Parlament Europejski
2019-2024

TEKSTY PRZYJĘTE

P9_TA(2024)0138

Akt w sprawie sztucznej inteligencji

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 13 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

(Zwykła procedura ustawodawcza: pierwsze czytanie)

Parlament Europejski,

– uwzględniając wniosek Komisji przedstawiony Parlamentowi Europejskiemu i Radzie (COM(2021)0206),

– uwzględniając art. 294 ust. 2 oraz art. 16 i 114 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C9-0146/2021),

– uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

– uwzględniając opinię Europejskiego Banku Centralnego z dnia 29 grudnia 2021 r.[1],

– uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 22 września 2021 r.[2],

– uwzględniając wstępne porozumienie zatwierdzone przez komisję przedmiotowo właściwą na podstawie art. 74 ust. 4 Regulaminu oraz przekazane pismem z dnia 2 lutego 2024 r. zobowiązanie przedstawiciela Rady do zatwierdzenia stanowiska Parlamentu, zgodnie z art. 294 ust. 4 Traktatu o funkcjonowaniu Unii Europejskiej,

– uwzględniając art. 59 Regulaminu,

– uwzględniając wyniki wspólnych posiedzeń Komisji Rynku Wewnętrznego i Ochrony Konsumentów oraz Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych zgodnie z art. 58 Regulaminu,

---

1 Dz.U. C 115 z 11.3.2022, s. 5.
2 Dz.U. C 517 z 22.12.2021, s. 56.

– uwzględniając opinie przedstawione przez Komisję Przemysłu, Badań Naukowych i Energii, Komisję Kultury i Edukacji, Komisję Prawną, Komisję Ochrony Środowiska Naturalnego, Zdrowia Publicznego i Bezpieczeństwa Żywności oraz Komisję Transportu i Turystyki,

– uwzględniając sprawozdanie Komisji Rynku Wewnętrznego i Ochrony Konsumentów oraz Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (A9-0188/2023),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu[3];

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli zastąpi ona pierwotny wniosek, wprowadzi w nim istotne zmiany lub planuje ich wprowadzenie;

3. zobowiązuje swoją przewodniczącą do przekazania stanowiska Parlamentu Radzie i Komisji oraz parlamentom narodowym.

---

[3] Niniejsze stanowisko zastępuje poprawki przyjęte dnia 14 czerwca 2023 r. (Teksty przyjęte, P9_TA(2023)0236).

P9_TC1-COD(2021)0106

Stanowisko Parlamentu Europejskiego przyjęte w pierwszym czytaniu w dniu 13 marca 2024 r. w celu przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/... ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniającego rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)*

(Tekst mający znaczenie dla EOG)

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[1],

uwzględniając opinię Europejskiego Banku Centralnego[2],

uwzględniając opinię Komitetu Regionów[3],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[4],

---

* TEKST NIE BYŁ JESZCZE PRZEDMIOTEM FINALIZACJI PRAWNO-JĘZYKOWEJ.

1 Dz.U. C 517 z 22.12.2021, s. 56.

2 ***Dz.U. C 115 z 11.3.2022, s. 5.***

3 Dz.U. C 97 z 28.2.2022, s. 60.

4 Stanowisko Parlamentu Europejskiego z dnia 13 marca 2024 r.

a także mając na uwadze, co następuje:

(1) Celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego przez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, ***wprowadzania do obrotu, oddawania do użytku i*** wykorzystywania ***systemów*** sztucznej inteligencji (systemy AI) ***w Unii*** zgodnie z wartościami Unii, ***promowanie upowszechniania ukierunkowanej na człowieka i godnej zaufania sztucznej inteligencji (AI) przy jednoczesnym zapewnieniu*** wysokiego poziomu ochrony zdrowia, bezpieczeństwa***,*** praw podstawowych ***zapisanych w Karcie praw podstawowych Unii Europejskiej (Karta)***, w ***tym demokracji, praworządności i ochrony środowiska, przed szkodliwymi skutkami systemów AI w Unii, a także wspieranie innowacji. Niniejsze rozporządzenie*** zapewnia swobodny transgraniczny przepływ towarów i usług opartych na AI, uniemożliwiając tym samym państwom członkowskim nakładanie ograniczeń na rozwój, wprowadzanie do obrotu i wykorzystywanie ***systemów AI***, chyba że jest to wyraźnie dozwolone w niniejszym rozporządzeniu.

(2) Niniejsze rozporządzenie należy stosować zgodnie z wartościami Unii zapisanymi w Karcie, ułatwiając ochronę osób fizycznych, przedsiębiorstw, demokracji i praworządności oraz środowiska, a jednocześnie pobudzając innowacje i zatrudnienie oraz czyniąc Unię liderem w upowszechnianiu godnej zaufania AI.

(3) ▌ Systemy AI ▌ mogą być łatwo wdrażane w wielu różnych sektorach gospodarki i obszarach życia społecznego, w tym w wymiarze transgranicznym, i mogą łatwo podlegać obrotowi w całej Unii. Niektóre państwa członkowskie zastanawiają się już nad przyjęciem przepisów krajowych w celu zapewnienia, aby AI była ***godna zaufania i*** bezpieczna oraz rozwijana i wykorzystywana w sposób zgodny z obowiązkami wynikającymi z praw podstawowych. Zróżnicowane przepisy krajowe mogą prowadzić do rozdrobnienia rynku wewnętrznego i mogą zmniejszyć pewność prawa dla operatorów, którzy opracowują***, importują*** lub wykorzystują systemy AI. ***Aby osiągnąć godną zaufania AI*** należy zatem zapewnić spójny i wysoki poziom ochrony w całej Unii poprzez ustanowienie jednolitych obowiązków dla operatorów 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), zapobiegając jednocześnie rozbieżnościom, które utrudniają swobodny obrót systemami AI oraz powiązanymi produktami i usługami na rynku wewnętrznym, a także utrudniają ***innowacje w zakresie systemów AI oraz ich wdrażanie i rozpowszechnianie***. W zakresie, w jakim niniejsze rozporządzenie zawiera przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w odniesieniu do ograniczenia wykorzystywania systemów AI do zdalnej identyfikacji biometrycznej ***do celów ścigania przestępstw, ograniczenia wykorzystywania systemów AI do oceny ryzyka w odniesieniu do osób fizycznych do celów ścigania przestępstw i ograniczenia wykorzystywania systemów AI kategoryzacji biometrycznej*** do celów ścigania przestępstw, 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.

