sztucznej inteligencji po jego wprowadzeniu do obrotu lub oddaniu do użytku, która wpływa na zgodność systemu sztucznej inteligencji z wymogami określonymi w tytule III rozdział 2 niniejszego rozporządzenia lub powoduje zmianę przeznaczenia, w odniesieniu do którego oceniono system sztucznej inteligencji;

24) „oznakowanie zgodności CE” (oznakowanie CE) oznacza oznakowanie, za pomocą którego dostawca wskazuje, że system sztucznej inteligencji spełnia wymogi określone w tytule III rozdział 2 niniejszego rozporządzenia i innych mających zastosowanie przepisach Unii harmonizujących warunki wprowadzania produktów do obrotu („unijne prawodawstwo harmonizacyjne”), przewidujących umieszczanie takiego oznakowania;

25) „monitorowanie po wprowadzeniu do obrotu” oznacza wszelkie działania prowadzone przez dostawców systemów sztucznej inteligencji służące gromadzeniu i przeglądowi doświadczeń zdobytych w wyniku użytkowania systemów sztucznej inteligencji, które wprowadzają oni do obrotu lub oddają do użytku, w celu stwierdzenia ewentualnej konieczności natychmiastowego zastosowania niezbędnych działań naprawczych lub zapobiegawczych;

26) „organ nadzoru rynku” oznacza organ krajowy prowadzący działania i stosujący środki zgodnie z rozporządzeniem (UE) 2019/1020;

27) „norma zharmonizowana” oznacza normę europejską określoną w art. 2 pkt 1 lit. c) rozporządzenia (UE) nr 1025/2012;

28) „wspólne specyfikacje” oznaczają dokument inny niż norma, zawierający rozwiązania techniczne zapewniające środki umożliwiające spełnienie niektórych wymogów i obowiązków ustanowionych na podstawie niniejszego rozporządzenia;

29) „dane treningowe” oznaczają dane wykorzystywane do trenowania systemu sztucznej inteligencji poprzez dopasowanie jego parametrów podlegających uczeniu, w tym wag sieci neuronowej;

30) „dane walidacyjne” oznaczają dane służące do oceny trenowanego systemu sztucznej inteligencji oraz do dostrajania jego parametrów niepodlegających uczeniu oraz procesu uczenia, między innymi w celu zapobiegania przetrenowaniu; przy czym zbiór danych walidacyjnych może stanowić oddzielny zbiór danych lub też może stanowić część zbioru danych treningowych, w którym to przypadku udział tego podzbioru w zbiorze danych treningowych może być stały lub zmienny;

31) „dane testowe” oznaczają dane wykorzystywane do przeprowadzenia niezależnej oceny trenowanego i poddanego walidacji systemu sztucznej inteligencji w celu potwierdzenia oczekiwanej skuteczności działania tego systemu przed wprowadzeniem go do obrotu lub oddaniem go do użytku;

32) „dane wejściowe” oznaczają dane dostarczone do systemu sztucznej inteligencji lub bezpośrednio przez niego pozyskane, na podstawie których system ten generuje wynik działania;

33) „dane biometryczne” oznaczają dane osobowe będące wynikiem specjalnego przetwarzania technicznego, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

34) „system rozpoznawania emocji” oznacza system sztucznej inteligencji służący do rozpoznawania lub odgadywania emocji lub zamiarów osób fizycznych na podstawie danych biometrycznych tych osób;

35) „system kategoryzacji biometrycznej” oznacza system sztucznej inteligencji służący do przypisywania osób fizycznych do określonych kategorii, takich jak płeć, wiek, kolor włosów, kolor oczu, tatuaże, pochodzenie etniczne lub orientacja seksualna bądź polityczna, na podstawie ich danych biometrycznych;

36) „system zdalnej identyfikacji biometrycznej” oznacza system sztucznej inteligencji służący do identyfikacji osób fizycznych na odległość poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, bez uprzedniej wiedzy użytkownika systemu sztucznej inteligencji, czy dana osoba będzie w nim figurować i czy może zostać zidentyfikowana;

37) „system zdalnej identyfikacji biometrycznej »w czasie rzeczywistym«” oznacza system zdalnej identyfikacji biometrycznej, w którym zbieranie danych biometrycznych, ich porównywanie i identyfikacja odbywają się bez znacznego opóźnienia. W celu uniknięcia obchodzenia przepisów za taki system uznaje się system, w którym identyfikacja następuje natychmiast, ale również z niewielkim opóźnieniem;

38) „system zdalnej identyfikacji biometrycznej »post factum«” oznacza system zdalnej identyfikacji biometrycznej inny niż system zdalnej identyfikacji biometrycznej „w czasie rzeczywistym”;

39) „przestrzeń publiczna” oznacza każde fizyczne miejsce dostępne publicznie, niezależnie od tego, czy mają zastosowanie określone warunki dostępu;

40) „organ ścigania” oznacza:

a) każdy organ publiczny właściwy w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub egzekwowania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; lub

b) każdy inny organ lub podmiot, któremu na podstawie prawa państwa członkowskiego powierzono sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub egzekwowania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

41) „egzekwowanie prawa” oznacza działania prowadzone przez organy ścigania w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub egzekwowania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

42) „krajowy organ nadzorczy” oznacza organ, któremu państwo członkowskie powierza odpowiedzialność za wdrożenie i stosowanie niniejszego rozporządzenia, za koordynację działań powierzonych danemu państwu członkowskiemu, za działanie w charakterze pojedynczego punktu kontaktowego w kontaktach z Komisją oraz za reprezentowanie państwa członkowskiego w Europejskiej Radzie ds. Sztucznej Inteligencji;

43) „właściwy organ krajowy” oznacza krajowy organ nadzorczy, organ notyfikujący i organ nadzoru rynku;

44) „poważny incydent” oznacza każdy incydent, który bezpośrednio lub pośrednio prowadzi, mógł prowadzić lub może prowadzić do któregokolwiek z poniższych zdarzeń:

a) śmierci osoby lub poważnego uszczerbku na zdrowiu osoby, uszkodzenia mienia lub szkody dla środowiska,

b) poważnego i nieodwracalnego zakłócenia w zarządzaniu infrastrukturą krytyczną i jej funkcjonowaniu.

Artykuł 4
Zmiany w załączniku I

Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73 w celu zmiany wykazu technik i podejść wymienionych w załączniku I, aby uaktualnić ten wykaz z uwzględnieniem rozwoju sytuacji rynkowej i rozwoju technologicznego na podstawie cech, które są podobne do technik i podejść w nim wymienionych.

TYTUŁ II

ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

Artykuł 5

1. Zakazuje się następujących praktyk w zakresie sztucznej inteligencji:

a) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który stosuje techniki podprogowe będące poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną;

b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który wykorzystuje dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;

c) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, kiedy to punktowa ocena społeczna prowadzi do jednego lub obu z następujących skutków:

(i) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zgromadzono dane;

(ii) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;

d) wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:

(i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;

(ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;

(iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW[62] i które w danym państwie członkowskim podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, zgodnie z prawem danego państwa członkowskiego.

2. Na potrzeby wykorzystania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa w odniesieniu do któregokolwiek z celów, o których mowa w ust. 1 lit. d), uwzględnia się następujące elementy:

a) charakter sytuacji powodującej konieczność ewentualnego wykorzystania systemu, w szczególności powagę, prawdopodobieństwo i skalę szkody wyrządzonej w przypadku niewykorzystania systemu;

b) konsekwencje wykorzystania systemu dla praw i wolności wszystkich zainteresowanych osób, w szczególności wagę, prawdopodobieństwo i skalę tych konsekwencji.

---

62 Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).

Ponadto wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa w odniesieniu do któregokolwiek z celów, o których mowa w ust. 1 lit. d), musi przebiegać z zachowaniem niezbędnych i proporcjonalnych zabezpieczeń i warunków w odniesieniu do takiego wykorzystywania, w szczególności w odniesieniu do ograniczeń czasowych, geograficznych i osobowych.

3. Jeżeli chodzi o ust. 1 lit. d) i ust. 2, każde pojedyncze wykorzystanie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa wymaga uzyskania uprzedniego zezwolenia udzielonego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego, w którym ma nastąpić wykorzystanie, wydanego na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego, o których mowa w ust. 4. W należycie uzasadnionych nagłych przypadkach można jednak rozpocząć wykorzystywanie systemu bez zezwolenia, a o zezwolenie można wystąpić dopiero w trakcie lub po zakończeniu wykorzystywania.

   Właściwy organ sądowy lub administracyjny udziela zezwolenia tylko wtedy, gdy jest przekonany, na podstawie obiektywnych dowodów lub jasnych przesłanek, które mu przedstawiono, że wykorzystanie danego systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” jest konieczne i proporcjonalne do osiągnięcia jednego z celów określonych w ust. 1 lit. d), wskazanego we wniosku. Podejmując decyzję w sprawie wniosku, właściwy organ sądowy lub administracyjny bierze pod uwagę elementy, o których mowa w ust. 2.

4. Państwo członkowskie może podjąć decyzję o wprowadzeniu możliwości pełnego lub częściowego zezwolenia na wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa w granicach i na warunkach wymienionych w ust. 1 lit. d), ust. 2 i 3. Dane państwo członkowskie ustanawia w swoim prawie krajowym niezbędne szczegółowe przepisy regulujące wnioski o zezwolenia, o których mowa w ust. 3, wydawanie i wykonywanie tych zezwoleń oraz ich nadzorowanie. W przepisach tych określa się również, w odniesieniu do których celów wymienionych w ust. 1 lit. d), w tym w odniesieniu do których przestępstw, o których mowa w ust. 1 lit. d) ppkt (iii), właściwe organy mogą uzyskać zezwolenie na wykorzystanie powyższych systemów do celów egzekwowania prawa.

TYTUŁ III

SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

ROZDZIAŁ 1

KLASYFIKACJA SYSTEMÓW SZTUCZNEJ INTELIGENCJI JAKO SYSTEMÓW WYSOKIEGO RYZYKA

Artykuł 6

Zasady klasyfikacji systemów sztucznej inteligencji wysokiego ryzyka

1. Bez względu na to, czy system sztucznej inteligencji wprowadza się do obrotu lub oddaje do użytku niezależnie od produktów, o których mowa w lit. a) i b), taki

system sztucznej inteligencji uznaje się za system wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

a) system sztucznej inteligencji jest przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam jest takim produktem;

b) produkt, którego związanym z bezpieczeństwem elementem jest system sztucznej inteligencji, lub sam system sztucznej inteligencji jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II – ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.

2. Oprócz systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w ust. 1, za systemy wysokiego ryzyka uznaje się również systemy sztucznej inteligencji, o których mowa w załączniku III.

Artykuł 7
Zmiany w załączniku III

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73 w celu aktualizacji wykazu zawartego w załączniku III poprzez dodanie systemów sztucznej inteligencji wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

a) systemy sztucznej inteligencji są przeznaczone do wykorzystywania w którymkolwiek z obszarów wymienionych w załączniku III pkt 1–8;

b) systemy sztucznej inteligencji stwarzają ryzyko szkody dla zdrowia i bezpieczeństwa lub ryzyko niekorzystnego wpływu na prawa podstawowe, które pod względem dotkliwości i prawdopodobieństwa wystąpienia jest równoważne ryzyku szkody lub niekorzystnego wpływu, które stwarzają systemy sztucznej inteligencji wysokiego ryzyka wymienione już w załączniku III, lub jest od niego większe.

2. Oceniając do celów ust. 1, czy system sztucznej inteligencji stwarza ryzyko szkody dla zdrowia i bezpieczeństwa lub ryzyko niekorzystnego wpływu na prawa podstawowe, które jest równoważne ryzyku szkody stwarzanemu przez systemy sztucznej inteligencji wysokiego ryzyka wymienione już w załączniku III lub jest od niego większe, Komisja uwzględnia następujące kryteria:

a) przeznaczenie systemu sztucznej inteligencji;

b) zakres, w jakim system sztucznej inteligencji był wykorzystywany lub może być wykorzystywany;

c) zakres, w jakim wykorzystywanie systemu sztucznej inteligencji spowodowało już szkodę dla zdrowia i bezpieczeństwa lub miało niekorzystny wpływ na prawa podstawowe lub wzbudziło istotne obawy co do możliwości wystąpienia takiej szkody lub niekorzystnego wpływu, czego potwierdzeniem są zgłoszenia lub udokumentowane zarzuty przedłożone właściwym organom krajowym;

d) potencjalny zakres takiej szkody lub takiego niekorzystnego wpływu, w szczególności pod względem ich nasilenia i możliwości oddziaływania na wiele osób;

e) zakres, w jakim osoby potencjalnie poszkodowane lub dotknięte niekorzystnym wpływem są zależne od wyniku działania systemu sztucznej inteligencji, w szczególności ze względu na fakt, że z przyczyn praktycznych lub prawnych nie jest możliwe zasadne zrezygnowanie z tego wyniku;

f) zakres, w jakim osoby potencjalnie poszkodowane lub dotknięte niekorzystnym wpływem znajdują się w słabszym położeniu względem użytkownika systemu sztucznej inteligencji, w szczególności z powodu nierównego układu sił, wiedzy, sytuacji gospodarczej lub społecznej lub wieku;

g) zakres, w jakim uzyskany za pomocą systemu sztucznej inteligencji wynik jest łatwo odwracalny, przy czym wyników działania systemu mających wpływ na zdrowie lub bezpieczeństwo osób nie uznaje się za łatwo odwracalne;

h) zakres, w jakim obowiązujące przepisy Unii przewidują:

(i) skuteczne środki dochodzenia roszczeń w związku z zagrożeniami stwarzanymi przez system sztucznej inteligencji, z wyłączeniem roszczeń o odszkodowanie;

(ii) skuteczne środki zapobiegania temu ryzyku lub jego znacznego zminimalizowania.

ROZDZIAŁ 2

WYMOGI DOTYCZĄCE SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

Artykuł 8
Zgodność z wymogami

1. Systemy sztucznej inteligencji wysokiego ryzyka muszą spełniać wymogi ustanowione w niniejszym rozdziale.

2. Przy zapewnianiu zgodności z tymi wymogami uwzględnia się przeznaczenie systemu sztucznej inteligencji wysokiego ryzyka oraz system zarządzania ryzykiem, o którym mowa w art. 9.

Artykuł 9
System zarządzania ryzykiem

1. Ustanawia się, wdraża, dokumentuje i utrzymuje system zarządzania ryzykiem w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka.

2. System zarządzania ryzykiem składa się z ciągłego, iteracyjnego procesu realizowanego przez cały cykl życia systemu sztucznej inteligencji wysokiego ryzyka, wymagającego regularnej, systematycznej aktualizacji. Obejmuje on następujące etapy:

a) identyfikację i analizę znanego i dającego się przewidzieć ryzyka związanego z każdym systemem sztucznej inteligencji wysokiego ryzyka;

b) oszacowanie i ocenę ryzyka, jakie może wystąpić podczas wykorzystywania systemu sztucznej inteligencji wysokiego ryzyka zgodnie z jego

przeznaczeniem i w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania;

c) ocenę innego mogącego wystąpić ryzyka na podstawie analizy danych zebranych z systemu monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 61;

d) przyjęcie odpowiednich środków zarządzania ryzykiem zgodnie z przepisami dalszych ustępów.

3. W ramach środków zarządzania ryzykiem, o których mowa w ust. 2 lit. d), należycie uwzględnia się skutki i możliwe interakcje wynikające z łącznego stosowania wymogów określonych w niniejszym rozdziale 2. Uwzględnia się w nich powszechnie uznawany stan techniki, w tym jego odzwierciedlenie w odpowiednich normach zharmonizowanych lub wspólnych specyfikacjach.

4. Środki zarządzania ryzykiem, o których mowa w ust. 2 lit. d), muszą być takie, aby wszelkie ryzyko szczątkowe związane z każdym zagrożeniem, jak również ogólne ryzyko szczątkowe systemów sztucznej inteligencji wysokiego ryzyka, oceniano jako dopuszczalne, pod warunkiem że system sztucznej inteligencji wysokiego ryzyka wykorzystuje się zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania. Użytkownika informuje się o tym ryzyku szczątkowym.

Przy określaniu najodpowiedniejszych środków zarządzania ryzykiem zapewnia się, co następuje:

a) eliminację lub ograniczenie ryzyka w możliwie największym stopniu poprzez odpowiedni projekt systemu i proces jego opracowywania;

b) w stosownych przypadkach wdrożenie odpowiednich środków służących ograniczeniu i kontroli ryzyka, którego nie można wyeliminować;

c) dostarczenie odpowiednich informacji zgodnie z art. 13, w szczególności w odniesieniu do ryzyka, o którym mowa w ust. 2 lit. b) niniejszego artykułu, oraz, w stosownych przypadkach, przeszkolenie użytkowników.

Przy eliminowaniu lub ograniczaniu ryzyka związanego z wykorzystaniem systemu sztucznej inteligencji wysokiego ryzyka należytą uwagę zwraca się na wiedzę techniczną, doświadczenie, wykształcenie, szkolenia, jakich oczekuje się od użytkownika, oraz środowisko, w którym ma być wykorzystywany system.

5. Systemy sztucznej inteligencji wysokiego ryzyka testuje się w celu określenia najodpowiedniejszych środków zarządzania ryzykiem. Testy muszą służyć zapewnieniu spójnego działania systemów sztucznej inteligencji wysokiego ryzyka zgodnie z ich przeznaczeniem oraz ich zgodności z wymogami określonymi w niniejszym rozdziale.

6. Procedury testowania muszą być odpowiednie do potwierdzenia funkcjonowania systemu sztucznej inteligencji zgodnie z jego przeznaczeniem i nie muszą wykraczać poza to, co jest niezbędne do osiągnięcia tego celu.

7. Testy systemów sztucznej inteligencji wysokiego ryzyka przeprowadza się, w stosownych przypadkach, w dowolnym momencie procesu opracowywania systemu, a w każdym przypadku przed wprowadzeniem go do obrotu lub oddaniem go do użytku. Testy przeprowadza się w odniesieniu do wstępnie określonych

wskaźników i progów probabilistycznych, stosownych do przeznaczenia systemu sztucznej inteligencji wysokiego ryzyka.

8. Podczas wdrażania systemu zarządzania ryzykiem opisanego w ust. 1–7 szczególną uwagę zwraca się na to, czy istnieje prawdopodobieństwo, że dostęp do systemu sztucznej inteligencji wysokiego ryzyka uzyskają dzieci lub że będzie on miał na nie wpływ.

9. W przypadku instytucji kredytowych podlegających przepisom dyrektywy 2013/36/UE aspekty opisane w ust. 1–8 stanowią część procedur służących zarządzaniu ryzykiem ustanowionych przez te instytucje zgodnie z art. 74 tej dyrektywy.

Artykuł 10
Dane i zarządzanie danymi

1. Systemy sztucznej inteligencji wysokiego ryzyka, które wykorzystują techniki obejmujące trenowanie modeli z wykorzystaniem danych, opracowuje się na podstawie zbiorów danych treningowych, walidacyjnych i testowych spełniających kryteria jakości, o których mowa w ust. 2–5.

2. Zbiory danych treningowych, walidacyjnych i testowych podlegają odpowiednim praktykom w zakresie zarządzania danymi. Praktyki te dotyczą w szczególności:

   a) odpowiednich decyzji projektowych;

   b) gromadzenia danych;

   c) odpowiednich operacji przetwarzania na potrzeby przygotowania danych, takich jak anotowanie, etykietowanie, czyszczenie, wzbogacanie i agregacja;

   d) sformułowanie odpowiednich założeń, zwłaszcza w odniesieniu do informacji, do których pomiaru i reprezentowania mają służyć dane;

   e) uprzedniej oceny dostępności, ilości i przydatności zbiorów danych, które są potrzebne;

   f) badania pod kątem ewentualnej tendencyjności;

   g) określenia wszelkich możliwych luk w danych lub braków w danych oraz tego, w jaki sposób można zaradzić tym lukom i brakom.

3. Zbiory danych treningowych, walidacyjnych i testowych muszą być adekwatne, reprezentatywne, wolne od błędów i kompletne. Muszą się one charakteryzować odpowiednimi właściwościami statystycznymi, w tym, w stosownych przypadkach, w odniesieniu do osób lub grup osób, wobec których ma być wykorzystywany system sztucznej inteligencji wysokiego ryzyka. Te kryteria zbiorów danych mogą zostać spełnione na poziomie pojedynczych zbiorów danych lub ich kombinacji.

4. Zbiory danych treningowych, walidacyjnych i testowych muszą uwzględniać, w zakresie wymaganym z uwagi na ich przeznaczenie, cechy lub elementy, które są specyficzne dla określonego kontekstu geograficznego, behawioralnego lub funkcjonalnego lub okoliczności, w których ma być wykorzystywany system sztucznej inteligencji wysokiego ryzyka.

5. W zakresie, w jakim jest to ściśle niezbędne do celów zapewnienia monitorowania, wykrywania i korygowania tendencyjności systemów sztucznej inteligencji wysokiego ryzyka, dostawcy takich systemów mogą przetwarzać szczególne

kategorie danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia (UE) 2016/679, art. 10 dyrektywy (UE) 2016/680 i art. 10 ust. 1 rozporządzenia (UE) 2018/1725, pod warunkiem stosowania odpowiednich zabezpieczeń gwarantujących ochronę podstawowych praw i wolności osób fizycznych, w tym środków technicznych ograniczających ponowne wykorzystanie tych danych i najnowocześniejszych środków służących zapewnieniu bezpieczeństwa i ochrony prywatności, takich jak pseudonimizacja lub – w przypadku gdy anonimizacja może znacząco wpłynąć na możliwość realizacji zakładanego celu – szyfrowanie.

6. Przy opracowywaniu systemów sztucznej inteligencji wysokiego ryzyka innych niż te, które wykorzystują techniki obejmujące trenowanie modeli, stosuje się odpowiednie praktyki w zakresie zarządzania danymi w celu zapewnienia zgodności tych systemów sztucznej inteligencji wysokiego ryzyka z wymogami ust. 2.

Artykuł 11
Dokumentacja techniczna

1. Dokumentację techniczną dla systemu sztucznej inteligencji wysokiego ryzyka sporządza się przed wprowadzeniem danego systemu do obrotu lub oddaniem go do użytku oraz dokonuje się jej aktualizacji.

   Dokumentację techniczną sporządza się w taki sposób, aby wykazać, że system sztucznej inteligencji wysokiego ryzyka spełnia wymogi określone w niniejszym rozdziale, oraz aby dostarczyć właściwym organom krajowym i jednostkom notyfikowanym wszystkich informacji niezbędnych do oceny zgodności systemu sztucznej inteligencji z tymi wymogami. Zawiera ona co najmniej elementy określone w załączniku IV.

2. W przypadku gdy system sztucznej inteligencji wysokiego ryzyka związany z produktem, do którego mają zastosowanie akty prawne wymienione w załączniku II sekcja A, jest wprowadzany do obrotu lub oddawany do użytku, sporządza się jedną dokumentację techniczną zawierającą wszystkie informacje określone w załączniku IV, jak również informacje wymagane na podstawie tych aktów prawnych.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73 w celu zmiany załącznika IV w razie potrzeby, aby zagwarantować, by w świetle postępu technicznego dokumentacja techniczna zawierała wszystkie informacje niezbędne do oceny zgodności systemu z wymogami określonymi w niniejszym rozdziale.

Artykuł 12
Rejestrowanie zdarzeń

1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się tak, aby zawierały funkcję umożliwiającą automatyczne rejestrowanie zdarzeń („rejestry zdarzeń”) podczas działania tych systemów. Ta funkcja rejestracji zdarzeń musi być zgodna z uznanymi normami lub wspólnymi specyfikacjami.

2. Funkcja rejestracji zdarzeń musi zapewniać, w całym cyklu życia systemu sztucznej inteligencji, poziom identyfikowalności jego funkcjonowania odpowiedni do przeznaczenia systemu.

3. W szczególności funkcja rejestracji zdarzeń musi umożliwiać monitorowanie działania systemu sztucznej inteligencji wysokiego ryzyka pod kątem występowania sytuacji, które mogą skutkować tym, że system sztucznej inteligencji będzie stwarzał ryzyko w rozumieniu art. 65 ust. 1, lub które mogą prowadzić do wystąpienia istotnej zmiany, oraz musi ułatwiać monitorowanie po wprowadzeniu do obrotu, o którym mowa w art. 61.

4. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załącznika III pkt 1 lit. a), funkcja rejestracji zdarzeń musi zapewniać ewidencjonowanie co najmniej:

   a) okresu każdego wykorzystania systemu (data i godzina rozpoczęcia oraz data i godzina zakończenia każdego wykorzystania);

   b) referencyjnej bazy danych, względem której system sprawdził dane wejściowe;

   c) danych wejściowych, w których przypadku wyszukiwanie doprowadziło do trafienia;

   d) danych umożliwiających identyfikację osób fizycznych zaangażowanych w weryfikację wyników, o których mowa w art. 14 ust. 5.

Artykuł 13
Przejrzystość i udostępnianie informacji użytkownikom

1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie. Zapewnia się odpowiedni rodzaj i stopień przejrzystości w celu osiągnięcia zgodności z odpowiednimi obowiązkami użytkownika i dostawcy, określonymi w rozdziale 3 niniejszego tytułu.

2. Do systemów sztucznej inteligencji wysokiego ryzyka dołącza się instrukcję obsługi w odpowiednim formacie cyfrowym lub innym formacie zawierającą zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla użytkowników.

3. Informacje, o których mowa w ust. 2, muszą obejmować:

   a) tożsamość i dane kontaktowe dostawcy oraz, w stosownych przypadkach, jego upoważnionego przedstawiciela;

   b) cechy, możliwości i ograniczenia skuteczności działania systemu sztucznej inteligencji wysokiego ryzyka, w tym:

      (i) jego przeznaczenie;

      (ii) poziom dokładności, solidności i cyberbezpieczeństwa, o którym mowa w art. 15, względem którego przetestowano system sztucznej inteligencji wysokiego ryzyka i dokonano jego walidacji oraz którego można oczekiwać, a także wszelkie znane i dające się przewidzieć okoliczności, które mogą mieć wpływ na ten oczekiwany poziom dokładności, solidności i cyberbezpieczeństwa;

      (iii) wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu sztucznej inteligencji wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie

przewidzieć niewłaściwego wykorzystania, które mogą powodować zagrożenia dla zdrowia i bezpieczeństwa lub praw podstawowych;

(iv) skuteczność działania systemu w odniesieniu do osób lub grup osób, względem których system ma być wykorzystywany;

(v) w stosownych przypadkach, specyfikacje dotyczące danych wejściowych lub wszelkie inne istotne informacje dotyczące wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, uwzględniając przeznaczenie systemu sztucznej inteligencji;

c) ewentualne zmiany w systemie sztucznej inteligencji wysokiego ryzyka i jego skuteczności działania, które zostały z góry zaplanowane przez dostawcę w momencie przeprowadzania pierwotnej oceny zgodności;

d) środki nadzoru ze strony człowieka, o których mowa w art. 14, w tym środki techniczne wprowadzone w celu ułatwienia użytkownikom interpretacji wyników działania systemów sztucznej inteligencji;

e) przewidywany cykl życia systemu sztucznej inteligencji wysokiego ryzyka oraz wszelkie niezbędne środki w zakresie konserwacji i utrzymania mające na celu zapewnienie właściwego funkcjonowania tego systemu sztucznej inteligencji, w tym dotyczące aktualizacji oprogramowania.

Artykuł 14
Nadzór ze strony człowieka

1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie wykorzystywania systemu sztucznej inteligencji wysokiego ryzyka mogły je skutecznie nadzorować osoby fizyczne.

2. Nadzór ze strony człowieka ma na celu zapobieganie ryzyku dla zdrowia, bezpieczeństwa lub praw podstawowych lub minimalizowanie takiego ryzyka, które może się pojawić, gdy system sztucznej inteligencji wysokiego ryzyka jest wykorzystywany zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, w szczególności gdy takie ryzyko utrzymuje się pomimo stosowania innych wymogów określonych w niniejszym rozdziale.

3. Nadzór ze strony człowieka zapewnia się za pośrednictwem środka lub środków:

a) określonych i wbudowanych, jeżeli jest to technicznie wykonalne, w system sztucznej inteligencji wysokiego ryzyka przez dostawcę przed wprowadzeniem systemu do obrotu lub oddaniem go do użytku;

b) określonych przez dostawcę przed wprowadzeniem systemu sztucznej inteligencji wysokiego ryzyka do obrotu lub oddaniem go do użytku i które to środki nadają się do wdrożenia przez użytkownika.

4. Osobom, którym powierzono sprawowanie nadzoru ze strony człowieka, środki, o których mowa w ust. 3, muszą umożliwiać, odpowiednio do okoliczności:

a) zrozumienie w pełni możliwości i ograniczeń systemu sztucznej inteligencji wysokiego ryzyka oraz należyte monitorowanie jego działania, tak aby oznaki anomalii, nieprawidłowego funkcjonowania i nieoczekiwanych wyników działania można było wykrywać i zaradzić im tak szybko, jak to możliwe;

b) bycie stale świadomym potencjalnej tendencji do automatycznego polegania lub nadmiernego polegania na wyniku działania systemu sztucznej inteligencji wysokiego ryzyka (tzw. „automation bias”), w szczególności w przypadku systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych do udzielania informacji lub zaleceń na potrzeby decyzji podejmowanych przez osoby fizyczne;

c) prawidłową interpretację wyniku działania systemu sztucznej inteligencji wysokiego ryzyka, biorąc pod uwagę w szczególności cechy systemu oraz dostępne narzędzia i metody interpretacji;

d) podjęcie decyzji, w każdej konkretnej sytuacji, o niekorzystaniu z systemu sztucznej inteligencji wysokiego ryzyka lub w inny sposób zignorowanie, ręczną zmianę lub odwrócenie wyniku działania systemu sztucznej inteligencji wysokiego ryzyka;

e) ingerowanie w działanie systemu sztucznej inteligencji wysokiego ryzyka lub przerwanie działania systemu za pomocą przycisku „stop” lub podobnej procedury.

5. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1 lit. a), środki, o których mowa w ust. 3, muszą ponadto zapewniać, aby użytkownik nie podejmował żadnego działania ani decyzji na podstawie identyfikacji będącej wynikiem działania systemu, jeżeli nie zweryfikowały jej ani nie potwierdziły co najmniej dwie osoby fizyczne.

Artykuł 15
Dokładność, solidność i cyberbezpieczeństwo

1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w taki sposób, aby osiągały, z uwagi na ich przeznaczenie, odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz działały konsekwentnie pod tymi względami w całym cyklu życia.

2. Poziomy dokładności i odpowiednie wskaźniki dokładności systemów sztucznej inteligencji wysokiego ryzyka deklaruje się w dołączonych do nich instrukcjach obsługi.

3. Systemy sztucznej inteligencji wysokiego ryzyka muszą być odporne na błędy, usterki lub niespójności, które mogą wystąpić w systemie lub w środowisku, w którym działa system, w szczególności w wyniku interakcji z osobami fizycznymi lub innymi systemami.

Solidność systemów sztucznej inteligencji wysokiego ryzyka można osiągnąć dzięki rozwiązaniom technicznym gwarantującym redundancję, które mogą obejmować plany zakładające dostępność systemu zapasowego lub plany zapewniające przejście systemu w stan bezpieczny (tzw. „fail-safe”).

Systemy sztucznej inteligencji wysokiego ryzyka, które po wprowadzeniu na rynek lub oddaniu do użytku nadal się uczą, opracowuje się w taki sposób, aby należycie zaradzić – za pomocą odpowiednich środków ograniczających ryzyko – ewentualnym tendencyjnym wynikom działania spowodowanym tym, że wyniki działania wykorzystuje się jako dane wejściowe w przyszłych operacjach („sprzężenie zwrotne”) .

4. Systemy sztucznej inteligencji wysokiego ryzyka muszą być odporne na próby nieupoważnionych osób trzecich mające na celu zmianę ich zastosowania lub skuteczności działania poprzez wykorzystanie słabych punktów systemu.

Rozwiązania techniczne mające na celu zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji wysokiego ryzyka muszą być dostosowane do odpowiednich okoliczności i ryzyka.

Rozwiązania techniczne mające na celu eliminowanie podatności charakterystycznych dla sztucznej inteligencji obejmują, w stosownych przypadkach, środki służące zapobieganiu atakom mającym na celu manipulowanie zbiorem danych treningowych („data poisoning"), danym wejściowym, które mają na celu spowodowanie błędu w modelu („niepożądane przykłady"), lub wadom modelu, a także środki służące weryfikacji działania systemu pod kątem tych zagrożeń.

ROZDZIAŁ 3

OBOWIĄZKI DOSTAWCÓW I UŻYTKOWNIKÓW SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA ORAZ INNYCH OSÓB

Artykuł 16
Obowiązki dostawców systemów sztucznej inteligencji wysokiego ryzyka

Dostawcy systemów sztucznej inteligencji wysokiego ryzyka:

a) zapewniają zgodność swoich systemów sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu;

b) posiadają system zarządzania jakością zgodny z art. 17;

c) sporządzają dokumentację techniczną systemu sztucznej inteligencji wysokiego ryzyka;

d) przechowują rejestry zdarzeń generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka, jeżeli znajdują się one pod ich kontrolą;

e) zapewniają, aby system sztucznej inteligencji wysokiego ryzyka poddano odpowiedniej procedurze oceny zgodności przed wprowadzeniem go do obrotu lub oddaniem go do użytku;

f) wypełniają obowiązki rejestracyjne, o których mowa w art. 51;

g) podejmują niezbędne działania naprawcze, jeżeli system sztucznej inteligencji wysokiego ryzyka nie spełnia wymogów ustanowionych w rozdziale 2 niniejszego tytułu;

h) informują właściwe organy krajowe państw członkowskich, w których udostępnili lub oddali do użytku system sztucznej inteligencji, oraz, w stosownych przypadkach, jednostkę notyfikowaną o niezgodności z wymogami i o wszelkich podjętych działaniach naprawczych;

i) umieszczają oznakowanie CE w swoich systemach sztucznej inteligencji wysokiego ryzyka na potwierdzenie zgodności z niniejszym rozporządzeniem zgodnie z art. 49;

j) wykazują, na żądanie właściwego organu krajowego, zgodność systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu.

Artykuł 17
Systemy zarządzania jakością

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzają system zarządzania jakością, który zapewnia zgodność z niniejszym rozporządzeniem. System ten dokumentuje się w systematyczny i uporządkowany sposób w formie pisemnych polityk, procedur i instrukcji oraz obejmuje on co najmniej następujące aspekty:

   a) strategię zgodności regulacyjnej, w tym zgodności z procedurami oceny zgodności i procedurami zarządzania zmianami w systemie sztucznej inteligencji wysokiego ryzyka;

   b) techniki, procedury i systematyczne działania, które należy stosować na potrzeby projektowania oraz kontroli i weryfikacji projektu systemu sztucznej inteligencji wysokiego ryzyka;

   c) techniki, procedury i systematyczne działania, które należy stosować na potrzeby opracowywania, kontroli jakości i zapewniania jakości systemu sztucznej inteligencji wysokiego ryzyka;

   d) procedury badania, testowania i walidacji, które należy przeprowadzić przed rozpoczęciem opracowywania systemu sztucznej inteligencji wysokiego ryzyka, w trakcie tego procesu i po jego zakończeniu, oraz częstotliwość, z jaką mają być przeprowadzane;

   e) specyfikacje techniczne, w tym normy, jakie należy stosować, a w przypadku gdy nie stosuje się w pełni odpowiednich norm zharmonizowanych, środki, jakie należy zastosować w celu zapewnienia zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w rozdziale 2 niniejszego tytułu;

   f) systemy i procedury zarządzania danymi, w tym gromadzenia danych, analizy danych, etykietowania danych, przechowywania danych, filtrowania danych, eksploracji danych, agregacji danych, zatrzymywania danych i wszelkich innych operacji dotyczących danych, które przeprowadza się przed wprowadzeniem do obrotu lub oddaniem do użytku systemów sztucznej inteligencji wysokiego ryzyka i do celów wprowadzenia ich do obrotu lub oddania ich do użytku;

   g) system zarządzania ryzykiem, o którym mowa w art. 9;

   h) ustanowienie, wdrożenie i utrzymanie systemu monitorowania po wprowadzeniu do obrotu, zgodnie z art. 61;

   i) procedury związane ze zgłaszaniem poważnych incydentów i nieprawidłowego działania zgodnie z art. 62;

   j) obsługę komunikacji z właściwymi organami krajowymi, właściwymi organami, w tym sektorowymi, zapewniającymi lub wspierającymi dostęp do danych, jednostkami notyfikowanymi, innymi operatorami, klientami lub innymi zainteresowanymi stronami;

   k) systemy i procedury ewidencjonowania wszelkiej istotnej dokumentacji i wszelkich istotnych informacji;

   l) zarządzanie zasobami, w tym środki związane z bezpieczeństwem dostaw;

m) ramy odpowiedzialności służące określeniu obowiązków kierownictwa i pozostałego personelu w odniesieniu do wszystkich aspektów wymienionych w niniejszym ustępie.

2. Wdrożenie aspektów, o których mowa w ust. 1, jest proporcjonalne do wielkości organizacji dostawcy.

3. Jeżeli chodzi o dostawców będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE, obowiązek wprowadzenia systemu zarządzania jakością uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi zasad, procedur i mechanizmów zarządzania wewnętrznego ustanowionymi w art. 74 tej dyrektywy. W tym kontekście uwzględnia się wszelkie normy zharmonizowane, o których mowa w art. 40 niniejszego rozporządzenia.

Artykuł 18
Obowiązek sporządzenia dokumentacji technicznej

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka sporządzają dokumentację techniczną, o której mowa w art. 11, zgodnie z załącznikiem IV.

2. Dostawcy będący instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE prowadzą dokumentację techniczną jako jeden z elementów dokumentacji dotyczącej zasad, procedur i mechanizmów zarządzania wewnętrznego zgodnie z art. 74 tej dyrektywy.

Artykuł 19
Ocena zgodności

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka zapewniają, aby ich systemy poddawano odpowiedniej procedurze oceny zgodności zgodnie z art. 43 przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku. W przypadku wykazania zgodności systemów sztucznej inteligencji z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu w wyniku wspomnianej oceny zgodności dostawcy sporządzają deklarację zgodności UE zgodnie z art. 48 i umieszczają oznakowanie zgodności CE zgodnie z art. 49.

2. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b), wprowadzanych do obrotu lub oddawanych do użytku przez dostawców będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE, ocenę zgodności przeprowadza się w toku procedury, o której mowa w art. 97–101 tej dyrektywy.

Artykuł 20
Automatycznie generowane rejestry zdarzeń

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka przechowują rejestry zdarzeń generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka, o ile tego rodzaju rejestry znajdują się pod ich kontrolą na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa. Rejestry zdarzeń przechowuje się przez okres odpowiedni w świetle przeznaczenia systemu sztucznej inteligencji wysokiego ryzyka i mających zastosowanie zobowiązań prawnych przewidzianych w prawie Unii lub prawie krajowym.

2. Dostawcy będący instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE przechowują rejestry zdarzeń wygenerowane przez ich systemy sztucznej inteligencji wysokiego ryzyka jako jeden z elementów dokumentacji zgodnie z art. 74 tej dyrektywy.

Artykuł 21
Działania naprawcze

Dostawcy systemów sztucznej inteligencji wysokiego ryzyka, którzy uznają lub mają powody, by uznać, że system sztucznej inteligencji wysokiego ryzyka, który wprowadzili do obrotu lub oddali do użytku, nie jest zgodny z niniejszym rozporządzeniem, niezwłocznie podejmują niezbędne działania naprawcze w celu, stosownie do przypadku, zapewnienia zgodności tego systemu, wycofania go z rynku lub wycofania go od użytkowników. Informują oni o tym dystrybutorów danego systemu sztucznej inteligencji wysokiego ryzyka oraz, w stosownych przypadkach, upoważnionego przedstawiciela i importerów.