(4) AI to szybko rozwijająca się grupa technologii, które ***przyczyniają się*** do wielu różnych korzyści ekonomicznych***, środowiskowych*** i społecznych we wszystkich gałęziach przemysłu i obszarach działalności społecznej. Ponieważ wykorzystywanie AI umożliwia lepsze prognozowanie, optymalizację operacji i przydzielania zasobów oraz personalizację rozwiązań cyfrowych dostępnych dla osób fizycznych i organizacji, może ono zapewnić przedsiębiorstwom kluczową przewagę konkurencyjną i wzmacniać korzyści społeczne i środowiskowe, na przykład w zakresie opieki zdrowotnej, rolnictwa, ***bezpieczeństwa żywności,*** kształcenia i szkolenia, ***mediów, sportu, kultury,*** zarządzania infrastrukturą, energetyki, transportu i logistyki, usług publicznych, bezpieczeństwa, wymiaru sprawiedliwości, zasobooszczędności i efektywności energetycznej, ***monitorowania środowiska, ochrony i odbudowy różnorodności biologicznej i ekosystemów*** oraz łagodzenia zmiany klimatu i przystosowywania się do niej.

(5) Jednocześnie AI może być źródłem zagrożeń i szkody dla interesu publicznego i praw ***podstawowych*** chronionych przepisami Unii, w zależności od okoliczności jej konkretnego zastosowania, ***wykorzystania oraz od poziomu rozwoju technologicznego***. Szkody te mogą być materialne lub niematerialne***, w tym fizyczne, psychiczne, społeczne lub ekonomiczne***.

(6) Biorąc pod uwagę istotny wpływ, jaki AI może mieć na społeczeństwo, oraz potrzebę budowania zaufania, AI i jej ramy regulacyjne należy rozwijać zgodnie z wartościami Unii zapisanymi w art. 2 Traktatu o Unii Europejskiej (TUE), prawami podstawowymi i wolnościami zapisanymi w traktatach i w świetle art. 6 TUE – w Karcie. Warunkiem wstępnym jest to, by AI była technologią ukierunkowaną na człowieka. Powinna ona służyć jako narzędzie dla ludzi, którego ostatecznym celem jest zwiększenie dobrostanu człowieka.

(7) W celu zapewnienia spójnego i wysokiego poziomu ochrony interesów publicznych w dziedzinie zdrowia, bezpieczeństwa i praw podstawowych należy ustanowić wspólne przepisy dla systemów AI wysokiego ryzyka. Przepisy te powinny być zgodne z Kartą, niedyskryminacyjne i zgodne z międzynarodowymi zobowiązaniami handlowymi Unii. Powinny również uwzględniać Europejską deklarację praw i zasad cyfrowych w cyfrowej dekadzie oraz Wytyczne w zakresie etyki dotyczące godnej zaufania AI grupy ekspertów wysokiego szczebla ds. AI.

(8) Unijne ramy prawne określające zharmonizowane przepisy dotyczące AI są zatem niezbędne, by wspierać rozwój, wykorzystywanie i upowszechnianie AI na rynku wewnętrznym, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony interesów publicznych, takich jak zdrowie i bezpieczeństwo oraz ochrona praw podstawowych***, w tym demokracji, praworządności i ochrony środowiska,*** uznanych i chronionych przez prawo Unii. Aby osiągnąć ten cel, należy ustanowić przepisy regulujące wprowadzanie do obrotu, oddawanie do użytku ***i wykorzystywanie*** niektórych systemów AI, zapewniając w ten sposób sprawne funkcjonowanie rynku wewnętrznego i obejmując te systemy zasadą swobodnego przepływu towarów i usług. ***Przepisy te powinny być jasne i solidne pod względem ochrony praw podstawowych, sprzyjać nowym innowacyjnym rozwiązaniom, umożliwiać tworzenie europejskiego ekosystemu podmiotów publicznych i prywatnych opracowujących systemy AI zgodnie z wartościami Unii oraz pozwalać realizować potencjał transformacji cyfrowej we wszystkich regionach Unii.*** Ustanawiając te przepisy***, a także środki wspierające innowacje, ze szczególnym uwzględnieniem małych i średnich przedsiębiorstw (MŚP), w tym przedsiębiorstw typu start-up,*** niniejsze rozporządzenie wspiera realizację celu, jakim jest ***promowanie europejskiego ukierunkowanego na człowieka podejścia do AI i*** znalezienie się przez UE w światowej czołówce, jeśli chodzi o rozwój bezpiecznej, godnej zaufania i etycznej ▌ AI, zgodnie z konkluzjami Rady Europejskiej[5], oraz zapewnia ochronę zasad etycznych, zgodnie z wyraźnym żądaniem Parlamentu Europejskiego[6].

---

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

6 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).

(9) Zharmonizowane przepisy mające zastosowanie do wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów AI wysokiego ryzyka należy ustanowić zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008[7], decyzją Parlamentu Europejskiego i Rady nr 768/2008/WE[8] oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/1020[9] („nowe ramy prawne"). ***Zharmonizowane przepisy określone w niniejszym rozporządzeniu powinny mieć zastosowanie we wszystkich sektorach i – zgodnie z nowymi ramami prawnymi – powinny pozostawać bez uszczerbku dla obowiązującego prawa Unii, w szczególności w zakresie ochrony danych, ochrony konsumentów, praw podstawowych, zatrudnienia i ochrony pracowników oraz bezpieczeństwa produktów, wobec którego to prawa niniejsze rozporządzenie ma charakter uzupełniający.***

---

7 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).

8 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).

9 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. 1–44).

W związku z tym wszystkie prawa i środki ochrony prawnej przysługujące na mocy prawa Unii konsumentom i innym osobom, na które systemy AI mogą mieć negatywny wpływ, w tym w odniesieniu do odszkodowania za ewentualne szkody zgodnie z dyrektywą Rady 85/374/EWG[10], pozostają nienaruszone i mają pełne zastosowanie. Ponadto w kontekście zatrudnienia i ochrony pracowników niniejsze rozporządzenie nie powinno zatem mieć wpływu na prawo Unii w dziedzinie polityki społecznej oraz na krajowe prawo pracy, zgodnie z prawem Unii, dotyczące warunków zatrudnienia i pracy, w tym bezpieczeństwa i higieny pracy, oraz stosunków między pracodawcami a pracownikami. Niniejsze rozporządzenie nie powinno mieć też wpływu na korzystanie z praw podstawowych uznanych w państwach członkowskich i na szczeblu Unii, w tym z prawa do strajku czy swobody podejmowania strajku lub innych działań objętych szczególnymi systemami stosunków pracy w państwach członkowskich, ani na korzystanie z prawa do negocjowania, zawierania i egzekwowania układów zbiorowych lub podejmowania działań zbiorowych zgodnie z prawem krajowym.

---

10 Dyrektywa Rady 85/374/EWG z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe (85/374/EWG) (Dz.U. L 210 z 7.8.1985, s. 29).

Niniejsze rozporządzenie nie powinno mieć wpływu na przepisy mające na celu poprawę warunków pracy świadczonej za pośrednictwem platform internetowych określone w dyrektywie Parlamentu Europejskiego i Rady (UE) 2024/...[11 +]. Ponadto niniejsze rozporządzenie ma na celu zwiększenie skuteczności takich istniejących praw i środków ochrony prawnej poprzez ustanowienie szczegółowych wymogów i obowiązków, w tym w zakresie przejrzystości, dokumentacji technicznej i rejestrowania zdarzeń w ramach systemów AI. Co więcej obowiązki nałożone na mocy niniejszego rozporządzenia na różnych operatorów uczestniczących w łańcuchu wartości AI powinny mieć zastosowanie bez uszczerbku dla prawa krajowego, zgodnie z prawem Unii, skutkującego ograniczeniem wykorzystania określonych systemów AI, gdy prawo to nie wchodzi w zakres niniejszego rozporządzenia lub służy innym niż cele niniejszego rozporządzenia uzasadnionym celom interesu publicznego. Na przykład niniejsze rozporządzenie nie powinno mieć wpływu na krajowe prawo pracy i przepisy dotyczące ochrony małoletnich (tj. osób poniżej 18. roku życia), uwzględniające opracowany przez ONZ komentarz ogólny nr 25 z 2021 r. w sprawie praw dziecka w środowisku cyfrowym, w zakresie w jakim prawo to i te przepisy nie dotyczą konkretnie systemów AI i służą innym uzasadnionym celom interesu publicznego.

---

11 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/... z dnia... w sprawie poprawy warunków pracy za pośrednictwem platform internetowych (Dz.U. L..., ELI: ...).

\+ Dz.U.: Proszę wstawić do tekstu numer dyrektywy PE XX/RR (2021/0414 (COD)) oraz uzupełnić odpowiadający przypis.

(10) Podstawowe prawo do ochrony danych osobowych jest gwarantowane w szczególności przez rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[12] i (UE) 2018/1725[13] oraz dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680[14]. Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE[15] dodatkowo chroni życie prywatne i poufność komunikacji, w tym określając warunki wszelkiego przechowywania danych osobowych i nieosobowych w urządzeniach końcowych oraz warunki uzyskiwania dostępu do tych danych z urządzeń końcowych. Te unijne akty prawne stanowią podstawę zrównoważonego i odpowiedzialnego przetwarzania danych, np. kiedy zbiory danych zawierają mieszankę danych osobowych i nieosobowych. Celem niniejszego rozporządzenia nie jest wpływanie na stosowanie obowiązującego prawa Unii regulującego przetwarzanie danych osobowych, w tym na zadania i uprawnienia niezależnych organów nadzoru właściwych do monitorowania zgodności z tymi instrumentami.

---

12 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).

13 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).

14 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 (Dz.U. L 119 z 4.5.2016, s. 89).

15 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

W zakresie, w jakim projektowanie, opracowywanie lub wykorzystywanie systemów AI wiąże się z przetwarzaniem danych osobowych, niniejsze rozporządzenie nie wpływa też na wynikające z unijnego lub krajowego prawa w dziedzinie ochrony danych osobowych obowiązki dostawców i podmiotów stosujących systemy AI, którzy pełnią funkcję administratorów danych lub podmiotów przetwarzających. Należy również wyjaśnić, że osoby, których dane dotyczą, zachowują wszystkie prawa i gwarancje przyznane im na mocy takiego prawa Unii, w tym prawa związane z całkowicie zautomatyzowanym podejmowaniem decyzji w indywidualnych przypadkach, w tym z profilowaniem. Ustanowione na podstawie niniejszego rozporządzenia zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów AI powinny ułatwiać skuteczne wdrażanie i umożliwiać korzystanie przez osoby, których dane dotyczą, z praw i innych środków ochrony prawnej zagwarantowanych na podstawie prawa Unii dotyczącego ochrony danych osobowych i innych praw podstawowych.

(11) Niniejsze rozporządzenie nie powinno naruszać przepisów dotyczących odpowiedzialności usługodawców będących pośrednikami, określonych w dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady[16].

---

16 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).

(12) Pojęcie **„**systemu AI***” w niniejszym rozporządzeniu*** powinno być jasno zdefiniowane i ***ściśle powiązane z pracami organizacji międzynarodowych zajmujących się AI***, aby zapewnić pewność prawa***, ułatwiać międzynarodową konwergencję i szeroką akceptację,*** przy jednoczesnym zapewnieniu elastyczności umożliwiającej dostosowanie się do ***szybkiego*** rozwoju technologicznego ***w tej dziedzinie. Ponadto*** pojęcie to powinno opierać się na ***kluczowych*** cechach ***systemów AI, które odróżniają je od prostszych tradycyjnych systemów oprogramowania lub podejść do programowania, i nie powinno obejmować systemów opartych na zasadach określonych wyłącznie przez osoby fizyczne w celu automatycznego wykonywania operacji. Jedną z kluczowych cech systemów AI jest ich zdolność do wnioskowania. Ta zdolność do wnioskowania odnosi się do procesu uzyskiwania*** wyników, takich jak ***predykcje, treści***, zalecenia lub decyzje, które ***mogą*** wpływać na środowisko ***fizyczne i wirtualne, oraz do zdolności systemów AI do uzyskiwania modeli lub algorytmów na podstawie informacji wejściowych lub danych. Techniki, które umożliwiają wnioskowanie podczas tworzenia systemu AI, obejmują mechanizmy uczenia się maszyn, które na podstawie danych uczą się, jak osiągnąć określone cele, oraz podejścia oparte na logice i wiedzy, które polegają na wnioskowaniu na podstawie zakodowanej wiedzy lub symbolicznego przedstawienia zadania, które należy rozwiązać. Zdolność systemu AI do wnioskowania wykracza poza podstawowe przetwarzanie danych i umożliwia uczenie się, rozumowanie lub modelowanie. Termin „maszynowy” odnosi się do faktu, że systemy AI działają z wykorzystaniem maszyn.***