Artykuł 22
Obowiązek informowania

Jeżeli system sztucznej inteligencji wysokiego ryzyka stwarza ryzyko w rozumieniu art. 65 ust. 1 i ryzyko to jest znane dostawcy danego systemu, dostawca ten niezwłocznie informuje właściwe organy krajowe państw członkowskich, w których udostępnił dany system, oraz, w stosownych przypadkach, jednostkę notyfikowaną, która wydała certyfikat dla danego systemu sztucznej inteligencji wysokiego ryzyka, w szczególności o niezgodności oraz o wszelkich podjętych działaniach naprawczych.

Artykuł 23
Współpraca z właściwymi organami

Dostawcy systemów sztucznej inteligencji wysokiego ryzyka, na żądanie właściwego organu krajowego, przekazują temu organowi wszelkie informacje i dokumenty niezbędne do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, w języku urzędowym Unii wskazanym przez dane państwo członkowskie. Na uzasadniony wniosek właściwego organu krajowego dostawcy zapewniają również temu organowi dostęp do rejestrów zdarzeń generowanych automatycznie przez system sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa.

Artykuł 24
Obowiązki producentów produktu

W przypadku gdy system sztucznej inteligencji wysokiego ryzyka powiązany z produktami, do których zastosowanie mają akty prawne wymienione w załączniku II sekcja A, wprowadza się do obrotu lub oddaje do użytku razem z produktem wytworzonym zgodnie z tymi aktami prawnymi pod nazwą handlową producenta produktu, za zapewnienie zgodności systemu sztucznej inteligencji z niniejszym rozporządzeniem odpowiedzialność ponosi producent produktu, który – w odniesieniu do systemu sztucznej inteligencji – podlega takim samym obowiązkom jak te, które na podstawie niniejszego rozporządzenia nałożono na dostawcę.

Artykuł 25
Upoważnieni przedstawiciele

1. W przypadku braku możliwości zidentyfikowania importera dostawcy mający siedzibę poza terytorium Unii są zobowiązani wyznaczyć – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego siedzibę w Unii przed wprowadzeniem swoich systemów na rynek Unii.

2. Upoważniony przedstawiciel wykonuje zadania powierzone mu na mocy pełnomocnictwa udzielonego przez dostawcę. Pełnomocnictwo uprawnia upoważnionego przedstawiciela do wykonywania następujących zadań:

   a) przechowywania kopii deklaracji zgodności UE i dokumentacji technicznej w celu ich udostępnienia właściwym organom krajowym i organom krajowym, o których mowa w art. 63 ust. 7;

   b) przekazywania właściwemu organowi krajowemu na jego uzasadniony wniosek wszelkich informacji i dokumentów niezbędnych do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, w tym zapewnienie temu organowi dostępu do rejestrów zdarzeń generowanych automatycznie przez system sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod kontrolą dostawcy na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa;

   c) współpraca z właściwymi organami krajowymi na ich uzasadniony wniosek przy wszelkich działaniach podejmowanych przez te organy w odniesieniu do systemu sztucznej inteligencji wysokiego ryzyka.

Artykuł 26
Obowiązki importerów

1. Przed wprowadzeniem systemu sztucznej inteligencji wysokiego ryzyka do obrotu importerzy takiego systemu zapewniają, aby:

   a) dostawca tego systemu sztucznej inteligencji przeprowadził odpowiednią procedurę oceny zgodności;

   b) dostawca sporządził dokumentację techniczną zgodnie z załącznikiem IV;

   c) system opatrzono wymaganym oznakowaniem zgodności oraz dołączono do niego wymaganą dokumentację i instrukcję obsługi.

2. Jeżeli importer uważa lub ma powód, aby uważać, że system sztucznej inteligencji wysokiego ryzyka jest niezgodny z niniejszym rozporządzeniem, nie wprowadza tego systemu do obrotu, dopóki nie zapewniona zostanie zgodność tego systemu z przepisami niniejszego rozporządzenia. Jeżeli system sztucznej inteligencji wysokiego ryzyka stwarza ryzyko w rozumieniu art. 65 ust. 1, importer informuje o tym dostawcę systemu sztucznej inteligencji i organy nadzoru rynku.

3. Importerzy podają swoje imię i nazwisko, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy i adres, pod którym można się z nimi skontaktować, w systemie sztucznej inteligencji wysokiego ryzyka lub – jeżeli nie jest to możliwe – na jego opakowaniu lub, w stosownych przypadkach, w towarzyszącej mu dokumentacji.

4. Importerzy zapewniają, aby – w stosownych przypadkach – w okresie, w którym ponoszą odpowiedzialność za system sztucznej inteligencji wysokiego ryzyka, warunki jego przechowywania lub transportu nie zagrażały jego zgodności z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu.

5. Importerzy przekazują właściwym organom krajowym na ich uzasadniony wniosek wszelkie informacje i dokumenty niezbędne do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu w języku łatwo zrozumiałym dla danego właściwego organu krajowego, w tym zapewniają temu organowi dostęp do rejestrów zdarzeń generowanych automatycznie przez system sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod kontrolą dostawcy na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa. Importerzy współpracują również z tymi organami przy wszelkich działaniach podejmowanych przez właściwy organ krajowy w odniesieniu do tego systemu.

Artykuł 27
Obowiązki dystrybutorów

1. Przed wprowadzeniem systemu sztucznej inteligencji wysokiego ryzyka do obrotu dystrybutorzy upewniają się, że system sztucznej inteligencji wysokiego ryzyka został opatrzony wymaganym oznakowaniem zgodności CE, że załączono do niego wymaganą dokumentację i instrukcję obsługi i że dostawca oraz – w stosownych przypadkach – importer systemu wywiązał się z obowiązków określonych w niniejszym rozporządzeniu.

2. Jeżeli dystrybutor uważa lub ma powód, aby uważać, że system sztucznej inteligencji wysokiego ryzyka jest niezgodny z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, nie wprowadza systemu sztucznej inteligencji wysokiego ryzyka do obrotu, dopóki nie zapewni jego zgodności z tymi wymogami. Ponadto jeżeli system stwarza ryzyko w rozumieniu art. 65 ust. 1, dystrybutor informuje o tym dostawcę lub, w stosownych przypadkach, importera systemu.

3. Dystrybutorzy zapewniają, aby – w stosownych przypadkach – w okresie, w którym ponoszą odpowiedzialność za system sztucznej inteligencji wysokiego ryzyka, warunki jego przechowywania lub transportu nie zagrażały zgodności systemu z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu.

4. Dystrybutor, który uważa lub ma powód, aby uważać, że system sztucznej inteligencji wysokiego ryzyka wprowadzony przez niego do obrotu jest niezgodny z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, podejmuje działania naprawcze konieczne do zapewnienia zgodności tego systemu ze stosownymi wymogami lub do wycofania go z rynku lub wycofania go od użytkowników lub zapewnia podjęcie takich działań naprawczych przez, stosownie do przypadku, dostawcę, importera lub dowolnego właściwego operatora. Jeżeli system sztucznej inteligencji wysokiego ryzyka stwarza ryzyko w rozumieniu art. 65 ust. 1, dystrybutor niezwłocznie informuje o tym fakcie właściwe organy krajowe państwa członkowskiego, w którym udostępnił produkt, przekazując szczegółowe informacje w szczególności na temat przyczyn niezgodności systemu z wymogami i na temat wszelkich podjętych działań naprawczych.

5. Na uzasadniony wniosek właściwego organu krajowego dystrybutorzy systemów sztucznej inteligencji wysokiego ryzyka przekazują temu organowi wszelkie informacje i dokumenty niezbędne do wykazania zgodności systemu wysokiego

ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu. Dystrybutorzy współpracują również z właściwym organem krajowym przy wszelkich działaniach podejmowanych przez ten organ.

Artykuł 28

Obowiązki dystrybutorów, importerów, użytkowników lub innych osób trzecich

1. Dystrybutora, importera, użytkownika lub inną osobę trzecią uznaje się za dostawcę do celów niniejszego rozporządzenia i nakłada się na nich obowiązki równoważne obowiązkom dostawcy określonym w art. 16 w dowolnym z poniższych przypadków:

   a) jeżeli wprowadzają do obrotu lub oddają do użytku system sztucznej inteligencji wysokiego ryzyka opatrzony ich nazwą handlową lub znakiem towarowym;

   b) jeżeli zmieniają przeznaczenie systemu sztucznej inteligencji wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku;

   c) jeżeli wprowadzają istotne zmiany w systemie sztucznej inteligencji wysokiego ryzyka.

2. W przypadku zaistnienia okoliczności, o których mowa w ust. 1 lit. b) lub c), dostawcy, który pierwotnie wprowadził system sztucznej inteligencji wysokiego ryzyka do obrotu lub który oddał ten system do użytku, nie uznaje się już za dostawcę do celów niniejszego rozporządzenia.

Artykuł 29

Obowiązki użytkowników systemów sztucznej inteligencji wysokiego ryzyka

1. Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka użytkują takie systemy zgodnie z dołączoną do nich instrukcją obsługi, z zastrzeżeniem ust. 2 i 5.

2. Obowiązki określone w ust. 1 pozostają bez uszczerbku dla innych obowiązków użytkownika wynikających z prawa Unii lub prawa krajowego oraz dla przysługującej użytkownikowi swobody organizowania jego zasobów własnych i działań w celu wdrożenia wskazanych przez dostawcę środków nadzoru ze strony człowieka.

3. Nie naruszając przepisów ust. 1, w zakresie, w jakim użytkownik sprawuje kontrolę nad danymi wejściowymi, użytkownik zapewnia adekwatność danych wejściowych w odniesieniu do przeznaczenia systemu sztucznej inteligencji wysokiego ryzyka.

4. Użytkownicy monitorują działanie systemu sztucznej inteligencji wysokiego ryzyka w oparciu o instrukcję obsługi. Jeżeli użytkownicy mają powody przypuszczać, że użytkowanie systemu sztucznej inteligencji zgodnie z instrukcją obsługi może doprowadzić do powstania ryzyka w rozumieniu art. 65 ust. 1, informują o tym fakcie dostawcę lub dystrybutora i wstrzymują użytkowanie systemu. Użytkownicy zgłaszają również dostawcy lub dystrybutorowi wszelkie stwierdzone przez siebie poważne incydenty lub wszelkie przypadki nieprawidłowego działania w rozumieniu art. 62 i zaprzestają użytkowania systemu sztucznej inteligencji. Jeżeli użytkownik nie jest w stanie skontaktować się z dostawcą, stosuje się odpowiednio przepisy art. 62.

   W odniesieniu do użytkowników będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE obowiązek w zakresie monitorowania, o którym

mowa w akapicie pierwszym, uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi zasad, procedur i mechanizmów zarządzania wewnętrznego ustanowionymi w art. 74 tej dyrektywy.

5. Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka przechowują rejestry zdarzeń generowane automatycznie przez dany system sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą. Rejestry zdarzeń przechowuje się przez okres odpowiedni w świetle przeznaczenia systemu sztucznej inteligencji wysokiego ryzyka i mających zastosowanie zobowiązań prawnych przewidzianych w prawie Unii lub prawie krajowym.

   Użytkownicy będący instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE przechowują rejestry zdarzeń jako jeden z elementów dokumentacji dotyczącej zasad, procedur i mechanizmów zarządzania wewnętrznego zgodnie z art. 74 tej dyrektywy.

6. Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka korzystają z informacji przekazanych na podstawie art. 13, aby wywiązać się ze spoczywającego na nich obowiązku przeprowadzenia oceny skutków dla ochrony danych zgodnie z, stosownie do przypadku, art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680.

ROZDZIAŁ 4

ORGANY NOTYFIKUJĄCE I JEDNOSTKI NOTYFIKOWANE

Artykuł 30
Organy notyfikujące

1. Każde państwo członkowskie wyznacza lub ustanawia organ notyfikujący odpowiedzialny za opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz za ich monitorowanie.

2. Państwa członkowskie mogą wyznaczyć krajową jednostkę akredytującą, o której mowa w rozporządzeniu (WE) nr 765/2008, jako organ notyfikujący.

3. Organy notyfikujące ustanawia się, organizuje się i zarządza się nimi w taki sposób, aby nie dopuścić do wystąpienia jakichkolwiek przypadków konfliktu interesów z jednostkami oceniającymi zgodność i aby zapewnić obiektywny i bezstronny charakter ich działalności.

4. Działalność organów notyfikujących organizuje się w taki sposób, aby decyzje dotyczące notyfikacji jednostek oceniających zgodność podejmowały kompetentne osoby, które nie brały udziału w procesie oceny tych jednostek.

5. Organy notyfikujące nie mogą oferować ani podejmować żadnych działań realizowanych przez jednostki oceniające zgodność ani świadczyć żadnych usług doradztwa na zasadzie komercyjnej lub konkurencyjnej.

6. Organy notyfikujące zapewniają poufność gromadzonych informacji.

7. Organy notyfikujące muszą dysponować odpowiednią liczbą kompetentnych pracowników, aby należycie wykonywać powierzone im zadania.

8. Organy notyfikujące zapewniają przeprowadzanie ocen zgodności w proporcjonalny sposób pozwalający uniknąć nakładania zbędnych obciążeń na dostawców oraz wykonywanie przez jednostki notyfikowane powierzonych im zadań z należytym uwzględnieniem wielkości przedsiębiorstwa, sektora, w którym prowadzi ono działalność, jego struktury oraz stopnia złożoności danego systemu sztucznej inteligencji.

Artykuł 31
Wniosek jednostki oceniającej zgodność o notyfikację

1. Jednostki oceniające zgodność przekazują wniosek o notyfikację organowi notyfikującemu państwa członkowskiego, w którym znajduje się ich siedziba.

2. Do wniosku o notyfikację załącza się opis czynności z zakresu oceny zgodności, modułu lub modułów oceny zgodności i technologii sztucznej inteligencji, w odniesieniu do których jednostka oceniająca zgodność uważa się za kompetentną, a także wydany przez krajową jednostkę akredytującą certyfikat akredytacji (o ile takowy istnieje) poświadczający, że jednostka oceniająca zgodność spełnia wymogi ustanowione w art. 33. Do wniosku załącza się również wszelkie ważne dokumenty dotyczące obowiązującego wyznaczenia występującej z wnioskiem jednostki notyfikowanej na podstawie wszelkiego innego unijnego prawodawstwa harmonizacyjnego.

3. Jeżeli zainteresowana jednostka oceniająca zgodność nie jest w stanie przedstawić certyfikatu akredytacji, przekazuje organowi notyfikującemu dowody w postaci dokumentów niezbędne do zweryfikowania, potwierdzenia i regularnego monitorowania przestrzegania przez tę jednostkę wymogów ustanowionych w art. 33. W odniesieniu do jednostek notyfikowanych wyznaczonych na podstawie wszelkiego innego unijnego prawodawstwa harmonizacyjnego w stosownych przypadkach dopuszcza się możliwość wykorzystania wszelkich dokumentów i certyfikatów dotyczącego takiego wyznaczenia w charakterze dowodów w toku procedury wyznaczania przeprowadzanej zgodnie z niniejszym rozporządzeniem.

Artykuł 32
Procedura notyfikacyjna

1. Organy notyfikujące mogą notyfikować wyłącznie te jednostki oceniające zgodność, które spełniają wymogi ustanowione w art. 33.

2. Organy notyfikujące dokonują notyfikacji na rzecz Komisji i pozostałych państw członkowskich za pomocą narzędzia do notyfikacji drogą elektroniczną opracowanego i obsługiwanego przez Komisję.

3. Notyfikacja zawiera wyczerpujące, szczegółowe informacje na temat czynności z zakresu oceny zgodności, modułu lub modułów oceny zgodności i odpowiednich technologii sztucznej inteligencji.

4. Zainteresowana jednostka oceniająca zgodność może podejmować działania właściwe dla jednostki notyfikowanej wyłącznie wówczas, gdy ani Komisja, ani pozostałe państwa członkowskie nie wniosą sprzeciwu w terminie miesiąca od daty notyfikacji.

5. Organy notyfikujące powiadamiają Komisję i pozostałe państwa członkowskie o wszelkich późniejszych istotnych zmianach w notyfikacji.

Artykuł 33
Jednostki notyfikowane

1. Jednostki notyfikowane weryfikują zgodność systemu sztucznej inteligencji wysokiego ryzyka zgodnie z procedurami oceny zgodności, o których mowa w art. 43.

2. Jednostki notyfikowane muszą spełniać wymogi organizacyjne, wymogi w zakresie zarządzania jakością oraz wymogi dotyczące zasobów i procesów niezbędne do tego, aby mogły wykonywać powierzone im zadania.

3. Struktura organizacyjna jednostek notyfikowanych, podział obowiązków w tych jednostkach, obowiązująca w nich hierarchia służbowa oraz ich funkcjonowanie muszą gwarantować, że działalność jednostek notyfikowanych oraz wyniki czynności z zakresu oceny zgodności prowadzonych przez te jednostki nie będą budziły żadnych wątpliwości.

4. Jednostki notyfikowane muszą być niezależne od dostawcy systemu sztucznej inteligencji wysokiego ryzyka, wobec którego podejmują czynności z zakresu oceny zgodności. Jednostki notyfikowane muszą być również niezależne od wszelkich innych operatorów mających interes gospodarczy we wprowadzeniu systemu sztucznej inteligencji wysokiego ryzyka będącego przedmiotem oceny do obrotu, a także od wszelkich innych konkurentów dostawcy.

5. Jednostki notyfikowane organizuje się i zarządza się nimi w sposób gwarantujący niezależność, obiektywizm i bezstronność podejmowanych przez nie działań. Jednostki notyfikowane dokumentują i wdrażają strukturę i procedury służące zagwarantowaniu ich bezstronności oraz propagowaniu i stosowaniu zasad bezstronności we wszystkich podejmowanych przez nie działaniach organizacyjnych i kadrowych oraz we wszystkich ich działaniach związanych z oceną.

6. Jednostki notyfikowane dysponują udokumentowanymi procedurami, które zapewniają zachowanie przez ich personel, komitety, jednostki zależne, podwykonawców oraz wszelkie stowarzyszone z nimi jednostki lub pracowników podmiotów zewnętrznych poufności informacji, które znalazły się w ich posiadaniu w toku czynności z zakresu oceny zgodności, chyba że ujawnienie takich informacji jest wymagane na mocy obowiązującego prawa. Personel jednostek notyfikowanych pozostaje związany tajemnicą zawodową w kwestii wszystkich informacji pozyskiwanych w toku wykonywania zadań powierzonych mu zgodnie z niniejszym rozporządzeniem, z wyjątkiem działań podejmowanych w odniesieniu do organów notyfikujących państwa członkowskiego, w którym wykonuje on te zadania.

7. Jednostki notyfikowane dysponują procedurami na potrzeby podejmowania działań z uwzględnieniem rozmiaru przedsiębiorstwa, sektora, w którym prowadzi ono działalność, jego struktury oraz stopnia złożoności danego systemu sztucznej inteligencji.

8. Jednostki notyfikowane zawierają odpowiednie umowy ubezpieczenia od odpowiedzialności cywilnej w odniesieniu do podejmowanych przez siebie czynności z zakresu oceny zgodności, chyba że zainteresowane państwo członkowskie bierze na siebie odpowiedzialność z tego tytułu zgodnie z prawem krajowym lub bezpośrednia odpowiedzialność za ocenę zgodności spoczywa na danym państwie członkowskim.

9. Jednostki notyfikowane posiadają zdolność wykonywania wszystkich zadań powierzonych im na podstawie niniejszego rozporządzenia z zachowaniem

najwyższego poziomu uczciwości zawodowej i wymaganych kompetencji w danej dziedzinie, niezależnie od tego, czy zadania te są wykonywane przez nie samodzielnie, czy też w ich imieniu i na ich odpowiedzialność.

10. Jednostki notyfikowane dysponują wystarczającymi kompetencjami wewnętrznymi, aby należycie oceniać zadania wykonywane w ich imieniu przez podmioty zewnętrzne. W tym celu jednostka notyfikowana zawsze zapewnia stałą dostępność odpowiedniej liczby pracowników administracyjnych, technicznych i naukowych dysponujących doświadczeniem i wiedzą w zakresie stosowania odpowiednich technologii sztucznej inteligencji, danych i metod przetwarzania danych oraz w zakresie wymogów ustanowionych w rozdziale 2 niniejszego tytułu, w odniesieniu do każdej procedury oceny zgodności i każdego rodzaju systemu sztucznej inteligencji wysokiego ryzyka, na potrzeby których ich wyznaczono.