Odniesienie do wyraźnych lub dorozumianych celów podkreśla, że systemy AI mogą działać według jasno określonych lub dorozumianych celów. Cele systemu AI ***mogą różnić się od przeznaczenia systemu AI w*** określonym ***kontekście. Na potrzeby niniejszego rozporządzenia środowiska*** należy ***rozumieć jako konteksty, w których działają systemy AI, natomiast wyniki generowane przez system AI odzwierciedlają różne funkcje wykonywane przez systemy AI i obejmują predykcje, treści, zalecenia lub decyzje. Systemy sztucznej inteligencji są zaprojektowane tak, aby działały z różnym poziomem autonomii, co oznacza, że są w pewnym stopniu niezależne od zaangażowania ze strony człowieka i zdolne do działania bez interwencji człowieka. Zdolność adaptacji, jaką system AI może wykazać po jego wdrożeniu, odnosi się do zdolności do samouczenia się, która umożliwia zmianę systemu w czasie jego użytkowania. Systemy AI mogą 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)***.

(13) Pojęcie „podmiotu stosującego AI", o którym mowa w niniejszym rozporządzeniu, należy interpretować jako każdą osobę fizyczną lub prawną, w tym organ publiczny, agencję lub inny podmiot, która korzysta z systemu AI i która odpowiada za to wykorzystywanie, oprócz przypadków gdy stosowanie systemu AI odbywa się w ramach osobistej działalności pozazawodowej. W zależności od rodzaju systemu AI korzystanie z takiego systemu może mieć wpływ na osoby inne niż podmiot stosujący AI.

(14) Pojęcie **„**danych biometrycznych**”** stosowane w niniejszym rozporządzeniu ▌ należy interpretować ***w świetle*** pojęcia danych biometrycznych zdefiniowanego w art. 4 pkt 14 rozporządzenia (UE) 2016/679, art. 3 pkt 18 rozporządzenia (UE) 2018/1725 i art. 3 pkt 13 dyrektywy (UE) 2016/680***. Dane biometryczne mogą umożliwiać uwierzytelnianie, identyfikację lub kategoryzację osób fizycznych oraz rozpoznawanie emocji osób fizycznych.***

(15) Pojęcie „identyfikacji biometrycznej”, o którym mowa w niniejszym rozporządzeniu, należy zdefiniować jako automatyczne rozpoznawanie fizycznych, fizjologicznych i behawioralnych cech człowieka, takich jak twarz, ruch gałek ocznych, kształt ciała, głos, właściwości mowy, chód, postawa, tętno, ciśnienie krwi, zapach, sposób pisania na klawiaturze, w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z przechowywanymi w referencyjnej bazie danych danymi biometrycznymi osób fizycznych, niezależnie od tego, czy osoba ta wyraziła na to zgodę. Do tej kategorii nie należą systemy AI przeznaczone do weryfikacji biometrycznej, która obejmuje uwierzytelnianie, prowadzonej jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie w celu uzyskania dostępu do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń.

(16) Pojęcie kategoryzacji biometrycznej, o którym mowa w niniejszym rozporządzeniu, należy zdefiniować jako przypisywanie osób fizycznych do określonych kategorii na podstawie danych biometrycznych tych osób. Takie szczególne kategorie mogą odnosić się do takich aspektów jak płeć, wiek, kolor włosów, kolor oczu, tatuaże, cechy dotyczące zachowania bądź osobowości, język, religia, przynależność do mniejszości narodowej, orientacja seksualna lub polityczna. Nie obejmuje to systemów kategoryzacji biometrycznej, które pełnią jedynie funkcję pomocniczą nieodłącznie związaną z inną usługą komercyjną, co oznacza, że z obiektywnych względów technicznych funkcja ta nie może być wykorzystywana bez usługi głównej, a włączenie takiej funkcji lub funkcjonalności nie jest sposobem na obejście stosowania przepisów niniejszego rozporządzenia. Przykładem wykorzystania takiej funkcji pomocniczej mogą być filtry klasyfikujące cechy twarzy lub ciała wykorzystywane na internetowych platformach handlowych, ponieważ można je stosować wyłącznie w powiązaniu z usługą główną, która polega na sprzedaży produktu przy jednoczesnym umożliwieniu konsumentowi uzyskania wyobrażenia, jak produkt będzie się na nim prezentował, by podjąć decyzję o zakupie. Filtry stosowane w internetowych serwisach społecznościowych, które kategoryzują cechy twarzy lub ciała, aby umożliwić użytkownikom dodawanie lub modyfikowanie zdjęć lub filmów wideo, można również uznać za funkcję pomocniczą, ponieważ filtry takie nie mogą być stosowane bez usługi głównej polegającej na udostępnianiu treści online w ramach serwisu społecznościowego.

(17) Pojęcie **„**systemu zdalnej identyfikacji biometrycznej**”**, o którym mowa w niniejszym rozporządzeniu, należy zdefiniować funkcjonalnie jako system AI służący do identyfikacji osób fizycznych ***bez aktywnego udziału tych osób, co do zasady*** na odległość, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych***, niezależnie od konkretnej stosowanej technologii oraz konkretnych wykorzystywanych procesów lub rodzajów danych biometrycznych. Takie systemy zdalnej identyfikacji biometrycznej są zwykle wykorzystywane do jednoczesnego obserwowania wielu osób lub ich zachowania w celu znacznego ułatwienia identyfikacji osób fizycznych*** bez ***ich aktywnego udziału. Do tej kategorii nie należą systemy AI przeznaczone do weryfikacji biometrycznej, która obejmuje uwierzytelnianie, prowadzonej jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie w celu uzyskania dostępu do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń. Wyłączenie to jest uzasadnione faktem, że takie systemy w niewielkim stopniu mogą wpływać na prawa podstawowe osób fizycznych w porównaniu z systemami zdalnej identyfikacji biometrycznej, które mogą być wykorzystywane do przetwarzania danych*** biometrycznych ***dużej liczby osób bez ich aktywnego udziału***. 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 AI w czasie rzeczywistym poprzez wprowadzanie niewielkich opóźnień. Systemy identyfikacji w czasie rzeczywistym obejmują wykorzystanie materiału rejestrowanego „na żywo” lub „niemal na żywo”, 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, które to materiały zostały wytworzone, zanim użyto systemu identyfikacji w stosunku do danej osoby fizycznej.

(18) Pojęcie „systemu rozpoznawania emocji”, o którym mowa w niniejszym rozporządzeniu, należy zdefiniować jako system AI służący do rozpoznawania emocji lub zamiarów osób fizycznych na podstawie danych biometrycznych tych osób, lub wyciągania wniosków odnośnie do tych emocji lub zamiarów. Pojęcie to dotyczy emocji lub zamiarów, takich jak radość, smutek, złość, zdziwienie, obrzydzenie, zakłopotanie, podekscytowanie, wstyd, pogarda, satysfakcja i rozbawienie. Nie obejmuje stanów fizycznych, takich jak ból lub zmęczenie – dotyczy to na przykład systemów stosowanych do wykrywania poziomu zmęczenia zawodowych pilotów lub kierowców w celu zapobiegania wypadkom. Nie obejmuje również samego wykrywania łatwych do zauważenia form wyrazu, gestów lub ruchów, chyba że wykorzystuje się je do identyfikacji lub wnioskowania na temat emocji. Te formy wyrazu mogą obejmować podstawowe rodzaje wyrazu twarzy, takie jak grymas lub uśmiech, gesty, takie jak ruch rąk, ramion lub głowy, albo cechy głosu danej osoby, takie jak podniesiony ton lub szept.

(19) Do celów niniejszego rozporządzenia pojęcie „przestrzeni publicznej” należy rozumieć jako odnoszące się do każdego miejsca fizycznego, które jest dostępne dla ***nieokreślonej liczby osób fizycznych i*** niezależnie od tego, czy dane miejsce jest własnością prywatną czy publiczną, a ***także niezależnie od rodzaju działalności, dla której się ją wykorzystuje, takiej jak działalność handlowa (np. sklepy, restauracje, kawiarnie), działalność usługowa (np. banki, działalność zawodowa, hotelarstwo), działalność sportowa (np. baseny, sale do ćwiczeń, stadiony), działalność transportowa (np. dworce autobusowe i kolejowe, stacje metra, lotniska, środki transportu), działalność rozrywkowa (np. kina, teatry, muzea, sale koncertowe i konferencyjne) lub miejsca służące wypoczynkowi lub innym celom (np. drogi publiczne i place, parki, lasy i place zabaw)***. ***Miejsce należy uznać za przestrzeń publiczną również wtedy, gdy niezależnie od potencjalnych ograniczeń w zakresie pojemności lub bezpieczeństwa, dostęp do niego podlega*** pewnym ***określonym z góry*** warunkom – ***które mogą zostać spełnione przez nieokreśloną liczbę osób –*** takich jak ***zakup biletu wstępu lub biletu na przejazd, uprzednia rejestracja lub osiągnięcie określonego wieku. Danego miejsca nie należy natomiast uznawać za przestrzeń publiczną, jeśli dostęp do niego ograniczony jest do konkretnych i określonych osób fizycznych na mocy prawa Unii lub prawa krajowego bezpośrednio związanego z bezpieczeństwem publicznym lub ochroną publiczną lub w wyniku wyraźnego wyrażenia woli przez osobę posiadającą odpowiednie uprawnienia związane z takim miejscem. Faktyczna możliwość samego dostępu (taka jak niezamknięte drzwi, otwarta bramka w ogrodzeniu)*** nie ***oznacza,*** że dane ***miejsce stanowi*** przestrzeń publiczną***, jeśli istnieją wskazania lub okoliczności sugerujące inaczej (takie jak znaki zakazujące dostępu lub go ograniczające). Tereny przedsiębiorstw i fabryk, a także biura i miejsca pracy, do których dostęp powinni mieć wyłącznie*** odpowiedni ***pracownicy i usługodawcy, to miejsca które nie stanowią przestrzeni publicznej. Do przestrzeni publicznej nie zaliczają się więzienia ani strefy kontroli granicznej. Niektóre miejsca mogą składać się z przestrzeni publicznych i niepublicznych,*** takie jak ***hol w prywatnym budynku mieszkalnym prowadzący do gabinetu lekarskiego lub lotnisko. Przestrzenie internetowe również nie są objęte niniejszym rozporządzeniem, ponieważ nie są to przestrzenie fizyczne***. To, czy dana przestrzeń jest dostępna publicznie, powinno być jednak ustalane indywidualnie w każdym przypadku, z uwzględnieniem specyfiki danej sytuacji.