11. Jednostki notyfikowane biorą udział w działaniach koordynacyjnych, o których mowa w art. 38. Angażują się także w działalność europejskich organizacji normalizacyjnych bezpośrednio lub za pośrednictwem swoich przedstawicieli lub dopilnowują, by posiadały znajomość odpowiednich norm i dysponowały zawsze aktualną wiedzą na ich temat.

12. Na żądanie organu notyfikującego, o którym mowa w art. 30, jednostki notyfikowane udostępniają i przekazują mu wszystkie stosowne dokumenty, uwzględniając dokumentację dostawców, aby zapewnić temu organowi możliwość podejmowania działań w zakresie oceny, wyznaczania, notyfikacji, monitorowania i nadzoru oraz aby ułatwić mu przeprowadzenie oceny opisanej w niniejszym rozdziale.

Artykuł 34

Jednostki zależne i podwykonawcy jednostek notyfikowanych

1. Jeżeli jednostka notyfikowana zleca wykonywanie określonych zadań związanych z oceną zgodności podwykonawcy lub korzysta w tym celu z usług jednostki zależnej, zapewnia spełnienie przez podwykonawcę lub przez jednostkę zależną wymogów ustanowionych w art. 33 oraz informuje o tym organ notyfikujący.

2. Jednostki notyfikowane ponoszą pełną odpowiedzialność za zadania wykonywane przez podwykonawców lub jednostki zależne bez względu na ich siedzibę.

3. Zadania mogą być zlecane podwykonawcy lub wykonywane przez jednostkę zależną wyłącznie za zgodą dostawcy.

4. Jednostki notyfikowane przechowują odpowiednie dokumenty dotyczące oceny kwalifikacji podwykonawcy lub jednostki zależnej oraz zadań wykonywanych przez te podmioty zgodnie z niniejszym rozporządzeniem w celu ich udostępnienia organowi notyfikującemu.

Artykuł 35

Numery identyfikacyjne i wykazy jednostek notyfikowanych wyznaczonych zgodnie z niniejszym rozporządzeniem

1. Komisja nadaje jednostkom notyfikowanym numer identyfikacyjny. Każdej jednostce nadaje się jeden tego rodzaju numer, nawet jeżeli notyfikowano ją na podstawie kilku aktów Unii.

2. Komisja podaje do wiadomości publicznej wykaz jednostek notyfikowanych na podstawie niniejszego rozporządzenia zawierający nadane im numery identyfikacyjne oraz działania, w związku z którymi zostały one notyfikowane. Komisja zapewnia aktualność tego wykazu.

Artykuł 36
Zmiany w notyfikacjach

1. W przypadku gdy organ notyfikujący podejrzewa lub otrzyma informację, że jednostka notyfikowana przestała spełniać wymogi określone w art. 33 lub nie wypełnia swoich obowiązków, organ ten niezwłocznie wszczyna postępowanie wyjaśniające w tej sprawie z zachowaniem największej staranności. W takim przypadku organ notyfikujący informuje daną jednostkę notyfikowaną o zgłoszonych zastrzeżeniach i zapewnia jej możliwość ustosunkowania się do tych zastrzeżeń. Jeżeli organ notyfikujący dojdzie do wniosku, że jednostka notyfikowana będąca przedmiotem postępowania wyjaśniającego przestała spełniać wymogi określone w art. 33 lub nie wypełnia swoich obowiązków, organ ten, stosownie do przypadku, ogranicza, zawiesza lub cofa notyfikację, w zależności od wagi uchybienia. Organ notyfikujący niezwłocznie informuje również o tym fakcie Komisję i pozostałe państwa członkowskie.

2. W przypadku ograniczenia, zawieszenia lub cofnięcia notyfikacji albo w przypadku zaprzestania działalności przez jednostkę notyfikowaną organ notyfikujący podejmuje odpowiednie kroki w celu zapewnienia, aby dokumentacja tej jednostki została przejęta przez inną jednostkę notyfikowaną albo pozostawała dostępna na żądanie odpowiedzialnych organów notyfikujących.

Artykuł 37
Kwestionowanie kompetencji jednostek notyfikowanych

1. W stosownych przypadkach Komisja bada wszystkie sytuacje, w których stwierdzi wystąpienie okoliczności dających podstawy do tego, by wątpić, że jednostka notyfikowana spełnia wymogi ustanowione w art. 33.

2. Organ notyfikujący przekazuje Komisji, na żądanie, wszystkie istotne informacje dotyczące notyfikacji danej jednostki notyfikowanej.

3. Komisja zapewnia poufność wszystkich informacji poufnych uzyskanych w toku postępowań wyjaśniających prowadzonych zgodnie z niniejszym artykułem.

4. W przypadku gdy Komisja stwierdzi, że jednostka notyfikowana nie spełnia lub przestała spełniać wymogi ustanowione w art. 33, przyjmuje uzasadnioną decyzję zobowiązującą notyfikujące państwo członkowskie do wdrożenie koniecznych środków naprawczych, obejmujących, w razie potrzeby, cofnięcie notyfikacji. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 38
Koordynacja jednostek notyfikowanych

1. Komisja zapewnia – w odniesieniu do obszarów objętych niniejszym rozporządzeniem – wprowadzenie i właściwy przebieg odpowiedniej koordynacji i współpracy jednostek notyfikowanych prowadzących działalność w zakresie

procedur oceny zgodności systemów sztucznej inteligencji zgodnie z niniejszym rozporządzeniem – w formie sektorowej grupy jednostek notyfikowanych.

2. Państwa członkowskie zapewniają, aby notyfikowane przez nie jednostki uczestniczyły w pracach tej grupy bezpośrednio lub za pośrednictwem wyznaczonych przedstawicieli.

Artykuł 39
Jednostki oceniające zgodność z państw trzecich

Jednostki oceniające zgodność ustanowione na mocy prawa państwa trzeciego, z którym Unia zawarła umowę, mogą być upoważnione do prowadzenia działalności właściwej dla jednostek notyfikowanych zgodnie z niniejszym rozporządzeniem.

ROZDZIAŁ 5

NORMY, OCENA ZGODNOŚCI, CERTYFIKATY, REJESTRACJA

Artykuł 40
Normy zharmonizowane

Systemy sztucznej inteligencji wysokiego ryzyka spełniające normy zharmonizowane lub części tych norm, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, uznaje się za spełniające wymogi ustanowione w rozdziale 2 niniejszego tytułu w zakresie, w jakim wspomniane normy obejmują te wymogi.

Artykuł 41
Wspólne specyfikacje

1. Jeżeli normy zharmonizowane, o których mowa w art. 40, nie istnieją lub jeżeli Komisja uzna, że odpowiednie normy zharmonizowane są niewystarczające lub że należy odnieść się do określonych zastrzeżeń dotyczących bezpieczeństwa lub poszanowania praw podstawowych, Komisja może – w drodze aktów wykonawczych – przyjąć wspólne specyfikacje w odniesieniu do wymogów ustanowionych w rozdziale 2 niniejszego tytułu. Wspomniane akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

2. Przygotowując wspólne specyfikacje, o których mowa w ust. 1, Komisja zbiera opinie właściwych jednostek lub grup ekspertów ustanowionych zgodnie z odpowiednimi unijnymi przepisami sektorowymi.

3. Systemy sztucznej inteligencji wysokiego ryzyka zgodne ze wspólnymi specyfikacjami, o których mowa w ust. 1, uznaje się za spełniające wymogi ustanowione w rozdziale 2 niniejszego tytułu w zakresie, w jakim wspomniane wspólne specyfikacje obejmują te wymogi.

4. W przypadku niezapewnienia zgodności ze wspólnymi specyfikacjami, o których mowa w ust. 1, dostawcy w należyty sposób wykazują, że przyjęli rozwiązania techniczne, które są co najmniej równoważne tym wspólnym specyfikacjom.

Artykuł 42
Domniemanie zgodności z określonymi wymogami

1. Biorąc pod uwagę ich przeznaczenie, systemy sztucznej inteligencji wysokiego ryzyka, które zostały wytrenowane i przetestowane przy użyciu danych dotyczących określonego środowiska geograficznego, behawioralnego i funkcjonalnego, w którym planuje się z nich korzystać, uznaje się za spełniające wymóg ustanowiony w art. 10 ust. 4.

2. Systemy sztucznej inteligencji wysokiego ryzyka, które uzyskały certyfikację lub w odniesieniu do których wydano deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881[63] i do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, uznaje się za spełniające wymogi w zakresie cyberbezpieczeństwa ustanowione w art. 15 niniejszego rozporządzenia w zakresie, w jakim certyfikat cyberbezpieczeństwa lub deklaracja zgodności, lub ich części obejmują te wymogi.

Artykuł 43
Ocena zgodności

1. W odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka wymienionych w załączniku III pkt 1, w przypadku gdy do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu dostawca zastosował normy zharmonizowane, o których mowa w art. 40, lub, w stosownych przypadkach, wspólne specyfikacje, o których mowa w art. 41, dostawca postępuje zgodnie z jedną z następujących procedur:

   a) procedurą oceny zgodności opierającą się na kontroli wewnętrznej, o której mowa w załączniku VI;

   b) procedurą oceny zgodności opierającą się na ocenie systemu zarządzania jakością i ocenie dokumentacji technicznej przeprowadzaną z udziałem jednostki notyfikowanej, o której to procedurze mowa w załączniku VII.

   Jeżeli przy wykazywaniu zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu dostawca nie zastosował norm zharmonizowanych, o których mowa w art. 40, lub zastosował te normy tylko częściowo lub jeżeli takie normy zharmonizowane nie istnieją, a wspólne specyfikacje, o których mowa w art. 41, nie są dostępne, dostawca postępuje zgodnie z procedurą oceny zgodności określoną w załączniku VII.

   Na potrzeby procedury oceny zgodności, o której mowa w załączniku VII, dostawca może wybrać dowolną jednostkę notyfikowaną. Jeżeli jednak system ma zostać oddany do użytku przez organy ścigania, organy imigracyjne lub organy odpowiedzialne za udzielanie azylu, a także przez instytucje, organy lub jednostki organizacyjne UE, funkcję jednostki notyfikowanej pełni organ nadzoru rynku, o którym mowa w art. 63 ust. 5 lub – w stosownych przypadkach – art. 63 ust. 6.

---

63 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 1).

2. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2–8, dostawcy postępują zgodnie z procedurą oceny zgodności opierająca się na kontroli wewnętrznej, o której mowa w załączniku VI i która nie przewiduje udziału jednostki notyfikowanej. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b), wprowadzanych do obrotu lub oddawanych do użytku przez instytucje kredytowe podlegające przepisom dyrektywy 2013/36/UE, ocenę zgodności przeprowadza się w toku procedury, o której mowa w art. 97–101 tej dyrektywy.

3. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, do których zastosowanie mają akty prawne wymienione w załączniku II sekcja A, dostawca przeprowadza odpowiednią ocenę zgodności wymaganą na podstawie tych aktów prawnych. W odniesieniu do tego rodzaju systemów sztucznej inteligencji wysokiego ryzyka zastosowanie mają wymogi ustanowione w rozdziale 2 niniejszego tytułu i stanowią one jeden z elementów tej oceny. W takim przypadku zastosowanie mają również przepisy załącznika VII pkt 4.3, pkt 4.4, pkt 4.5 i pkt 4.6 akapit piąty.

   Na potrzeby tej oceny jednostki notyfikowane, które notyfikowano zgodnie z tymi aktami prawnymi, są uprawnione do przeprowadzania kontroli zgodności systemów sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, o ile zgodność tych jednostek notyfikowanych z wymogami ustanowionymi w art. 33 ust. 4, 9 i 10 została oceniona w kontekście procedury notyfikacyjnej przewidzianej w tych aktach prawnych.

   Jeżeli akty prawne wymienione w załączniku II sekcja A zapewniają producentowi produktu możliwość zrezygnowania z oceny zgodności przeprowadzanej przez osobę trzecią, o ile zapewnił on zgodność ze wszystkimi normami zharmonizowanymi obejmującymi wszystkie stosowne wymogi, taki producent może skorzystać z tej możliwość wyłącznie w przypadku, gdy zapewnił również zgodność z normami zharmonizowanymi lub – w stosownych przypadkach – wspólnymi specyfikacjami, o których mowa w art. 41, obejmującymi wymogi ustanowione w rozdziale 2 niniejszego tytułu.

4. Systemy sztucznej inteligencji wysokiego ryzyka poddaje się nowej procedurze oceny zgodności za każdym razem, gdy wprowadza się w nich istotne zmiany, niezależnie od tego, czy zmieniony system ma być przedmiotem dalszej dystrybucji, czy też ma być nadal wykorzystywany przez jego obecnego użytkownika.

   W przypadku systemów sztucznej inteligencji wysokiego ryzyka, które nadal uczą się po wprowadzeniu ich do obrotu lub po oddaniu ich do użytku, istotnej zmiany nie stanowią zmiany w systemie sztucznej inteligencji wysokiego ryzyka i jego skuteczności działania, które dostawca z góry zaplanował w chwili przeprowadzania wstępnej oceny zgodności i które są częścią informacji zawartych w dokumentacji technicznej, o której mowa w pkt 2 lit. f) załącznika IV, .

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73, aby zaktualizować załączniki VI i VII w celu wprowadzenia elementów procedur oceny zgodności, które stały się konieczne z uwagi na postęp techniczny.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych, aby zmienić przepisy ust. 1 i 2 w celu objęcia systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2–8, procedurą oceny zgodności, o której mowa w załączniku VII, lub elementami tej procedury. Komisja przyjmuje takie akty

delegowane, biorąc pod uwagę skuteczność procedury oceny zgodności opierającej się na kontroli wewnętrznej, o której mowa w załączniku VI, w zapobieganiu zagrożeniom dla zdrowia i bezpieczeństwa oraz ochrony praw podstawowych stwarzanym przez takie systemy lub minimalizowaniu tych zagrożeń, a także uwzględniając dostępność odpowiednich zdolności i zasobów wśród jednostek notyfikowanych.

Artykuł 44
Certyfikaty

1. Certyfikaty wydawane przez jednostki notyfikowane zgodnie z załącznikiem VII sporządza się w języku urzędowym Unii określonym przez państwo członkowskie, w którym znajduje się siedziba jednostki notyfikowanej, lub języku urzędowym Unii, który jednostka notyfikowana uznaje za odpowiedni z innych względów.

2. Certyfikaty zachowują ważność przez wskazany w nich okres, który nie może przekraczać pięciu lat. Na wniosek dostawcy ważność certyfikatu można przedłużyć na kolejne okresy, które nie mogą każdorazowo przekraczać pięciu lat, w oparciu o wyniki ponownej oceny przeprowadzonej zgodnie z mającymi zastosowanie procedurami oceny zgodności.

3. Jeżeli jednostka notyfikowana stwierdzi, że system sztucznej inteligencji przestał spełniać wymogi ustanowione w rozdziale 2 niniejszego tytułu, zawiesza lub cofa wydany certyfikat lub nakłada na niego ograniczenia, biorąc pod uwagę zasadę proporcjonalności, chyba że dostawca systemu zapewni zgodność z tymi wymogami poprzez podjęcie odpowiedniego działania naprawczego w stosownym terminie wyznaczonym przez jednostkę notyfikowaną. Jednostka notyfikowana uzasadnia swoją decyzję.

Artykuł 45
Odwołanie od decyzji jednostek notyfikowanych

Państwa członkowskie zapewniają stronom posiadającym prawnie uzasadniony interes związany z decyzjami jednostek notyfikowanych możliwość wniesienia odwołania od tych decyzji.

Artykuł 46
Obowiązki jednostek notyfikowanych w zakresie informowania

1. Jednostki notyfikowane informują organ notyfikujący:

   a) o wszelkich unijnych certyfikatach oceny dokumentacji technicznej, wszelkich suplementach do tych certyfikatów i wszelkich decyzjach zatwierdzających system zarządzania jakością wydanych zgodnie z wymogami załącznika VII;

   b) o każdej odmowie wydania, każdym ograniczeniu, zawieszeniu lub cofnięciu unijnego certyfikatu oceny dokumentacji technicznej lub decyzji zatwierdzającej system zarządzania jakością wydanych zgodnie z wymogami załącznika VII;

   c) o wszelkich okolicznościach wpływających na zakres lub warunki notyfikacji;

   d) o każdym przypadku wystąpienia przez organy nadzoru rynku z żądaniem udzielenia informacji o czynnościach z zakresu oceny zgodności;

e) na żądanie, o czynnościach z zakresu oceny zgodności objętych zakresem ich notyfikacji oraz o wszelkiej innej prowadzonej działalności, w tym działalności transgranicznej i podwykonawstwie.

2. Każda jednostka notyfikowana informuje pozostałe jednostki notyfikowane:

a) o decyzjach zatwierdzających system zarządzania jakością, których wydania odmówiła, które zawiesiła lub które cofnęła, oraz – na żądanie – o wydanych przez siebie decyzjach zatwierdzających system zarządzania jakością;

b) o unijnych certyfikatach oceny dokumentacji technicznej lub o wszelkich suplementach do tych certyfikatów, których wydania odmówiła, które cofnęła, które zawiesiła lub na które nałożyła innego rodzaju ograniczenia, oraz – na żądanie – o wydanych przez siebie certyfikatach lub suplementach do certyfikatów.

3. Każda jednostka notyfikowana przekazuje pozostałym jednostkom notyfikowanym prowadzącym podobne czynności z zakresu oceny zgodności w odniesieniu do tych samych technologii sztucznej inteligencji stosowne informacje na temat kwestii związanych z negatywnymi, a także – na ich żądanie – pozytywnymi wynikami oceny zgodności.

Artykuł 47
Odstępstwo od procedury oceny zgodności

1. Na zasadzie odstępstwa od art. 43 każdy organ nadzoru rynku może wydać zezwolenie na wprowadzenie do obrotu lub oddanie do użytku konkretnych systemów sztucznej inteligencji wysokiego ryzyka na terytorium danego państwa członkowskiego w związku z wystąpieniem nadzwyczajnych względów dotyczących bezpieczeństwa publicznego lub ochrony zdrowia i życia osób, ochrony środowiska i ochrony kluczowych aktywów przemysłowych i infrastrukturalnych. Wspomniane zezwolenie wydaje się na ograniczony okres na czas przeprowadzenia niezbędnych procedur oceny zgodności, a jego ważność wygasa po zakończeniu tych procedur. Dokłada się starań, aby procedury te ukończono bez zbędnej zwłoki.

2. Zezwolenie, o którym mowa w ust. 1, wydaje się wyłącznie wówczas, gdy organ nadzoru rynku stwierdzi, że system sztucznej inteligencji wysokiego ryzyka spełnia wymogi ustanowione w rozdziale 2 niniejszego tytułu. Organ nadzoru rynku informuje Komisję i pozostałe państwa członkowskie o wszelkich zezwoleniach wydanych zgodnie z ust. 1.

3. Jeżeli w terminie 15 dni kalendarzowych od dnia otrzymania informacji, o której mowa w ust. 2, ani żadne państwo członkowskie, ani Komisja nie zgłoszą zastrzeżeń dotyczących zezwolenia wydanego przez organ nadzoru rynku państwa członkowskiego zgodnie z ust. 1, takie zezwolenie uznaje się za uzasadnione.

4. Jeżeli w terminie 15 dni kalendarzowych od dnia otrzymania informacji, o której mowa w ust. 2, państwo członkowskie zgłosi zastrzeżenia dotyczące zezwolenia wydanego przez organ nadzoru rynku innego państwa członkowskiego lub jeżeli Komisja uzna zezwolenie za sprzeczne z prawem Unii lub uzna za bezpodstawne dokonane przez państwo członkowskie stwierdzenie zgodność systemu z wymogami, o czym jest mowa w ust. 2, Komisja niezwłocznie przystępuje do konsultacji z odpowiednim państwem członkowskim; w takim przypadku zasięga się opinii zainteresowanych operatorów i zapewnia się im możliwość przedstawienia ich stanowiska. Na tej podstawie Komisja podejmuje decyzję, czy dane zezwolenie jest

uzasadnione, czy też nie. Komisja kieruje swoją decyzję do zainteresowanego państwa członkowskiego i zainteresowanego operatora lub zainteresowanych operatorów.