(20) ***Dostawców, podmioty stosujące AI i osoby, na które AI ma wpływ, należy wyposażyć w niezbędne kompetencje w zakresie AI umożliwiające im podejmowanie świadomych decyzji w odniesieniu do systemów AI, co pozwoli czerpać największe korzyści z systemów AI, a jednocześnie chronić prawa podstawowe, zdrowie i bezpieczeństwo oraz sprawować kontrolę demokratyczną. Kompetencje te mogą różnić się w zależności od danego kontekstu i mogą obejmować rozumienie prawidłowego stosowania elementów technicznych na etapie opracowywania systemu AI, rozumienie środków, które mają być stosowane podczas jego wykorzystywania, odpowiednich sposobów interpretacji wyników działania systemu AI oraz, w przypadku osób, na które AI ma wpływ – wiedzę niezbędną do zrozumienia, jaki wpływ będą miały na nie decyzje podejmowane przy pomocy AI. W kontekście stosowania niniejszego rozporządzenia kompetencje w zakresie AI powinny oznaczać, że wszystkie odpowiednie podmioty w łańcuchu wartości AI będą posiadać wiedzę konieczną do zapewnienia odpowiedniej zgodności z przepisami rozporządzenia i ich prawidłowego egzekwowania. Ponadto szerokie wdrażanie środków rozwijających kompetencje w zakresie AI oraz wprowadzanie odpowiednich działań następczych mogłyby przyczynić się do poprawy warunków pracy, a w ostatecznym rozrachunku wsparłyby konsolidację i oparte na innowacji dążenie do godnej zaufania AI w Unii. Europejska Rada ds. Sztucznej Inteligencji (Rada ds. AI) powinna wspierać Komisję w promowaniu narzędzi rozwijających kompetencje w zakresie AI, świadomości społecznej oraz zrozumienia korzyści, ryzyka, zabezpieczeń, praw i obowiązków związanych z korzystaniem z systemów AI. We współpracy z odpowiednimi zainteresowanymi stronami Komisja i państwa członkowskie powinny ułatwiać opracowywanie dobrowolnych kodeksów postępowania w celu podnoszenia kompetencji w zakresie AI wśród osób zajmujących się opracowywaniem, eksploatacją i wykorzystywaniem AI.***

(21) 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 AI w sposób niedyskryminacyjny, niezależnie od tego, czy mają oni siedzibę w Unii, czy w państwie trzecim, oraz do ***podmiotów stosujących*** systemy AI mających siedzibę w Unii.

(22) Ze względu na swój cyfrowy charakter niektóre systemy AI 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 operatorowi mającemu siedzibę w państwie trzecim określone usługi w związku z działaniem, które ma być wykonywane przez system AI, który zostałby zakwalifikowany jako system wysokiego ryzyka ▌. W takich okolicznościach system AI wykorzystywany w państwie trzecim przez operatora mógłby przetwarzać dane, które legalnie zgromadzono w Unii i przekazano poza Unię, oraz przekazywać zlecającemu operatorowi z Unii wynik przetwarzania tych danych przez system AI, natomiast sam system AI 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 podmiotów stosujących*** systemy AI, którzy mają siedzibę w państwie trzecim, w zakresie, w jakim wyniki działania tych systemów ***są przeznaczone do*** wykorzystywania w Unii.

Aby uwzględnić jednak istniejące ustalenia i szczególne potrzeby w zakresie ***przyszłej*** 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 ***współpracy lub*** na mocy zawartych na szczeblu unijnym lub krajowym umów międzynarodowych o współpracy organów ścigania i wymiarów sprawiedliwości z Unią lub jej państwami członkowskimi, ***pod warunkiem zapewnienia przez to państwo trzecie lub organizacje międzynarodowe odpowiednich zabezpieczeń w odniesieniu do ochrony podstawowych praw i wolności jednostek. W stosownych przypadkach może to obejmować działania podmiotów, którym państwa trzecie powierzyły wykonywanie szczególnych zadań w ramach wsparcia ścigania przestępstw i współpracy wymiarów sprawiedliwości. Takie ramy współpracy lub*** umowy zostały ***ustanowione*** dwustronnie między państwami członkowskimi a państwami trzecimi lub między Unią Europejską, Europolem i innymi agencjami Unii a państwami trzecimi i organizacjami międzynarodowymi. ***Organy właściwe do sprawowania nadzoru nad organami ścigania i organami sądowymi na mocy niniejszego rozporządzenia powinny ocenić, czy te ramy współpracy lub umowy międzynarodowe zawierają odpowiednie zabezpieczenia w odniesieniu do ochrony podstawowych praw i wolności jednostek. Będące odbiorcami organy państw członkowskich oraz będące odbiorcami instytucje, organy i jednostki organizacyjne Unii korzystające z takich wyników w Unii pozostają odpowiedzialne za zapewnienie zgodności ich stosowania z prawem Unii. W przypadku zmiany takich umów międzynarodowych lub zawierania nowych w przyszłości umawiające się strony powinny dołożyć wszelkich starań, by dostosować takie umowy do wymogów niniejszego rozporządzenia.***

(23) Niniejsze rozporządzenie powinno mieć również zastosowanie do instytucji, organów i jednostek organizacyjnych Unii, gdy działają one jako dostawca systemu AI lub ***podmiot stosujący system AI***. ▌

(24) Jeżeli i w zakresie, w jakim systemy AI wprowadza się do obrotu, oddaje do użytku lub korzysta się z nich ze zmianami lub bez zmian – do celów wojskowych, obronnych lub celów bezpieczeństwa narodowego, systemy te należy wyłączyć z zakresu stosowania niniejszego rozporządzenia niezależnie od tego, jaki podmiot wykonuje te działania – nie ma znaczenia na przykład, czy jest podmiotem publicznym czy prywatnym. Jeżeli chodzi o cele wojskowe i obronne, takie wyłączenie jest uzasadnione zarówno art. 4 ust. 2 TUE, jak i specyfiką polityki obronnej państw członkowskich i wspólnej polityki obronnej Unii objętej tytułem V rozdział 2 TUE, które podlegają prawu międzynarodowemu publicznemu stanowiącemu zatem bardziej odpowiednie ramy prawne dla regulacji systemów AI w kontekście stosowania śmiercionośnej siły i innych systemów AI w kontekście działań wojskowych i obronnych. W odniesieniu do celów bezpieczeństwa narodowego wyłączenie to jest uzasadnione zarówno faktem, że za bezpieczeństwo narodowe wyłączną odpowiedzialność ponoszą państwa członkowskie zgodnie z art. 4 ust. 2 TUE, jak i faktem, że działania w zakresie bezpieczeństwa narodowego mają szczególny charakter, wiążą się ze szczególnymi potrzebami operacyjnymi i że zastosowanie do nich mają szczególne przepisy krajowe. Jeżeli jednak system AI opracowany, wprowadzony do obrotu, oddany do użytku lub wykorzystywany do celów wojskowych, obronnych lub celów bezpieczeństwa narodowego jest tymczasowo lub na stałe wykorzystywany do innych celów, na przykład do celów cywilnych lub humanitarnych, do celów ścigania przestępstw lub bezpieczeństwa publicznego, system taki objęty zostanie zakresem stosowania niniejszego rozporządzenia.