5. Jeżeli zezwolenie zostanie uznane za bezpodstawne, organ nadzoru rynku zainteresowanego państwa członkowskiego jest zobowiązany je cofnąć.

6. Na zasadzie odstępstwa od ust. 1–5, w przypadku systemów sztucznej inteligencji wysokiego ryzyka, które mają być wykorzystywane w charakterze związanych z bezpieczeństwem elementów wyrobów podlegających przepisom rozporządzenia (UE) 2017/745 i rozporządzenia (UE) 2017/746 lub które same są takimi wyrobami, w odniesieniu do odstępstwa od konieczności przeprowadzenia oceny zgodności z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu stosuje się również art. 59 rozporządzenia (UE) 2017/745 i art. 54 rozporządzenia (UE) 2017/746.

Artykuł 48
Deklaracja zgodności UE

1. Dostawca sporządza pisemną deklarację zgodności UE dla każdego systemu sztucznej inteligencji i przechowuje ją w celu jej udostępnienia właściwym organom krajowym przez okres 10 lat od dnia wprowadzenia systemu sztucznej inteligencji do obrotu lub oddania go do użytku. W deklaracji zgodności UE wskazuje się system sztucznej inteligencji, dla którego ją sporządzono. Kopię deklaracji zgodności UE przekazuje się odpowiednim właściwym organom krajowym na ich żądanie.

2. W deklaracji zgodności UE potwierdza się, że dany system sztucznej inteligencji wysokiego ryzyka spełnia wymogi ustanowione w rozdziale 2 niniejszego tytułu. Deklaracja zgodności UE zawiera informacje przedstawione w załączniku V i musi zostać przetłumaczona na język urzędowy Unii lub na języki wskazane przez państwa członkowskie, w których udostępnia się system sztucznej inteligencji wysokiego ryzyka.

3. Jeżeli systemy sztucznej inteligencji wysokiego ryzyka podlegają innemu unijnemu prawodawstwu harmonizacyjnemu, w którym również ustanowiono wymóg sporządzenia deklaracji zgodności UE, na potrzeby wszystkich aktów prawa Unii mających zastosowanie do systemu sztucznej inteligencji wysokiego ryzyka sporządza się jedną deklarację zgodności UE. W deklaracji zamieszcza się wszystkie informacje niezbędne do zidentyfikowania unijnego prawodawstwa harmonizacyjnego, do którego się ona odnosi.

4. Sporządzając deklarację zgodności UE, dostawca bierze na siebie odpowiedzialność za zgodność z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu. W stosownych przypadkach dostawca zapewnia aktualność deklaracji zgodności UE.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73, aby zaktualizować treść deklaracji zgodności UE określoną w załączniku V w celu wprowadzenia elementów, które stały się konieczne z uwagi na postęp techniczny.

Artykuł 49
Oznakowanie zgodności CE

1. Oznakowanie CE umieszcza się na systemie sztucznej inteligencji wysokiego ryzyka w sposób widoczny, czytelny i trwały. Jeżeli z uwagi na charakter systemu sztucznej inteligencji wysokiego ryzyka oznakowanie systemu w powyższy sposób nie jest

możliwe lub uzasadnione, oznakowanie to umieszcza się na opakowaniu lub – w stosownych przypadkach – w dokumentacji towarzyszącej systemowi.

2. Oznakowanie CE, o którym mowa w ust. 1 niniejszego artykułu, podlega ogólnym zasadom ustanowionym w art. 30 rozporządzenia (WE) nr 765/2008.

3. W stosownych przypadkach oznakowaniu CE towarzyszy również numer identyfikacyjny jednostki notyfikowanej odpowiedzialnej za przeprowadzenie procedur oceny zgodności ustanowionych w art. 43. Numer identyfikacyjny umieszcza się również na wszelkich materiałach promocyjnych zawierających informacje o tym, że system sztucznej inteligencji wysokiego ryzyka spełnia wymogi konieczne do opatrzenia go oznakowaniem CE.

Artykuł 50
Przechowywanie dokumentów

Przez okres 10 lat od dnia wprowadzenia systemu sztucznej inteligencji do obrotu lub oddania go do użytku dostawca przechowuje do dyspozycji właściwych organów krajowych:

a) dokumentację techniczną, o której mowa w art. 11;

b) dokumentację dotyczącą systemu zarządzania jakością, o którym mowa w art. 17;

c) w stosownych przypadkach dokumentację dotyczącą zmian zatwierdzonych przez jednostki notyfikowane;

d) w stosownych przypadkach decyzje i inne dokumenty wydane przez jednostki notyfikowane;

e) deklarację zgodności UE, o której mowa w art. 48.

Artykuł 51
Rejestracja

Przed wprowadzeniem do obrotu systemu sztucznej inteligencji wysokiego ryzyka, o którym mowa w art. 6 ust. 2, lub przed oddaniem go do użytku dostawca lub – w stosownych przypadkach – jego upoważniony przedstawiciel rejestruje ten system w unijnej bazie danych, o której mowa w art. 60.

TYTUŁ IV

OBOWIĄZKI W ZAKRESIE PRZEJRZYSTOŚCI W ODNIESIENIU DO OKREŚLONYCH SYSTEMÓW SZTUCZNEJ INTELIGENCJI

Artykuł 52
Obowiązki w zakresie przejrzystości w odniesieniu do określonych systemów sztucznej inteligencji

1. Dostawcy zapewniają, aby systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi projektowano i opracowywano w taki sposób, aby osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem sztucznej inteligencji, chyba że okoliczności i kontekst korzystania z systemu jednoznacznie na to wskazują. Obowiązek ten nie ma zastosowania do systemów sztucznej inteligencji zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia dochodzeń/śledztw

w związku z przestępstwami i ścigania ich sprawców, chyba że systemy te udostępnia się ogółowi społeczeństwa na potrzeby składania zawiadomień o popełnieniu przestępstwa.

2. Użytkownicy systemów rozpoznawania emocji lub systemów kategoryzacji biometrycznej informują osoby fizyczne, wobec których systemy te są stosowane, o fakcie ich stosowania. Obowiązek ten nie ma zastosowania do systemów sztucznej inteligencji wykorzystywanych do kategoryzacji biometrycznej zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom i prowadzenia dochodzeń/śledztw w związku z przestępstwami.

3. Użytkownicy systemu sztucznej inteligencji, który generuje obrazy, treści dźwiękowe lub treści wideo, które łudząco przypominają istniejące osoby, obiekty, miejsca lub inne podmioty lub zdarzenia, lub który tymi obrazami i treściami manipuluje, przez co osoba będąca ich odbiorcą mogłaby niesłusznie uznać je za autentyczne lub prawdziwe („deepfake”), ujawniają, że dane treści zostały wygenerowane lub zmanipulowane przez system sztucznej inteligencji.

   Przepisy akapitu pierwszego nie mają jednak zastosowania w przypadku, gdy korzystanie z takich rozwiązań zatwierdzono z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia dochodzeń/śledztw w związku z przestępstwami i ścigania ich sprawców lub gdy jest to konieczne do wykonywania prawa do wolności wypowiedzi i prawa do wolności sztuki i nauki zagwarantowanych w Karcie praw podstawowych Unii Europejskiej, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.

4. Przepisy ust. 1, 2 i 3 pozostają bez wpływu na wymogi i obowiązki ustanowione w tytule III niniejszego rozporządzenia.

TYTUŁ V

ŚRODKI WSPIERAJĄCE INNOWACYJNOŚĆ

Artykuł 53
Piaskownice regulacyjne w zakresie AI

1. Piaskownice regulacyjne w zakresie AI tworzone przez jeden właściwy organ państwa członkowskiego lub większą liczbę takich organów, lub przez Europejskiego Inspektora Ochrony Danych zapewniają kontrolowane środowisko ułatwiające opracowywanie, testowanie i walidację innowacyjnych systemów sztucznej inteligencji przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem ich do użytku zgodnie z określonym planem. Tego rodzaju działalność musi przebiegać pod bezpośrednim nadzorem właściwych organów i zgodnie z ich wytycznymi, aby zapewnić zgodność z wymogami niniejszego rozporządzenia oraz – w stosownych przypadkach – z innymi przepisami prawa Unii i prawa państw członkowskich objętymi nadzorem w ramach piaskownicy.

2. Państwa członkowskie zapewniają, aby w zakresie, w jakim innowacyjne systemy sztucznej inteligencji wiążą się z przetwarzaniem danych osobowych lub z innego tytułu wchodzą w zakres kompetencji nadzorczych innych organów krajowych lub właściwych organów zapewniających dostęp do danych lub wsparcie w uzyskaniu dostępu do danych, krajowe organy ochrony danych oraz te inne organy krajowe włączono w działalność piaskownicy regulacyjnej w zakresie AI.

3. Piaskownice regulacyjne w zakresie AI pozostają bez wpływu na uprawnienia właściwych organów w zakresie nadzoru i stosowania środków naprawczych. Wykrycie jakichkolwiek istotnych zagrożeń dla zdrowa i bezpieczeństwa oraz dla praw podstawowych na etapie opracowywania i testowania takich systemów powoduje konieczność natychmiastowego zaradzenia tym zagrożeniom, a w przypadku ich nieusunięcia – skutkuje zawieszeniem procesu opracowywania i testowania systemu, dopóki wspomniane zagrożenia nie zostaną wyeliminowane.

4. Uczestnicy korzystający z piaskownicy regulacyjnej w zakresie AI ponoszą odpowiedzialność, przewidzianą w mających zastosowanie przepisach dotyczących odpowiedzialności przyjętych na szczeblu Unii i na szczeblu państw członkowskich, za wszelkie szkody wyrządzone osobom trzecim w wyniku eksperymentów prowadzonych w piaskownicy.

5. Właściwe organy państw członkowskich, które utworzyły piaskownice regulacyjne w zakresie AI, koordynują swoje działania i prowadzą współpracę w ramach Europejskiej Rady ds. Sztucznej Inteligencji. Wspomniane organy przedkładają Radzie i Komisji sprawozdania roczne dotyczące rezultatów wdrażania tych programów, uwzględniając dobre praktyki, wyciągnięte wnioski, zalecenia dotyczące tworzenia piaskownic regulacyjnych i – w stosownych przypadkach – zalecenia dotyczące stosowania niniejszego rozporządzenia i innych przepisów Unii objętych nadzorem w ramach piaskownicy.

6. Zasady i warunki funkcjonowania piaskownic regulacyjnych w zakresie AI, w tym kryteria kwalifikowalności i procedury regulujące ubieganie się o uczestnictwo w piaskownicy, selekcję uczestników, uczestnictwo i rezygnowanie z uczestnictwa w piaskownicy regulacyjnej, a także kwestie dotyczące praw i obowiązków uczestników piaskownic określa się w aktach wykonawczych. Wspomniane akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 54

Dalsze przetwarzanie danych osobowych na potrzeby opracowywania określonych systemów sztucznej inteligencji w interesie publicznym w ramach piaskownicy regulacyjnej w zakresie AI

1. W piaskownicy regulacyjnej w zakresie AI dane osobowe zgromadzone zgodnie z prawem w innych celach przetwarza się na potrzeby opracowywania i testowania określonych innowacyjnych systemów sztucznej inteligencji w ramach piaskownicy na następujących warunkach:

   a) innowacyjne systemy sztucznej inteligencji opracowuje się w celu zapewnienia ochrony ważnego interesu publicznego w co najmniej jednym z poniższych obszarów:

      (i) zapobieganie przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub egzekwowania sankcji karnych, w tym ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom pod nadzorem właściwych organów i na ich odpowiedzialność. Przetwarzanie prowadzi się w oparciu o prawo państwa członkowskiego lub prawo Unii;

(ii) bezpieczeństwo publiczne i zdrowie publiczne, uwzględniając zapobieganie chorobom, zwalczanie ich i ich leczenie;

(iii) wysoki poziom ochrony środowiska i poprawa jego jakości;

b) przetwarzane dane są niezbędne do spełnienia co najmniej jednego z wymogów, o których mowa w tytule III rozdział 2, przy czym wymogów tych nie można skutecznie spełnić, przetwarzając dane zanonimizowane, dane syntetyczne lub innego rodzaju dane nieosobowe;

c) ustanowiono skuteczne mechanizmy monitorowania pozwalające zidentyfikować wszelkie poważne zagrożenia dla praw podstawowych osób, których dane dotyczą, jakie mogą wystąpić w trakcie przeprowadzania eksperymentów w ramach piaskownicy, a także mechanizm reagowania zapewniający możliwość szybkiego zaradzenia tym zagrożeniom oraz – w stosownych przypadkach – wstrzymania przetwarzania;

d) wszelkie dane osobowe, które mają być przetwarzane w kontekście piaskownicy, znajdują się w funkcjonalnie wyodrębnionym, odizolowanym i chronionym środowisku przetwarzania danych podlegającym kontroli uczestników korzystających z piaskownicy, a dostęp do tych danych posiadają wyłącznie upoważnione osoby;

e) wszelkie przetwarzane dane osobowe nie mogą być przenoszone, przekazywane ani w żaden inny sposób udostępniane osobom trzecim;

f) żadne przypadki przetwarzania danych osobowych w kontekście piaskownicy nie mogą prowadzić do wdrożenia środków lub podjęcia decyzji wywierających wpływ na osoby, których dane dotyczą;

g) wszelkie dane osobowe przetwarzane w kontekście piaskownicy usuwa się po zakończeniu uczestnictwa w piaskownicy lub po upływie okresu przechowywania danych osobowych;

h) rejestry ewidencjonujące przetwarzanie danych osobowych w kontekście piaskownicy przechowuje się przez cały czas uczestnictwa w piaskownicy oraz przez jeden rok po jego zakończeniu, wyłącznie w celu wywiązania się z obowiązków w zakresie rozliczalności i dokumentacji ustanowionych w niniejszym artykule lub w innych mających zastosowanie przepisach prawa Unii lub prawa państw członkowskich i wyłącznie przez okres niezbędny do wywiązania się z tych obowiązków;

i) w dokumentacji technicznej, o której mowa w załączniku IV, zamieszcza się wyczerpujący i szczegółowy opis procesu trenowania, testowania i walidacji systemu sztucznej inteligencji wraz ze stosownym uzasadnieniem oraz wyniki przeprowadzonych testów;

j) krótkie podsumowanie projektu w zakresie sztucznej inteligencji opracowanego w ramach piaskownicy, jego celów i oczekiwanych rezultatów opublikowano na stronie internetowej właściwych organów.

2. Przepisy ust. 1 nie naruszają przepisów prawa Unii ani prawa państw członkowskich, na których podstawie wyłączono przetwarzanie danych w celach innych niż cele wskazane wprost w tych przepisach prawa Unii lub prawa państw członkowskich.

Artykuł 55
Środki na rzecz drobnych dostawców i użytkowników

1. Państwa członkowskie podejmują następujące działania:

   a) zapewniają drobnym dostawcom i przedsiębiorstwom typu start-up dostęp do piaskownic regulacyjnych w zakresie AI na zasadzie pierwszeństwa, o ile spełniają oni warunki kwalifikowalności;

   b) organizują specjalne wydarzenia informacyjne poświęcone stosowaniu przepisów niniejszego rozporządzenia dostosowane do indywidualnych potrzeb drobnych dostawców i użytkowników;

   c) w stosownych przypadkach tworzą specjalny kanał komunikacji z drobnymi dostawcami i z użytkownikami oraz z innymi innowacyjnymi podmiotami, aby zapewniać im wytyczne i odpowiadać na ich pytania dotyczące wdrażania niniejszego rozporządzenia.

2. Przy ustalaniu wysokości opłat z tytułu oceny zgodności przeprowadzanej zgodnie z art. 43 bierze się pod uwagę szczególne interesy i potrzeby drobnych dostawców, obniżając te opłaty proporcjonalnie do wielkości wspomnianych dostawców i do wielkości rynku.

TYTUŁ VI

ZARZĄDZANIE

ROZDZIAŁ 1

EUROPEJSKA RADA DS. SZTUCZNEJ INTELIGENCJI

Artykuł 56
Ustanowienie Europejskiej Rady ds. Sztucznej Inteligencji

1. Ustanawia się Europejską Radę ds. Sztucznej Inteligencji („Rada”).

2. Rada udziela Komisji porad i wsparcia, aby:

   a) przyczyniać się do zapewnienia owocnej współpracy między krajowymi organami nadzorczymi a Komisją w kwestiach wchodzących w zakres niniejszego rozporządzenia;

   b) koordynować proces sporządzania przez Komisję i krajowe organy nadzorcze oraz inne właściwe organy wytycznych i analiz dotyczących nowych kwestii pojawiających się na rynku wewnętrznym w odniesieniu do kwestii wchodzących w zakres niniejszego rozporządzenia oraz współuczestniczyć w sporządzaniu takich wytycznych i analiz;

   c) wspierać krajowe organy nadzorcze i Komisję w dążeniu do zapewnienia spójnego stosowania przepisów niniejszego rozporządzenia.

Artykuł 57
Struktura Rady

1. W skład Rady wchodzą krajowe organy nadzorcze reprezentowane przez osobę stojącą na czele danego organu lub równoważnego wysokiego rangą urzędnika danego organu oraz Europejski Inspektor Ochrony Danych. Inne organy krajowe mogą być zapraszane na posiedzenia Rady, na których omawia się istotne dla nich kwestie.

2. Rada przyjmuje regulamin wewnętrzny, po zatwierdzeniu go przez Komisję, zwykłą większością głosów swoich członków. Regulamin wewnętrzny reguluje również aspekty operacyjne związane z wykonywaniem zadań Rady wyszczególnionych w art. 58. W stosownych przypadkach Rada może również tworzyć podgrupy na potrzeby zbadania konkretnych kwestii.

3. Radzie przewodniczy Komisja. Komisja zwołuje posiedzenia i przygotowuje porządek obrad zgodnie z zadaniami Rady określonymi w niniejszym rozporządzeniu oraz z jej regulaminem wewnętrznym. Komisja udziela administracyjnego i analitycznego wsparcia na potrzeby działań Rady podejmowanych na podstawie niniejszego rozporządzenia.

4. Rada może zapraszać zewnętrznych ekspertów i obserwatorów do udziału w swoich posiedzeniach oraz może organizować konsultacje z zainteresowanymi osobami trzecimi, wykorzystując w odpowiednim stopniu uzyskane w ten sposób informacje jako wkład w jej działalność. W tym celu Komisja może podejmować działania sprzyjające wymianie informacji między Radą a innymi organami, urzędami, agencjami i grupami doradczymi Unii.

Artykuł 58
Zadania Rady

Udzielając Komisji porad i wsparcia zgodnie z art. 56 ust. 2, Rada w szczególności:

a) gromadzi wiedzę fachową i najlepsze praktyki i udostępnia je państwom członkowskim;

b) wnosi wkład w wypracowywanie jednolitych praktyk administracyjnych w państwach członkowskich, w tym praktyk w zakresie funkcjonowania piaskownic regulacyjnych, o których mowa w art. 53;

c) wydaje opinie, zalecenia lub pisemne uwagi dotyczące kwestii związanych z wdrażaniem niniejszego rozporządzenia, w szczególności:

   (i) w kwestii specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w tytule III rozdział 2,

   (ii) w kwestii stosowania norm zharmonizowanych lub wspólnych specyfikacji, o których mowa w art. 40 i 41,

   (iii) w kwestii sporządzania wytycznych, z uwzględnieniem wytycznych dotyczących ustalania wysokości administracyjnych kar pieniężnych, o których mowa w art. 71.

ROZDZIAŁ 2

WŁAŚCIWE ORGANY KRAJOWE

Artykuł 59
Wyznaczanie właściwych organów krajowych

1. Każde państwo członkowskie ustanawia lub wyznacza właściwe organy krajowe na potrzeby zapewnienia stosowania i wdrażania niniejszego rozporządzenia. Właściwe organy krajowe organizuje się w sposób gwarantujący obiektywizm i bezstronność podejmowanych przez nie działań i wykonywanych przez nie zadań.

2. Każde państwo członkowskie wyznacza krajowy organ nadzorczy spośród właściwych organów krajowych. Krajowy organ nadzorczy pełni funkcję organu notyfikującego i organu nadzoru rynku, chyba że za wyznaczeniem przez państwo członkowskie więcej niż jednego organu przemawiają względy organizacyjne i administracyjne.