W takim przypadku podmiot wykorzystujący taki system do celów inne niż cele wojskowe, obronne lub cele bezpieczeństwa narodowego powinien zapewnić zgodność systemu z niniejszym rozporządzeniem, chyba że system ten jest już z nim zgodny. Systemy AI wprowadzane do obrotu lub oddawane do użytku do celu stanowiącego podstawę wyłączenia, tzn. celu wojskowego, obronnego lub celu bezpieczeństwa narodowego, oraz do jednego lub kilku celów nieobjętych wyłączeniem, takich jak cele cywilne lub ściganie przestępstw, są objęte zakresem niniejszego rozporządzenia i dostawcy tych systemów powinni zapewnić zgodność z niniejszym rozporządzeniem. W takich przypadkach fakt, że system AI może wchodzić w zakres niniejszego rozporządzenia, nie powinien mieć wpływu na możliwość wykorzystywania – przez podmioty prowadzące działania dotyczące bezpieczeństwa narodowego, działania obronne i wojskowe, bez względu na rodzaj podmiotu prowadzącego te działania – systemów AI do celów bezpieczeństwa narodowego, celów wojskowych i obronnych, których wykorzystanie jest wyłączone z zakresu niniejszego rozporządzenia. System AI wprowadzany do obrotu do celów cywilnych lub w celu ścigania przestępstw, który jest wykorzystywany ze zmianami lub bez zmian do celów wojskowych, obronnych lub do celów bezpieczeństwa narodowego, nie powinien być objęty zakresem niniejszego rozporządzenia, bez względu na rodzaj podmiotu prowadzącego działania związane z tymi celami.

(25) ***Niniejsze rozporządzenie powinno wspierać innowacje, szanować wolność nauki i nie powinno osłabiać działalności badawczo-rozwojowej. Należy zatem wyłączyć z jego zakresu systemy i modele AI opracowane i oddane do użytku wyłącznie do celów badań naukowych i rozwoju. Ponadto należy zapewnić, aby niniejsze rozporządzenie nie wpływało w żaden inny sposób na badania naukowe i działalność rozwojową dotyczące systemów lub modeli AI przed wprowadzeniem tych systemów lub modeli do obrotu lub oddaniem do użytku. Przepisy niniejszego rozporządzenia nie powinny mieć również zastosowania do ukierunkowanej na produkty działalności badawczej, testowej i rozwojowej dotyczącej systemów lub modeli AI przed oddaniem tych systemów i modeli do użytku lub wprowadzaniem do obrotu. Pozostaje to bez uszczerbku dla obowiązku przestrzegania niniejszego rozporządzenia, gdy system AI objęty zakresem niniejszego rozporządzenia jest wprowadzany do obrotu lub oddawany do użytku w wyniku takiej działalności badawczo-rozwojowej, oraz dla stosowania przepisów dotyczących piaskownic regulacyjnych i testów w warunkach rzeczywistych. Ponadto bez uszczerbku dla wyłączenia dotyczącego systemów AI opracowanych i oddanych do użytku wyłącznie do celów badań naukowych i rozwoju, wszelkie inne systemy AI, które mogą być wykorzystywane do prowadzenia wszelkiej działalności badawczo-rozwojowej, powinny podlegać przepisom niniejszego rozporządzenia. W każdym przypadku wszelka działalność badawczo-rozwojowa powinna być prowadzona zgodnie z uznanymi normami etycznymi i zawodowymi dotyczącymi badań naukowych oraz zgodnie z mającym zastosowanie prawem Unii.***

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

(27) Chociaż podstawą proporcjonalnego i skutecznego zestawu wiążących przepisów jest podejście oparte na analizie ryzyka, należy przypomnieć Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji z 2019 r. opracowane przez niezależną grupę ekspertów wysokiego szczebla ds. AI powołaną przez Komisję. W tych wytycznych grupa ekspertów wysokiego szczebla ds. AI opracowała siedem niewiążących zasad etycznych dotyczących AI, które mają pomóc zapewnić, aby AI była godna zaufania i zgodna z normami etycznymi. Te siedem zasad to: przewodnia i nadzorcza rola człowieka; techniczna solidność i bezpieczeństwo; ochrona prywatności i zarządzanie danymi; przejrzystość; różnorodność, niedyskryminacja i sprawiedliwość; dobrostan społeczny i środowiskowy oraz odpowiedzialność. Bez uszczerbku dla prawnie wiążących wymogów niniejszego rozporządzenia i wszelkich innych mających zastosowanie przepisów prawa Unii, wspomniane wytyczne przyczyniają się do opracowania spójnej, wiarygodnej i ukierunkowanej na człowieka AI, zgodnie z Kartą i wartościami, na których opiera się Unia. Zgodnie z wytycznymi tej grupy „przewodnia i nadzorcza rola człowieka" oznacza, że systemy AI opracowuje się i wykorzystuje jako narzędzia służące ludziom, szanujące godność ludzką i autonomię osobistą oraz działające w sposób, który może być odpowiednio kontrolowany i nadzorowany przez człowieka.