3. Państwa członkowskie informują Komisję o wyznaczonym przez siebie organie lub wyznaczonych przez siebie organach, w stosownych przypadkach podając przyczyny wyznaczenia więcej niż jednego organu.

4. Państwa członkowskie zapewniają, aby właściwe organy krajowe dysponowały odpowiednimi zasobami finansowymi i ludzkimi umożliwiającymi im wykonywanie zadań powierzonych im na podstawie niniejszego rozporządzenia. Właściwe organy krajowe muszą w szczególności stale mieć do dyspozycji wystarczającą liczbą pracowników, których kompetencje i wiedza fachowa obejmują dogłębną znajomość kwestii z zakresu technologii sztucznej inteligencji, danych i metod przetwarzania danych, praw podstawowych, zagrożeń dla zdrowia i bezpieczeństwa oraz wiedzę na temat obowiązujących norm i wymogów prawnych.

5. Państwa członkowskie co roku przekazują Komisji sprawozdania dotyczące stanu zasobów finansowych i ludzkich właściwych organów krajowych wraz z oceną ich odpowiedniości. Komisja przekazuje te informacje Radzie w celu ich omówienia i ewentualnego wydania zaleceń.

6. Komisja ułatwia wymianę doświadczeń między właściwymi organami krajowymi.

7. Właściwe organy krajowe mogą udzielać wytycznych i porad dotyczących wdrażania niniejszego rozporządzenia, w tym również drobnym dostawcom. Jeżeli właściwe organy krajowe zamierzają udzielić wytycznych i porad dotyczących systemu sztucznej inteligencji w dziedzinach objętych innymi przepisami Unii, są zobowiązane – w stosownych przypadkach – do każdorazowego zasięgnięcia opinii właściwych organów krajowych wyznaczonych na podstawie tych przepisów Unii. Państwa członkowskie mogą również utworzyć jeden centralny punkt kontaktowy na potrzeby wymiany informacji z operatorami.

8. Jeżeli instytucje, organy i jednostki organizacyjne Unii są objęte zakresem niniejszego rozporządzenia, funkcję właściwego organu odpowiedzialnego za sprawowanie nad nimi nadzoru pełni Europejski Inspektor Ochrony Danych.

TYTUŁ VII

UNIJNA BAZA DANYCH DLA SAMODZIELNYCH SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

Artykuł 60

Unijna baza danych dla samodzielnych systemów sztucznej inteligencji wysokiego ryzyka

1. Komisja – we współpracy z państwami członkowskimi – tworzy i prowadzi unijną bazę danych zawierającą informacje, o których mowa w ust. 2, dotyczące systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w art. 6 ust. 2, które podlegają rejestracji zgodnie z art. 51.
2. Do unijnej bazy danych dane wymienione w załączniku VIII wprowadzają dostawcy. Komisja udziela im wsparcia technicznego i administracyjnego.
3. Informacje zawarte w unijnej bazie danych są publicznie dostępne.
4. Unijna baza danych zawiera dane osobowe wyłącznie w zakresie, w jakim jest to konieczne do celów związanych z gromadzeniem i przetwarzaniem informacji zgodnie z niniejszym rozporządzeniem. Wspomniane informacje obejmują imiona i nazwiska oraz dane kontaktowe osób fizycznych, które są odpowiedzialne za rejestrację systemu i posiadają umocowanie do reprezentowania dostawcy.
5. Komisja pełni funkcję administratora unijnej bazy danych. Zapewnia również dostawcom odpowiednie wsparcie techniczne i administracyjne.

TYTUŁ VIII

MONITOROWANIE PO WPROWADZENIU DO OBROTU, WYMIANA INFORMACJI, NADZÓR RYNKU

ROZDZIAŁ 1

MONITOROWANIE PO WPROWADZENIU DO OBROTU

Artykuł 61

Prowadzone przez dostawców monitorowanie po wprowadzeniu do obrotu i plan monitorowania systemów sztucznej inteligencji wysokiego ryzyka po ich wprowadzeniu do obrotu

1. Dostawcy ustanawiają i dokumentują system monitorowania po wprowadzeniu do obrotu w sposób proporcjonalny do charakteru technologii sztucznej inteligencji i ryzyka związanego ze stosowaniem danego systemu sztucznej inteligencji wysokiego ryzyka.
2. W ramach systemu monitorowania po wprowadzeniu do obrotu w aktywny i systematyczny sposób gromadzi się, dokumentuje i analizuje stosowne dane przekazywane przez użytkowników lub gromadzone z innych źródeł dotyczące skuteczności działania systemów sztucznej inteligencji wysokiego ryzyka w całym cyklu ich życia, przy czym system ten zapewnia dostawcy możliwość oceny, czy

systemy sztucznej inteligencji stale spełniają wymogi ustanowione w tytule III rozdział 2.

3. System monitorowania po wprowadzeniu do obrotu jest oparty na planie monitorowania po wprowadzeniu do obrotu. Plan monitorowania po wprowadzeniu do obrotu stanowi jeden z elementów dokumentacji technicznej, o której mowa w załączniku IV. Komisja przyjmuje akt wykonawczy zawierające szczegółowe przepisy określające wzór planu monitorowania po wprowadzeniu do obrotu oraz wykaz elementów, które należy zawrzeć w tym planie.

4. W przypadku systemów sztucznej inteligencji wysokiego ryzyka objętych przepisami aktów prawnych, o których mowa w załączniku II, jeżeli ustanowiono już system i plan monitorowania po wprowadzeniu do obrotu zgodnie z tymi przepisami, elementy opisane w ust. 1, 2 i 3 włącza się, stosownie do przypadku, do tego systemu i planu.

Przepisy akapitu pierwszego stosuje się również do systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b), wprowadzanych do obrotu lub oddawanych do użytku przez instytucje kredytowe podlegające przepisom dyrektywy 2013/36/UE.

ROZDZIAŁ 2

WYMIANA INFORMACJI NA TEMAT INCYDENTÓW I NIEPRAWIDŁOWEGO DZIAŁANIA

Artykuł 62
Zgłaszanie poważnych incydentów i nieprawidłowego działania

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzanych do obrotu w Unii zgłaszają wszelkie poważne incydenty związane z tymi systemami lub wszelkie przypadki nieprawidłowego działania tych systemów, które stanowią naruszenie obowiązków przewidzianych w prawie Unii mającym na celu ochronę praw podstawowych, organom nadzoru rynku państw członkowskich, w których doszło do danego incydentu lub naruszenia.

Dostawca dokonuje takiego zgłoszenia niezwłocznie po ustaleniu związku przyczynowego między systemem sztucznej inteligencji a incydentem lub nieprawidłowym działaniem lub po potwierdzeniu dostatecznie wysokiego prawdopodobieństwa istnienia takiego związku, a każdym razie najpóźniej w terminie 15 dni od dnia powzięcia przez dostawców wiedzy o wystąpieniu poważnego incydentu lub nieprawidłowego działania.

2. Po otrzymaniu zgłoszenia dotyczącego naruszenia obowiązków przewidzianych w prawie Unii mającym na celu ochronę praw podstawowych organ nadzoru rynku informuje o tym fakcie krajowe organy publiczne lub organy, o których mowa w art. 64 ust. 3. Komisja opracowuje specjalne wytyczne ułatwiające zapewnienie zgodności z obowiązkami określonymi w ust. 1. Wytyczne wydaje się najpóźniej w terminie 12 miesięcy od dnia wejścia niniejszego rozporządzenia w życie.

3. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b), wprowadzanych do obrotu lub oddawanych do użytku przez dostawców będących instytucjami kredytowymi podlegającymi przepisom dyrektywy 2013/36/UE i w przypadku systemów sztucznej inteligencji wysokiego

ryzyka, które są związanymi z bezpieczeństwem elementami wyrobów podlegających przepisom rozporządzenia (UE) 2017/745 i rozporządzenia (UE) 2017/746 lub które same są wyrobami podlegającymi wspomnianym przepisom, zgłaszanie poważnych incydentów lub nieprawidłowego działania ogranicza się do tych poważnych incydentów i przypadków nieprawidłowego działania, które stanowią naruszenie obowiązków przewidzianych w prawie Unii mającym na celu ochronę praw podstawowych.

ROZDZIAŁ 3

EGZEKWOWANIE PRZEPISÓW

Artykuł 63
Nadzór rynku i kontrola systemów sztucznej inteligencji na rynku Unii

1. W odniesieniu do systemów sztucznej inteligencji objętych niniejszym rozporządzeniem zastosowanie mają przepisy rozporządzenia (UE) 2019/1020. Jednak do celów skutecznego egzekwowania przepisów niniejszego rozporządzenia:

   a) wszelkie odniesienia do podmiotu gospodarczego w rozporządzeniu (UE) 2019/1020 rozumie się jako obejmujące wszystkich operatorów zidentyfikowanych w tytule III rozdział 3 niniejszego rozporządzenia;

   b) wszelkie odniesienia do produktu w rozporządzeniu (UE) 2019/1020 rozumie się jako obejmujące wszystkie systemy sztucznej inteligencji wchodzące w zakres niniejszego rozporządzenia.

2. Krajowy organ nadzorczy regularnie przekazuje Komisji sprawozdania dotyczące rezultatów stosownych działań w zakresie nadzoru rynku. Krajowy organ nadzorczy niezwłocznie przekazuje Komisji i odpowiednim krajowym organom ochrony konkurencji wszelkie informacje zgromadzone w trakcie podejmowania działań w zakresie nadzoru rynku, które mogą mieć potencjalnie wartość w kontekście stosowania reguł konkurencji przewidzianych w prawie Unii.

3. W przypadku systemów sztucznej inteligencji wysokiego ryzyka powiązanych z produktami, do których zastosowanie mają przepisy aktów prawnych wymienionych w załączniku II sekcja A, za organ nadzoru rynku do celów niniejszego rozporządzenia uznaje się organ odpowiedzialny za podejmowanie działań w zakresie nadzoru rynku wyznaczony na podstawie tych aktów prawnych.

4. W przypadku systemów sztucznej inteligencji wprowadzonych do obrotu, oddawanych do użytku lub wykorzystywanych przez instytucje finansowe podlegające przepisom Unii dotyczącym usług finansowych za organ nadzoru rynku do celów niniejszego rozporządzenia uznaje się właściwy organ odpowiedzialny za sprawowanie nadzoru finansowego nad tymi instytucjami na podstawie wspomnianych przepisów.

5. W przypadku systemów sztucznej inteligencji wymienionych w załączniku III pkt 1 lit. a) – w zakresie, w jakim systemy te są wykorzystywane do celów związanych z egzekwowaniem prawa – oraz w załączniku III pkt 6 i 7 państwa członkowskie wyznaczają jako organy nadzoru rynku do celów niniejszego rozporządzenia albo właściwe organy nadzorcze odpowiedzialne za ochronę danych, o których mowa w dyrektywie (UE) 2016/680 lub w rozporządzeniu 2016/679, albo właściwe organy krajowe sprawujące nadzór nad działaniami organów ścigania, organów

imigracyjnych lub organów odpowiedzialnych za udzielanie azylu oddających te systemy do użytku lub korzystających z tych systemów.

6. Jeżeli instytucje, organy i jednostki organizacyjne Unii są objęte zakresem niniejszego rozporządzenia, w stosunku do nich rolę organu nadzoru rynku pełni Europejski Inspektor Ochrony Danych.

7. Państwa członkowskie ułatwiają koordynację działań między organami nadzoru rynku wyznaczonymi na podstawie niniejszego rozporządzenia a innymi odpowiednimi organami lub podmiotami krajowymi sprawującymi nadzór nad stosowaniem unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II lub innych przepisów Unii, które mogą być istotne w kontekście systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III.

Artykuł 64
Dostęp do danych i dokumentacji

1. Jeżeli chodzi o dostęp do danych i dokumentacji w kontekście działalności prowadzonej przez organy nadzoru rynku, organom tym zapewnia się pełny dostęp do zbiorów danych treningowych, walidacyjnych i testowych wykorzystywanych przez dostawcę, w tym za pośrednictwem interfejsów programowania aplikacji lub innych odpowiednich środków i narzędzi technicznych umożliwiających zdalny dostęp.

2. Jeżeli jest to konieczne do oceny zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w tytule III rozdział 2 oraz na uzasadniony wniosek, organom nadzoru rynku zapewnia się również dostęp do kodu źródłowego systemu sztucznej inteligencji.

3. Krajowe organy lub podmioty publiczne, które nadzorują lub egzekwują przestrzeganie obowiązków wynikających z prawa Unii służącego ochronie praw podstawowych w odniesieniu do stosowania systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III, są uprawnione do żądania wszelkiej dokumentacji sporządzonej lub prowadzonej na podstawie niniejszego rozporządzenia i do uzyskania do niej dostępu, jeżeli dostęp do tej dokumentacji jest niezbędny do wykonywania ich kompetencji w ramach ich mandatu w granicach ich jurysdykcji. Odpowiedni organ lub podmiot publiczny informuje organ nadzoru rynku zainteresowanego państwa członkowskiego o każdym takim żądaniu.

4. W terminie trzech miesięcy od wejścia w życie niniejszego rozporządzenia każde państwo członkowskie określa organy lub podmioty publiczne, o których mowa w ust. 3, i podaje ich wykaz do publicznej wiadomości na stronie internetowej krajowego organu nadzorczego. Państwa członkowskie przekazują ten wykaz Komisji i wszystkim pozostałym państwom członkowskim oraz na bieżąco go aktualizują.

5. W przypadku gdy dokumentacja, o której mowa w ust. 3, jest niewystarczająca do stwierdzenia, czy nastąpiło naruszenie obowiązków wynikających z prawa Unii mającego na celu ochronę praw podstawowych, organ lub podmiot publiczny, o którym mowa w ust. 3, może wystąpić do organu nadzoru rynku z uzasadnionym wnioskiem o zorganizowanie testów systemu sztucznej inteligencji wysokiego ryzyka przy użyciu środków technicznych. Organ nadzoru rynku organizuje testy

w ścisłej współpracy z wnioskującym organem lub podmiotem publicznym w rozsądnym terminie po otrzymaniu wniosku.

6. Wszelkie informacje i dokumenty uzyskane na podstawie przepisów niniejszego artykułu przez krajowe organy lub podmioty publiczne, o których mowa w ust. 3, traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 70.

Artykuł 65
Procedura postępowania na szczeblu krajowym z systemami sztucznej inteligencji stwarzającymi ryzyko

1. Systemy sztucznej inteligencji stwarzające ryzyko rozumie się jako produkt stwarzający ryzyko w rozumieniu art. 3 pkt 19 rozporządzenia (UE) 2019/1020, o ile ryzyko wiąże się z zagrożeniem dla zdrowia i bezpieczeństwa lub praw podstawowych obywateli.

2. Jeżeli organ nadzoru rynku państwa członkowskiego ma wystarczające powody, aby uznać, że system sztucznej inteligencji stwarza ryzyko, o którym mowa w ust. 1, organ ten przeprowadza ocenę tego systemu sztucznej inteligencji pod kątem zgodności systemu ze wszystkimi wymogami i obowiązkami określonymi w niniejszym rozporządzeniu. W przypadku wystąpienia ryzyka zagrażającego ochronie praw podstawowych organ nadzoru rynku informuje o tym fakcie również odpowiednie krajowe organy lub podmioty publiczne, o których mowa w art. 64 ust. 3. Operatorzy, których to dotyczy, współpracują w razie konieczności z organami nadzoru rynku i innymi krajowymi organami lub podmiotami publicznymi, o których mowa w art. 64 ust. 3.

   Jeżeli w trakcie wspomnianej oceny organ nadzoru rynku stwierdzi, że system sztucznej inteligencji nie jest zgodny z wymogami i obowiązkami określonymi w niniejszym rozporządzeniu, niezwłocznie zobowiązuje danego operatora do podjęcia wszelkich odpowiednich działań naprawczych, aby zapewnić zgodność systemu sztucznej inteligencji z wymogami, wycofać system sztucznej inteligencji z rynku lub wycofać go od użytkowników w wyznaczonym przez organ rozsądnym terminie, stosownym do charakteru ryzyka.

   Organ nadzoru rynku informuje o tym odpowiednią jednostkę notyfikowaną. Art. 18 rozporządzenia (UE) 2019/1020 stosuje się do środków, o których mowa w akapicie drugim.

3. Jeżeli organ nadzoru rynku uzna, że niezgodność nie ogranicza się do terytorium jego państwa, informuje Komisję i inne państwa członkowskie o wynikach oceny i działaniach, do których podjęcia zobowiązał operatora.

4. Operator zapewnia podjęcie wszelkich odpowiednich działań naprawczych w odniesieniu do wszystkich odnośnych systemów sztucznej inteligencji, które wprowadził do obrotu w całej Unii.

5. W przypadku niepodjęcia przez operatora systemu sztucznej inteligencji odpowiednich działań naprawczych w terminie, o którym mowa w ust. 2, organ nadzoru rynku wprowadza wszelkie odpowiednie środki tymczasowe w celu zakazania lub ograniczenia udostępniania systemu sztucznej inteligencji na właściwym dla siebie rynku krajowym, wycofania produktu z rynku lub wycofania go od użytkowników. Organ ten niezwłocznie powiadamia Komisję i pozostałe państwa członkowskie o tych środkach.

6. W powiadomieniu, o którym mowa w ust. 5, zawiera się wszelkie dostępne informacje szczegółowe, w szczególności dane niezbędne do identyfikacji niezgodnego z przepisami systemu sztucznej inteligencji, pochodzenie systemu sztucznej inteligencji, charakter domniemanej niezgodności i związanego z nią ryzyka, charakter i okres obowiązywania zastosowanych środków krajowych oraz argumenty przedstawione przez operatora, którego to dotyczy. W szczególności organy nadzoru rynku wskazują, czy niezgodność wynika z co najmniej jednego z następujących czynników:

   a) niespełnienia przez system sztucznej inteligencji wymogów określonych w tytule III rozdział 2;

   b) braków w normach zharmonizowanych lub wspólnych specyfikacjach, o których mowa w art. 40 i 41, stanowiących podstawę domniemania zgodności.

7. Organy nadzoru rynku państw członkowskich inne niż organ nadzoru rynku państwa członkowskiego, w którym wszczęto postępowanie, niezwłocznie informują Komisję i pozostałe państwa członkowskie o wszelkich przyjętych środkach i przekazują wszelkie posiadane dodatkowe informacje dotyczące niezgodności odnośnego systemu sztucznej inteligencji z przepisami, a w przypadku gdy nie zgadzają się ze zgłoszonym środkiem krajowym – zgłaszają swój sprzeciw.

8. Jeżeli w terminie trzech miesięcy od dnia otrzymania powiadomienia, o którym mowa w ust. 5, ani państwo członkowskie, ani Komisja nie zgłoszą sprzeciwu wobec środka tymczasowego przyjętego przez dane państwo członkowskie, taki środek uznaje się za uzasadniony. Pozostaje to bez uszczerbku dla praw procesowych odnośnego operatora określonych w art. 18 rozporządzenia (UE) 2019/1020.

9. Organy nadzoru rynku we wszystkich państwach członkowskich zapewniają niezwłoczne wprowadzenie odpowiednich środków ograniczających w odniesieniu do danego produktu, takich jak wycofanie produktu z ich rynku.

Artykuł 66
Unijna procedura ochronna

1. Jeżeli w terminie trzech miesięcy od dnia otrzymania powiadomienia, o którym mowa w art. 65 ust. 5, państwo członkowskie zgłosi sprzeciw wobec środka wprowadzonego przez inne państwo członkowskie lub jeżeli Komisja uzna taki środek za sprzeczny z prawem Unii, Komisja niezwłocznie przystępuje do konsultacji z odpowiednim państwem członkowskim i operatorem lub operatorami i poddaje taki środek krajowy ocenie. Na podstawie wyników tej oceny Komisja podejmuje decyzję, czy środek krajowy jest uzasadniony, czy nie, w terminie dziewięciu miesięcy od otrzymania powiadomienia, o którym mowa w art. 65 ust. 5, i powiadamia o tej decyzji zainteresowane państwo członkowskie.

2. W przypadku uznania krajowego środka za uzasadniony wszystkie państwa członkowskie wprowadzają środki konieczne do zapewnienia wycofania niezgodnego z przepisami systemu sztucznej inteligencji ze swoich rynków oraz informują o nich Komisję. W przypadku uznania krajowego środka za nieuzasadniony państwo członkowskie, które dany środek wprowadziło, wycofuje ten środek.

3. W przypadku uznania krajowego środka za uzasadniony i stwierdzenia, że niezgodność systemu sztucznej inteligencji wynika z braków w normach

zharmonizowanych lub wspólnych specyfikacjach, o których mowa w art. 40 i 41 niniejszego rozporządzenia, Komisja stosuje procedurę przewidzianą w art. 11 rozporządzenia (UE) nr 1025/2012.

Artykuł 67
Zgodne z przepisami systemy sztucznej inteligencji, które stwarzają ryzyko

1. Jeżeli po przeprowadzeniu oceny zgodnie z art. 65 organ nadzoru rynku państwa członkowskiego stwierdzi, że chociaż system sztucznej inteligencji jest zgodny z niniejszym rozporządzeniem, stwarza on ryzyko dla zdrowia lub bezpieczeństwa osób, dla wypełnienia obowiązków wynikających z przepisów prawa Unii lub prawa krajowego mających na celu ochronę praw podstawowych lub dla innych aspektów ochrony interesu publicznego, organ ten zobowiązuje właściwego operatora do wprowadzenia wszelkich odpowiednich środków w celu zapewnienia, aby odnośny system sztucznej inteligencji system po wprowadzeniu do obrotu lub oddaniu do użytku nie stwarzał już takiego ryzyka, do wycofania systemu sztucznej inteligencji z rynku lub do wycofania go od użytkowników w wyznaczonym przez organ rozsądnym terminie, stosownym do charakteru ryzyka.

2. Dostawca lub inni właściwi operatorzy zapewniają podjęcie działań naprawczych w odniesieniu do wszystkich odnośnych systemów sztucznej inteligencji, które wprowadzili do obrotu w całej Unii, w terminie wyznaczonym przez organ nadzoru rynku państwa członkowskiego, o którym mowa w ust. 1.

3. To państwo członkowskie niezwłocznie powiadamia o tym Komisję i pozostałe państwa członkowskie. W powiadomieniu tym zawiera się wszelkie dostępne szczegółowe informacje, w szczególności dane niezbędne do identyfikacji odnośnego systemu sztucznej inteligencji, pochodzenie systemu sztucznej inteligencji i informacje na temat jego łańcucha dostaw, charakter przedmiotowego ryzyka oraz charakter i okres obowiązywania zastosowanych środków krajowych.

4. Komisja niezwłocznie przystępuje do konsultacji z państwem członkowskim i właściwym operatorem i poddaje ocenie wprowadzone środki krajowe. Na podstawie wyników tej oceny Komisja podejmuje decyzję, czy środek krajowy jest uzasadniony, czy nie, i w razie potrzeby proponuje odpowiednie środki.

5. Komisja kieruje swoją decyzję do państw członkowskich.

Artykuł 68
Formalna niezgodność z przepisami

1. Jeżeli organ nadzoru rynku państwa członkowskiego dokona jednego z poniższych ustaleń, wymaga od właściwego dostawcy usunięcia danej niezgodności:

   a) umieszczenie oznakowania zgodności z naruszeniem art. 49;

   b) nieumieszczenie oznakowania zgodności;

   c) niesporządzenie deklaracji zgodności UE;

   d) nieprawidłowe sporządzenie deklaracji zgodności UE;

   e) nieumieszczenie numeru identyfikacyjnego jednostki notyfikowanej zaangażowanej, w stosownych przypadkach, w procedurę oceny zgodności.

2. W przypadku gdy niezgodność, o której mowa w ust. 1, utrzymuje się, zainteresowane państwo członkowskie wprowadza wszelkie odpowiednie środki

w celu ograniczenia lub zakazania udostępniania na rynku takiego systemu sztucznej inteligencji wysokiego ryzyka lub zapewnienia, aby system wycofano od użytkowników lub by wycofano go z rynku.

TYTUŁ IX

KODEKSY POSTĘPOWANIA

Artykuł 69
Kodeksy postępowania

1. Komisja i państwa członkowskie zachęcają do tworzenia (i ułatwiają tworzenie) kodeksów postępowania sprzyjających dobrowolnemu stosowaniu w odniesieniu do systemów sztucznej inteligencji innych niż systemy sztucznej inteligencji wysokiego ryzyka wymogów określonych w tytule III rozdział 2, w oparciu o specyfikacje i rozwiązania techniczne, które stanowią odpowiedni sposób zapewnienia zgodności z takimi wymogami w świetle przeznaczenia tych systemów.

2. Komisja i Rada zachęcają do tworzenia (i ułatwiają tworzenie) kodeksów postępowania sprzyjających dobrowolnemu stosowaniu w odniesieniu do systemów sztucznej inteligencji wymogów związanych na przykład ze zrównoważeniem środowiskowym, dostępnością dla osób z niepełnosprawnościami, udziałem zainteresowanych stron w projektowaniu i opracowywaniu systemów sztucznej inteligencji oraz różnorodnością zespołów programistycznych na podstawie jasno określonych celów i kluczowych wskaźników skuteczności działania służących do pomiaru stopnia realizacji tych celów.

3. Kodeksy postępowania mogą być opracowywane przez poszczególnych dostawców systemów sztucznej inteligencji lub przez reprezentujące ich organizacje bądź przez obie te grupy, w tym z udziałem użytkowników i wszelkich zainteresowanych stron oraz reprezentujących je organizacji. Kodeksy postępowania mogą obejmować jeden lub większą liczbę systemów sztucznej inteligencji, mając na uwadze podobieństwa w przeznaczeniu danych systemów.

4. W ramach wspierania i ułatwiania tworzenia kodeksów postępowania Komisja i Rada uwzględniają szczególne interesy i potrzeby drobnych dostawców i przedsiębiorstw typu start-up.

TYTUŁ X

POUFNOŚĆ I KARY

Artykuł 70
Poufność

1. Właściwe organy krajowe i jednostki notyfikowane zaangażowane w stosowanie niniejszego rozporządzenia przestrzegają zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności tak, aby w szczególności:

   a) chronić prawa własności intelektualnej oraz poufne informacje handlowe lub tajemnice przedsiębiorstwa osoby fizycznej lub prawnej, w tym kod źródłowy, chyba że zastosowanie mają przypadki określone w art. 5 dyrektywy (UE)

2016/943 w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem;

b) zagwarantować skuteczne wdrożenie niniejszego rozporządzenia, w szczególności na potrzeby inspekcji, dochodzeń lub kontroli;

c) chronić interesy bezpieczeństwa publicznego i narodowego;

d) gwarantować uczciwy przebieg postępowań karnych i administracyjnych.

2. Nie naruszając przepisów ust. 1, informacji wymienianych na zasadzie poufności między właściwymi organami krajowymi oraz między właściwymi organami krajowymi i Komisją nie można ujawniać bez uprzedniej konsultacji z właściwym organem krajowym, który je przekazał, oraz z użytkownikiem, gdy z systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7, korzystają organy ścigania, organy imigracyjne lub organy odpowiedzialne za udzielanie azylu, jeżeli takie ujawnienie mogłoby zagrozić interesom bezpieczeństwa publicznego i narodowego.

Jeżeli dostawcami systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7, są organy ścigania, organy imigracyjne lub organy odpowiedzialne za udzielanie azylu, dokumentację techniczną, o której mowa w załączniku IV, przechowuje się w siedzibie tych organów. Organy te zapewniają, aby organy nadzoru rynku, o których mowa odpowiednio w art. 63 ust. 5 i 6, mogły uzyskać na żądanie natychmiastowy dostęp do tej dokumentacji lub otrzymać jej kopię. Dostęp do tej dokumentacji lub jej kopii zastrzeżony jest wyłączenia dla pracowników organu nadzoru rynku posiadający poświadczenie bezpieczeństwa na odpowiednim poziomie.

3. Ust. 1 i 2 pozostają bez uszczerbku dla praw i obowiązków Komisji, państw członkowskich i jednostek notyfikowanych w zakresie wymiany informacji i wydawania ostrzeżeń oraz obowiązków zainteresowanych stron w zakresie udzielania informacji zgodnie z prawem karnym państw członkowskich.

4. Komisja i państwa członkowskie mogą, w razie potrzeby, wymieniać informacje poufne z organami regulacyjnymi państw trzecich, z którymi zawarły dwustronne lub wielostronne porozumienia o poufności gwarantujące odpowiedni stopień poufności.

Artykuł 71
Kary

1. Zgodnie z zasadami i warunkami określonymi w niniejszym rozporządzeniu państwa członkowskie przyjmują przepisy dotyczące kar, w tym administracyjnych kar pieniężnych, mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i podejmują wszelkie działania niezbędne do zapewnienia ich właściwego i skutecznego wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Uwzględniają one w szczególności interesy drobnych dostawców i przedsiębiorstw typu start-up oraz ich rentowność.

2. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach, a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.

3. Następujące naruszenia podlegają administracyjnej karze pieniężnej w wysokości do 30 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo –

w wysokości do 6 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

a) nieprzestrzeganie zakazu praktyk w zakresie sztucznej inteligencji, o których mowa w art. 5;

b) niezgodność systemu sztucznej inteligencji z wymogami określonymi w art. 10.

4. Niezgodność systemu sztucznej inteligencji z jakimikolwiek wymogami lub obowiązkami wynikającymi z niniejszego rozporządzenia, innymi niż te określone w art. 5 i 10, podlega administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

5. Przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym i właściwym organ krajowym w odpowiedzi na ich wezwanie podlega administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

6. Ustalając wysokość administracyjnej kary pieniężnej, w każdym indywidualnym przypadku uwzględnia się wszystkie istotne okoliczności danej sytuacji i zwraca się należytą uwagę na następujące kwestie:

a) charakter, wagę i czas trwania naruszenia oraz jego konsekwencje;

b) czy inne organy nadzoru rynku nałożyły już na tego samego operatora administracyjne kary pieniężne za to samo naruszenie;

c) wielkość operatora dopuszczającego się naruszenia i jego udział w rynku.

7. Każde państwo członkowskie określa, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

8. W zależności od systemu prawnego państw członkowskich przepisy dotyczące administracyjnych kar pieniężnych można stosować w taki sposób, że kary w tych państwach członkowskich nakładają, stosownie do przypadku, właściwe sądy krajowe lub inne odpowiednie organy. Stosowanie takich przepisów w tych państwach członkowskich ma skutek równoważny.

Artykuł 72

Administracyjne kary pieniężne nakładane na instytucje, organy i jednostki organizacyjne Unii

1. Europejski Inspektor Ochrony Danych może nakładać administracyjne kary pieniężne na instytucje, organy i jednostki organizacyjne Unii objęte zakresem stosowania niniejszego rozporządzenia. Przy podejmowaniu decyzji, czy nałożyć administracyjną karę pieniężną, oraz przy ustalaniu jej wysokość, uwzględnia się wszystkie istotne okoliczności danej sytuacji i zwraca się w każdym indywidualnym przypadku należytą uwagę na:

a) charakter, wagę i czas trwania naruszenia oraz jego konsekwencje;

b) współpracę z Europejskim Inspektorem Ochrony Danych w celu zaradzenia naruszeniu i złagodzenia ewentualnego niekorzystnego wpływu naruszenia, w tym zastosowanie się do wszelkich środków zarządzonych wcześniej przez Europejskiego Inspektora Ochrony Danych wobec danej instytucji lub organu, lub jednostki organizacyjnej Unii w odniesieniu do tego samego przedmiotu;

c) wszelkie podobne wcześniejsze naruszenia popełnione przez instytucję, organ lub jednostkę organizacyjną Unii.

2. Następujące naruszenia podlegają administracyjnej karze pieniężnej w wysokości do 500 000 EUR:

a) nieprzestrzeganie zakazu praktyk w zakresie sztucznej inteligencji, o których mowa w art. 5;

b) niezgodność systemu sztucznej inteligencji z wymogami określonymi w art. 10.

3. Niezgodność systemu sztucznej inteligencji z jakimikolwiek wymogami lub obowiązkami wynikającymi z niniejszego rozporządzenia, innymi niż te określone w art. 5 i 10, podlega administracyjnej karze pieniężnej w wysokości do 250 000 EUR.

4. Przed podjęciem decyzji na podstawie niniejszego artykułu Europejski Inspektor Ochrony Danych zapewnia instytucji, organowi lub jednostce organizacyjnej Unii, które są przedmiotem postępowania prowadzonego przez Europejskiego Inspektora Ochrony Danych, możliwość bycia wysłuchanym w kwestii dotyczącej ewentualnego naruszenia. Podstawą decyzji wydanej przez Europejskiego Inspektora Ochrony Danych mogą być wyłącznie elementy i okoliczności, co do których zainteresowane strony mogły się wypowiedzieć. Skarżący, jeżeli tacy istnieją, są ściśle włączeni w postępowanie.

5. W toku postępowania w pełni respektuje się prawo zainteresowanych stron do obrony. Strony mają prawo dostępu do akt Europejskiego Inspektora Ochrony Danych z zastrzeżeniem prawnie uzasadnionego interesu osób fizycznych i przedsiębiorstw w zakresie ochrony ich danych osobowych lub tajemnic handlowych.

6. Środki finansowe pochodzące z kar nałożonych na podstawie niniejszego artykułu stanowią dochód budżetu ogólnego Unii.

TYTUŁ XI

PRZEKAZANIE UPRAWNIEŃ I PROCEDURA KOMITETOWA

Artykuł 73
Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 4, art. 7 ust. 1, art. 11 ust. 3, art. 43 ust. 5 i 6 oraz art. 48 ust. 5, powierza się Komisji na czas nieokreślony od dnia [*data wejścia w życie niniejszego rozporządzenia*].

3. Przekazanie uprawnień, o którym mowa w art. 4, art. 7 ust. 1, art. 11 ust. 3, art. 43 ust. 5 i 6 oraz art. 48 ust. 5, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

5. Akt delegowany przyjęty na podstawie art. 4, art. 7 ust. 1, art. 11 ust. 3, art. 43 ust. 5 i 6 oraz art. 48 ust. 5 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 74
Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

TYTUŁ XII

PRZEPISY KOŃCOWE

Artykuł 75
Zmiana rozporządzenia (WE) nr 300/2008

W art. 4 ust. 3 rozporządzenia (WE) nr 300/2008 dodaje się akapit w brzmieniu:

„Przy przyjmowaniu szczegółowych środków związanych ze specyfikacjami technicznymi i procedurami zatwierdzania i korzystania ze sprzętu służącego do ochrony w odniesieniu do systemów sztucznej inteligencji w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [w sprawie sztucznej inteligencji]* uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”.

---

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 76
Zmiana rozporządzenia (UE) nr 167/2013

W art. 17 ust. 5 rozporządzenia (UE) nr 167/2013 dodaje się akapit w brzmieniu:

„Przy przyjmowaniu aktów delegowanych na podstawie akapitu pierwszego dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [w sprawie

sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 77
Zmiana rozporządzenia (UE) nr 168/2013

W art. 22 ust. 5 rozporządzenia (UE) nr 168/2013 dodaje się akapit w brzmieniu:

„Przy przyjmowaniu aktów delegowanych na podstawie akapitu pierwszego dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX w sprawie [sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 78
Zmiana dyrektywy 2014/90/UE

W art. 8 dyrektywy 2014/90/UE dodaje się ustęp w brzmieniu:

„4. W odniesieniu do systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [w sprawie sztucznej inteligencji]*, przy wykonywaniu swoich działań zgodnie z ust. 1 oraz przy przyjmowaniu specyfikacji technicznych i norm badań zgodnie z ust. 2 i 3 Komisja uwzględnia wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 79
Zmiana dyrektywy (UE) 2016/797

W art. 5 dyrektywy (UE) 2016/797 dodaje się ustęp w brzmieniu:

„12. Przy przyjmowaniu aktów delegowanych na podstawie ust. 1 oraz aktów wykonawczych na podstawie ust. 11 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 80
Zmiana rozporządzenia (UE) 2018/858

W art. 5 rozporządzenia (UE) 2018/858 dodaje się ustęp w brzmieniu:

„4. Przy przyjmowaniu aktów delegowanych na podstawie ust. 3 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 81
Zmiana rozporządzenia (UE) 2018/1139

W rozporządzeniu (UE) 2018/1139 wprowadza się następujące zmiany:

1) w art. 17 dodaje się ustęp w brzmieniu:

„3. Bez uszczerbku dla ust. 2 przy przyjmowaniu aktów wykonawczych na podstawie ust. 1 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [*w sprawie sztucznej inteligencji*]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”;

2) w art. 19 dodaje się ustęp w brzmieniu:

„4. Przy przyjmowaniu aktów delegowanych na podstawie ust. 1 i 2 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”;

3) w art. 43 dodaje się ustęp w brzmieniu:

„4. Przy przyjmowaniu aktów wykonawczych na podstawie ust. 1 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”;

4) w art. 47 dodaje się ustęp w brzmieniu:

„3. Przy przyjmowaniu aktów delegowanych na podstawie ust. 1 i 2 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”;

5) w art. 57 dodaje się akapit w brzmieniu:

„Przy przyjmowaniu tych aktów wykonawczych dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”;

6) w art. 58 dodaje się ustęp w brzmieniu:

„3. Przy przyjmowaniu aktów delegowanych na podstawie ust. 1 i 2 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu

rozporządzenia (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”.

Artykuł 82
Zmiana rozporządzenia (UE) 2019/2144

W art. 11 rozporządzenia (UE) 2019/2144 dodaje się ustęp w brzmieniu:

„3. Przy przyjmowaniu aktów wykonawczych na podstawie ust. 2 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) YYY/XX [w sprawie sztucznej inteligencji]*, uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

_____

* Rozporządzenie (UE) YYY/XX [w sprawie sztucznej inteligencji] (Dz.U. ...).”.

Artykuł 83
Systemy sztucznej inteligencji już wprowadzone do obrotu lub oddane do użytku

1. Niniejsze rozporządzenie nie ma zastosowania do systemów sztucznej inteligencji, które stanowią elementy wielkoskalowych systemów informatycznych utworzonych na podstawie aktów prawnych wymienionych w załączniku IX i które wprowadzono do obrotu lub oddano do użytku przed dniem *[12 miesięcy od daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2]* r., chyba że na skutek zastąpienia lub zmiany tych aktów prawnych zajdzie znacząca zmiana projektu lub przeznaczenia odnośnego systemu sztucznej inteligencji lub odnośnych systemów sztucznej inteligencji.

   Wymogi określone w niniejszym rozporządzeniu uwzględnia się, w stosownych przypadkach, w ocenach każdego z wielkoskalowych systemów informatycznych utworzonych na podstawie aktów prawnych wymienionych w załączniku IX, które to oceny należy przeprowadzić zgodnie z odnośnymi przepisami tych aktów.

2. Niniejsze rozporządzenie ma zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka innych niż te określone w ust. 1, które wprowadzono do obrotu lub oddano do użytku przed dniem [*data rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*] r., wyłącznie wówczas, gdy po tej dacie projekt lub przeznaczenie tych systemów ulegną znaczącym zmianom.

Artykuł 84
Ocena i przegląd

1. Komisja ocenia potrzebę wprowadzenia zmian w wykazie zawartym w załączniku III raz w roku po wejściu w życie niniejszego rozporządzenia.

2. Do dnia [*trzy lata od daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*] r., a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia. Sprawozdania te są podawane do wiadomości publicznej.

3. W sprawozdaniach, o których mowa w ust. 2, szczególną uwagę zwraca się na następujące kwestie:

a) stan zasobów finansowych i ludzkich właściwych organów krajowych wymaganych, by mogły one skutecznie wykonywać zadania powierzone im na podstawie niniejszego rozporządzenia;

b) sytuację w zakresie kar, a w szczególności administracyjnych kar pieniężnych, o których mowa w art. 71 ust. 1, nakładanych przez państwa członkowskie w przypadku naruszenia przepisów niniejszego rozporządzenia.

4. Do dnia [*trzy lata od daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*] r., a następnie co cztery lata Komisja ocenia wpływ i skuteczność kodeksów postępowania sprzyjających stosowaniu wymogów określonych w tytule III rozdział 2 oraz ewentualnie innych dodatkowych wymogów dotyczących systemów sztucznej inteligencji innych niż systemy sztucznej inteligencji wysokiego ryzyka.

5. Do celów ust. 1–4 Rada, państwa członkowskie i właściwe organy krajowe przekazują Komisji informacje na jej wniosek.

6. Dokonując ocen i przeglądów, o których mowa w ust. 1–4, Komisja uwzględnia stanowiska i ustalenia Rady, Parlamentu Europejskiego, Rady Unii Europejskiej oraz innych stosownych podmiotów lub źródeł.

7. W razie potrzeby Komisja przedkłada odpowiednie wnioski w celu zmiany niniejszego rozporządzenia, uwzględniając w szczególności rozwój technologii oraz stan postępu w społeczeństwie informacyjnym.

Artykuł 85
Wejście w życie i stosowanie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie stosuje się od dnia [24 miesiące po wejściu w życie niniejszego rozporządzenia] r..

3. Na zasadzie odstępstwa od ust. 2:

a) tytuł III rozdział 4 i tytuł VI stosuje się od dnia [trzy miesiące od daty wejścia w życie niniejszego rozporządzenia] r.;

b) art. 71 stosuje się od dnia [dwanaście miesięcy od daty wejścia w życie niniejszego rozporządzenia] r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego
Przewodniczący

W imieniu Rady
Przewodniczący

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

1.3. Wniosek/inicjatywa dotyczy:

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

1.4.2. Cel(e) szczegółowy(e)

1.4.3. Oczekiwane wyniki i wpływ

1.4.4. Wskaźniki dotyczące realizacji celów

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

1.5.5 Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

1.6. Okres trwania i wpływ finansowy wniosku/inicjatywy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Synteza szacunkowego wpływu na środki operacyjne

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

3.2.3. Synteza szacunkowego wpływu na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

Sieci komunikacyjne, treści i technologie;

rynek wewnętrzny, przemysł, przedsiębiorczość i MŚP;

wpływ na budżet wiąże się z nowymi zadaniami powierzonymi Komisji, w tym z zadaniami z zakresu wsparcia na rzecz Europejskiej Rady ds. Sztucznej Inteligencji.

Działanie: Kształtowanie cyfrowej przyszłości Europy.

1.3. Wniosek/inicjatywa dotyczy:

X **nowego działania**

☐ **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[64]

☐ **przedłużenia bieżącego działania**

☐ **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Celem ogólnym interwencji jest zapewnienie prawidłowego funkcjonowania jednolitego rynku przez stworzenie warunków sprzyjających rozwijaniu i wykorzystywaniu w Unii wiarygodnej sztucznej inteligencji.

1.4.2. Cel(e) szczegółowy(e)

Cel szczegółowy nr 1

Określenie wymogów odnoszących się do systemów sztucznej inteligencji oraz obowiązków nałożonych na wszystkich uczestników łańcucha wartości w celu zapewnienia, aby systemy sztucznej inteligencji wprowadzane do obrotu i znajdujące się w użyciu były bezpieczne i zgodne z obowiązującym prawem w obszarze praw podstawowych oraz z unijnymi wartościami.

Cel szczegółowy nr 2

Zapewnienie pewności prawa na potrzeby ułatwienia inwestycji i innowacji w dziedzinie sztucznej inteligencji poprzez jasne określenie podstawowych wymogów, obowiązków, a także procedur dotyczących zgodności i przestrzegania przepisów, które należy spełnić, aby wprowadzić system sztucznej inteligencji do obrotu na rynku unijnym lub z niego korzystać.

[64] O którym mowa w art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

Cel szczegółowy nr 3

Poprawa zarządzania i skuteczne egzekwowanie obowiązujących przepisów prawa dotyczących praw podstawowych i wymogów bezpieczeństwa mających zastosowanie do systemów sztucznej inteligencji poprzez zapewnienie odpowiednim organom nowych uprawnień, zasobów i jasnych zasad dotyczących procedur oceny zgodności i monitorowania *ex post* oraz podziału zadań w zakresie zarządzania i nadzoru między szczeblem krajowym i unijnym.

Cel szczegółowy nr 4

Ułatwienie rozwoju jednolitego rynku zgodnych z prawem, bezpiecznych i wiarygodnych zastosowań sztucznej inteligencji oraz zapobieganie fragmentacji rynku poprzez podjęcie działań na szczeblu UE na rzecz określenia minimalnych wymogów dotyczących systemów sztucznej inteligencji, które mają być wprowadzane na rynek unijny i wykorzystywane na nim zgodnie z obowiązującym prawem w zakresie praw podstawowych i bezpieczeństwa.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Dostawcy sztucznej inteligencji powinni odnieść korzyści dzięki istnieniu niewielkiego, ale jasnego zbioru wymogów, który zapewni pewność prawa i dostęp do całego jednolitego rynku.

Użytkownicy sztucznej inteligencji powinni odnieść korzyści dzięki pewności prawa polegającej na tym, że nabywane przez nich systemy sztucznej inteligencji wysokiego ryzyka będą zgodne z europejskimi przepisami i wartościami.

Konsumenci powinni odnieść korzyści dzięki zmniejszeniu ryzyka naruszenia ich bezpieczeństwa lub praw podstawowych.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

Wskaźnik 1

Liczba poważnych incydentów lub wyników działania sztucznej inteligencji, które stanowią poważny incydent lub naruszenie obowiązków wynikających z praw podstawowych (w ujęciu półrocznym), w podziale na dziedziny zastosowań, i obliczona a) w ujęciu bezwzględnym, b) jako odsetek wdrożonych zastosowań oraz c) jako odsetek liczby obywateli, wobec których systemy te są stosowane.

Wskaźnik 2

a) całkowita wartość inwestycji w sztuczną inteligencję w UE (w ujęciu rocznym)

b) całkowita wartość inwestycji w sztuczną inteligencję według państw członkowskich (w ujęciu rocznym)

c) odsetek przedsiębiorstw wykorzystujących sztuczną inteligencję (w ujęciu rocznym)

d) odsetek MŚP wykorzystujących sztuczną inteligencję (w ujęciu rocznym)

a) i b) zostaną obliczone w oparciu o oficjalne źródła i porównane z prywatnymi oszacowaniami

c) i d) będą gromadzone za pomocą regularnych badań dotyczących przedsiębiorstw

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Rozporządzenie powinno w pełni obowiązywać półtora roku po jego przyjęciu. Elementy struktury zarządzania powinny jednak zacząć funkcjonować wcześniej. W szczególności państwa członkowskie powinny wcześniej wyznaczyć istniejące organy lub ustanowić nowe organy do wykonania zadań określonych w przepisach; powinna także powstać i rozpocząć działalność Europejska Rada ds. Sztucznej Inteligencji. Do momentu rozpoczęcia stosowania europejska baza danych dla systemów sztucznej inteligencji powinna w pełni funkcjonować. Prace nad stworzeniem bazy danych powinny zatem toczyć się równolegle do procedury ustawodawczej, aby dobiegły końca w momencie wejścia w życie rozporządzenia.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej

efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Powstające niejednolite ramy potencjalnie rozbieżnych przepisów krajowych utrudnią sprawne dostarczanie systemów sztucznej inteligencji w całej UE i są nieskuteczne w zapewnianiu bezpieczeństwa i ochrony praw podstawowych oraz wartości unijnych w poszczególnych państwach członkowskich. Wspólne działania legislacyjne UE w zakresie sztucznej inteligencji mogą wzmocnić rynek wewnętrzny i mają znaczny potencjał zapewnienia przemysłowi europejskiemu przewagi konkurencyjnej na poziomie globalnym oraz korzyści skali, których nie mogą osiągnąć samodzielnie poszczególne państwa członkowskie.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

W dyrektywie 2000/31/WE o handlu elektronicznym zapewniono podstawowe ramy funkcjonowania jednolitego rynku usług cyfrowych i nadzoru nad takimi usługami oraz określono podstawową strukturę mechanizmu ogólnej współpracy między państwami członkowskimi, która obejmuje zasadniczo wszystkie wymogi mające zastosowanie do usług cyfrowych. W wyniku oceny wspomnianej dyrektywy zidentyfikowano niedociągnięcia dotyczące szeregu aspektów tego mechanizmu współpracy, w tym istotnych aspektów proceduralnych, między innymi brak wyraźnych terminów na udzielenie odpowiedzi przez państwa członkowskie w połączeniu z ogólnym brakiem reagowania na wnioski ze strony innych państw. Na przestrzeni lat doprowadziło to do braku zaufania między państwami członkowskimi pod względem rozwiązywania problemów dotyczących dostawców oferujących transgraniczne usługi cyfrowe. Z oceny dyrektywy wynika, że konieczne jest określenie zróżnicowanego zestawu przepisów i wymogów na szczeblu europejskim. Z tego względu wypełnienie obowiązków określonych w niniejszym rozporządzeniu wymagałoby szczególnego mechanizmu współpracy na szczeblu UE, ze strukturą zarządzania zapewniającą koordynację określonych odpowiedzialnych organów na szczeblu UE.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

W rozporządzeniu ustanawiającym zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniającym niektóre akty ustawodawcze Unii określono nowe wspólne ramy dotyczące wymogów mających zastosowanie do systemów sztucznej inteligencji, które to ramy znacznie wykraczają poza ramy ustanowione w obowiązującym prawodawstwie. Z tego względu należy ustanowić niniejszym wnioskiem nową krajową i europejską funkcję regulacyjną i koordynacyjną.

Jeśli chodzi o możliwe synergie z innymi odpowiednimi instrumentami, rolę organów notyfikujących na poziomie krajowym mogą pełnić organy krajowe pełniące podobne funkcje zgodnie z innymi rozporządzeniami UE.

Ponadto dzięki zwiększeniu zaufania do sztucznej inteligencji, a tym samym zachęceniu do inwestycji w rozwijanie i absorpcję sztucznej inteligencji, wniosek uzupełnia program „Cyfrowa Europa", w ramach którego promocję rozpowszechniania sztucznej inteligencji określono jako jeden z pięciu celów priorytetowych.

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Nastąpi realokacja personelu. Pozostałe koszty zostaną pokryte ze środków przydzielonych na program „Cyfrowa Europa”, ponieważ cel niniejszego rozporządzenia – zapewnienie wiarygodnej sztucznej inteligencji – bezpośrednio przyczynia się do realizacji jednego z kluczowych celów programu – przyspieszenia rozwoju i wdrażania sztucznej inteligencji w Europie.

1.6. Okres trwania i wpływ finansowy wniosku/inicjatywy

☐ **Ograniczony czas trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

X **Nieograniczony czas trwania**

– Wprowadzenie w życie z okresem rozruchu 1–2 lat (do potwierdzenia),

– po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[65]

X **Bezpośrednie zarządzanie** przez Komisję

– ☐ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze;

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

– *W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.*

Uwagi

65 Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Rozporządzenie zostanie poddane przeglądowi i ocenie po upływie pięciu lat od jego wejścia w życie. Komisja przedstawi sprawozdanie z wyników oceny Parlamentowi Europejskiemu, Radzie oraz Europejskiemu Komitetowi Ekonomiczno-Społecznemu.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

W rozporządzeniu ustanawia się nową politykę w odniesieniu do zharmonizowanych przepisów dotyczących dostarczania systemów sztucznej inteligencji na rynku wewnętrznym przy jednoczesnym zapewnieniu poszanowania bezpieczeństwa i praw podstawowych. Te nowe przepisy wymagają również ustanowienia mechanizmu spójności w zakresie transgranicznego stosowania obowiązków wynikających z niniejszego rozporządzenia w postaci utworzenia nowej grupy doradczej koordynującej działania organów krajowych.

Konieczne jest zapewnienie służbom Komisji odpowiednich zasobów, aby mogły sprostać tym nowym zadaniom. Szacuje się, że egzekwowanie przepisów nowego rozporządzenia będzie wymagało 10 EPC (5 EPC na potrzeby wspierania działalności Rady oraz 5 EPC na rzecz Europejskiego Inspektora Ochrony Danych działającego jako organ notyfikujący w odniesieniu do systemów sztucznej inteligencji wdrożonych przez organ Unii Europejskiej).

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

Aby zapewnić członkom Rady możliwość przeprowadzania uzasadnionych analiz na podstawie dowodów, przewiduje się, że Radę powinna wspierać struktura administracyjna Komisji oraz że powstanie grupa ekspertów w celu zapewnienia dodatkowej wiedzy specjalistycznej stosownie do potrzeb.

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

Jeżeli chodzi o wydatki na posiedzenia, biorąc pod uwagę niską wartość pojedynczej transakcji (np. zwrot kosztów podróży dla delegata na posiedzenie), standardowe procedury kontroli wydają się wystarczające. Jeśli chodzi o rozwijanie bazy danych, w DG CNECT wdrożono silny system kontroli wewnętrznej dzięki scentralizowanemu udzielaniu zamówień.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

Dodatkowe potrzeby w zakresie środków niezbędnych do celów niniejszego rozporządzenia zostaną zaspokojone w ramach istniejących środków zapobiegania nadużyciom finansowym mających zastosowanie do Komisji.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn[66].	państw EFTA[67]	krajów kandydujących[68]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
7	20 02 06 Wydatki administracyjne	Niezróżn.	NIE	NIE	NIE	NIE
1	02 04 03 Program „Cyfrowa Europa” – sztuczna inteligencja	Zróżn.	TAK	NIE	NIE	NIE
1	02 01 30 01 Wydatki na wsparcie dotyczące programu „Cyfrowa Europa”	Niezróżn.	TAK	NIE	NIE	NIE

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Synteza szacunkowego wpływu na wydatki na środki operacyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– X Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

66 Środki zróżnicowane / środki niezróżnicowane.
67 EFTA: Europejskie Stowarzyszenie Wolnego Handlu.
68 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

Dział wieloletnich ram finansowych	1	

DG: CNECT				Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**[69]	**OGÓŁEM**	
• Środki operacyjne											
Linia budżetowa[70] 02 04 03		Środki na zobowiązania	(1a)		1,000						**1,000**
		Środki na płatności	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Linia budżetowa		Środki na zobowiązania	(1b)								
		Środki na płatności	(2b)								
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[71]											
Linia budżetowa 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
OGÓŁEM środki na rzecz DG CNECT		Środki na zobowiązania	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Środki na płatności	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 Orientacyjne i zależne od dostępności środków budżetowych.

70 Zgodnie z oficjalną nomenklaturą budżetową.

71 Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)		1,000						**1,000**
	Środki na płatności	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
OGÓŁEM środki na DZIAŁ 1 wieloletnich ram finansowych	Środki na zobowiązania	=4+ 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Środki na płatności	=5+ 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu, należy powtórzyć powyższą sekcję:

• OGÓŁEM środki operacyjne (wszystkie działy operacyjne)	Środki na zobowiązania	(4)								
	Środki na płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne (wszystkie działy operacyjne)		(6)								
OGÓŁEM środki na DZIAŁY 1–6 wieloletnich ram finansowych (Kwota referencyjna)	Środki na zobowiązania	=4+ 6								
	Środki na płatności	=5+ 6								

Dział wieloletnich ram finansowych	**7**	„Wydatki administracyjne”

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznik V do przepisów wewnętrznych), przesyłanego do DECIDE w celu konsultacji między służbami.

w mln EUR (do trzech miejsc po przecinku)

		Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Po roku 2027**[72]	**OGÓŁEM**
DG: CNECT								
• Zasoby ludzkie		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Pozostałe wydatki administracyjne		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
OGÓŁEM DG CNECT	**Środki**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Europejski Inspektor Ochrony Danych								
• Zasoby ludzkie		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Pozostałe wydatki administracyjne								
OGÓŁEM EIOD	**Środki**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

w mln EUR (do trzech miejsc po przecinku)

	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**		**OGÓŁEM**

[72] Wszystkie dane liczbowe w tej kolumnie mają charakter orientacyjny i są zależne od kontynuacji programów oraz dostępności środków.

OGÓŁEM środki na DZIAŁY 1–7 wieloletnich ram finansowych	Środki na zobowiązania		2,770	1,770	1,770	1,770	1,770		**9,850**
	Środki na płatności		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty ⇩			Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		Po roku **2027**[73]		**OGÓŁEM**	
	PRODUKT																	
	Rodzaj	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[74]...																		
Baza danych					1	1,000	1		1		1		1		1	0,100	1	1,000
Posiedzenia –					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Działania komunikacyjne					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Cel szczegółowy nr 1 – suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2 ...																		
– Produkt																		
Cel szczegółowy nr 2 – suma cząstkowa																		
OGÓŁEM					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Wszystkie dane liczbowe w tej kolumnie mają charakter orientacyjny i są zależne od kontynuacji programów oraz dostępności środków.

[74] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”

3.2.3. Synteza szacunkowego wpływu na środki administracyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– X Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Corocznie po 2027**[75]	**OGÓŁEM**
DZIAŁ 7 wieloletnich ram finansowych								
Zasoby ludzkie		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Pozostałe wydatki administracyjne		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**

Poza DZIAŁEM 7[76] **wieloletnich ram finansowych**								
Zasoby ludzkie								
Pozostałe wydatki o charakterze administracyjnym		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Suma cząstkowa poza DZIAŁEM 7 wieloletnich ram finansowych		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**

OGÓŁEM		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

75 Wszystkie dane liczbowe w tej kolumnie mają charakter orientacyjny i są zależne od kontynuacji programów oraz dostępności środków.

76 Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

3.2.3.1. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

– X Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

.		Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Po roku 2027**[77]	
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)		10	10	10	10	10	10	
20 01 02 03 (w delegaturach)								
01 01 01 01 (pośrednie badania naukowe)								
01 01 01 11 (bezpośrednie badania naukowe)								
Inna linia budżetowa (określić)								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)[78]								
20 02 01 (CA, SNE, INT z globalnej koperty finansowej)								
20 02 03 (CA, LA, SNE, INT i JPD w delegaturach)								
XX 01 xx **yy zz** [79]	– w centrali							
	– w delegaturach							
01 01 01 02 (CA, SNE, INT – pośrednie badania naukowe)								
01 01 01 12 (CA, INT, SNE – bezpośrednie badania naukowe)								
Inna linia budżetowa (określić)								
OGÓŁEM		**10**	**10**	**10**	**10**	**10**	**10**	

XX oznacza odpowiedni obszary polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Oczekuje się, że EIOD zapewni połowę wymaganych zasobów.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Organizacja łącznie 13–16 posiedzeń, sporządzanie projektów sprawozdań, kontynuowanie prac w zakresie polityki, np. dotyczących przyszłych zmian w wykazie zastosowań sztucznej inteligencji wysokiego ryzyka, oraz utrzymywanie stosunków z organami państw członkowskich wymagać będą czterech EPC w grupie funkcyjnej AD i jednego EPC w grupie funkcyjnej AST. W przypadku systemów sztucznej inteligencji opracowanych przez instytucje Unii odpowiedzialny jest Europejski Inspektor Ochrony Danych. Na podstawie

[77] Wszystkie dane liczbowe w tej kolumnie mają charakter orientacyjny i są zależne od kontynuacji programów oraz dostępności środków.

[78] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JPD = młodszy specjalista w delegaturze.

[79] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

	dotychczasowych doświadczeń można oszacować, że do wypełnienia obowiązków EIOD wynikających z projektu aktu prawnego potrzeba 5 EPC w grupie funkcyjnej AD.
Personel zewnętrzny	

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

– X mogą być w pełni sfinansowane przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF).

Nie ma potrzeby przeprogramowania.

– ☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF.

Należy wyjaśnić, który wariant jest konieczny, określając działy i linie budżetowe, których ma dotyczyć, odpowiadające im kwoty oraz proponowane instrumenty, które należy zastosować.

– ☐ wymaga rewizji WRF.

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

– X nie przewiduje współfinansowania ze strony osób trzecich

– ☐ przewiduje współfinansowanie ze strony osób trzecich szacowane zgodnie z poniższymi szacunkami:

Środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**[80]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (zob. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

[80] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy. „N” należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021). Tak samo należy postąpić dla kolejnych lat.

3.3. Szacunkowy wpływ na dochody

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

  – ☐ wpływ na dochody inne

  – ☐ wpływ na dochody inne

  – Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków ☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[81]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (zob. pkt 1.6)		
Artykuł …								

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

[81] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.