Techniczna solidność i bezpieczeństwo oznaczają, że systemy AI opracowuje się i wykorzystuje w taki sposób, by okazały się wytrzymałe w przypadku wystąpienia problemów oraz odporne na próby zmiany ich wykorzystania lub działania, co pozwoli zapobiec bezprawnemu wykorzystaniu przez osoby trzecie i zminimalizować niezamierzone szkody. Ochrona prywatności i zarządzanie danymi oznaczają, że systemy AI opracowuje się i wykorzystuje zgodnie z przepisami dotyczącymi prywatności i ochrony danych, przy czym przetwarzanie danych spełnia wysokie standardy pod względem jakości i integralności. Przejrzystość oznacza, że systemy AI opracowuje się i wykorzystuje w sposób umożliwiający odpowiednią identyfikowalność i wytłumaczalność, jednocześnie informując ludzi o tym, że komunikują się z systemem AI lub podejmują z nim interakcję, a także należycie informując podmioty stosujące AI o możliwościach i ograniczeniach tego systemu AI, a osoby, na które AI ma wpływ, o przysługujących im prawach. Różnorodność, niedyskryminacja i sprawiedliwość oznaczają, że systemy AI opracowuje się i wykorzystuje w sposób, który angażuje różne podmioty i propaguje równy dostęp, równouprawnienie płci i różnorodność kulturową, jednocześnie unikając dyskryminujących skutków i niesprawiedliwej stronniczości, których zakazują prawo Unii lub prawo krajowe. Dobrostan społeczny i środowiskowy oznacza, że systemy AI opracowuje się i wykorzystuje w sposób zrównoważony, przyjazny dla środowiska i przynoszący korzyści wszystkim ludziom, jednocześnie monitorując i oceniając długoterminowy wpływ tych systemów na jednostkę, społeczeństwo i demokrację. Stosowanie tych zasad powinno w miarę możliwości znaleźć odzwierciedlenie w projektowaniu i wykorzystywaniu modeli AI. Zasady te powinny w każdym przypadku stanowić fundament przy opracowywaniu kodeksów postępowania na podstawie niniejszego rozporządzenia. Wszystkie zainteresowane strony, w tym przedstawicieli przemysłu, środowisko akademickie, społeczeństwo obywatelskie i organizacje normalizacyjne, zachęca się, by przy opracowywaniu dobrowolnych najlepszych praktyk i norm uwzględniali odpowiednio wyżej wymienione zasady etyczne.

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

(29) ***Techniki manipulacyjne oparte na sztucznej inteligencji mogą być wykorzystywane w celu nakłaniania osób do niepożądanych zachowań lub w celu wprowadzania ich w błąd poprzez skłanianie ich do podejmowania decyzji w sposób, który podważa i ogranicza ich autonomię, decyzyjność i swobodę wyboru.*** Wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie niektórych systemów AI ***w celu lub ze skutkiem istotnego zniekształcenia*** ludzkiego zachowania, w związku z czym mogą wystąpić ***poważne szkody, w szczególności mające wystarczająco istotny niepożądany wpływ na zdrowie*** fizyczne***, psychiczne lub na interesy finansowe, są szczególnie niebezpieczne i w związku z tym*** powinny być zakazane. Systemy tego rodzaju wykorzystują elementy działające podprogowo, ***takie jak bodźce dźwiękowe, bodźce będące obrazami lub materiałami wideo, których*** nie można dostrzec***, ponieważ bodźce takie wykraczają poza świadomą ludzką percepcję, lub stosują inne techniki manipulacyjne lub wprowadzające w błąd, które podważają lub ograniczają autonomię człowieka, decyzyjność lub swobodę wyboru w taki sposób, że osoby narażone na działanie takich systemów nie są świadome lub nawet jeśli są świadome, zostają wprowadzone w błąd lub nie są w stanie sprawować nad nimi kontroli ani im się sprzeciwić. Przyczyniać się do tego mogą na przykład interfejsy maszyna-mózg lub rzeczywistość wirtualna, ponieważ pozwalają one na większą kontrolę nad tym, jakie bodźce są przedstawiane osobom, do tego stopnia, że mogą one istotnie zniekształcać zachowanie tych osób w sposób znacząco szkodliwy. Ponadto systemy AI mogą również w inny sposób*** wykorzystywać słabości ***danej osoby lub określonej grupy osób*** ze względu na ich wiek, ***niepełnosprawność w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/882[17] lub szczególną sytuację społeczną lub ekonomiczną, która może sprawić, że osoby te, takie jak osoby żyjące w skrajnym ubóstwie, osoby z mniejszości etnicznych lub religijnych, będą bardziej narażone na wykorzystywanie.***

---

17 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z dnia 17 kwietnia 2019 r. w sprawie wymogów dostępności produktów i usług (Dz.U. L 151 z 7.6.2019, s. 70).

Takie systemy AI mogą być wprowadzane do obrotu, oddawane do użytku lub wykorzystywane w ***celu lub ze skutkiem*** istotnego ***zniekształcenia*** zachowania danej osoby, oraz w sposób, który powoduje lub może z ***uzasadnionym prawdopodobieństwem*** spowodować ***poważną*** szkodę w odniesieniu do tej osoby lub innej osoby ***lub grupy osób, w tym szkody kumulujące się z biegiem czasu, i w związku z tym powinny być zakazane***. Nie można zakładać, że zaistniał zamiar ***zniekształcenia zachowania***, jeżeli zniekształcenie to ▌ wynika z czynników, które mają charakter zewnętrzny w stosunku do systemu AI i które są poza kontrolą dostawcy lub ***podmiotu stosującego AI, a zatem ani dostawca ani podmiot stosujący AI nie mogą ich racjonalnie przewidzieć ani im przeciwdziałać. W każdym razie nie ma znaczenia, czy dostawca lub podmiot stosujący AI mieli zamiar wyrządzić poważną szkodę, istotny jest fakt, że szkoda wynika z opartych na AI praktyk polegających na manipulacji lub wykorzystywaniu. Zakazy dotyczące takich praktyk w zakresie AI stanowią uzupełnienie przepisów zawartych w dyrektywie Parlamentu Europejskiego i Rady 2005/29/WE[18], w szczególności przepisu zakazującego stosowania we wszelkich okolicznościach nieuczciwych praktyk handlowych powodujących dla konsumentów szkody ekonomiczne lub finansowe, niezależnie od tego, czy praktyki te stosuje się za pomocą systemów AI czy w innym kontekście. Zawarty w niniejszym rozporządzeniu zakaz praktyk polegających na manipulacji lub wykorzystywaniu nie powinien mieć wpływu na zgodne z prawem praktyki w kontekście leczenia, takie jak terapia psychologiczna w związku z chorobą psychiczną lub rehabilitacja fizyczna, gdy praktyki te są*** prowadzone zgodnie z ***mającymi zastosowanie prawem i*** normami ***medycznymi, na przykład za wyraźną zgodą danej osoby lub jej przedstawiciela prawnego. Ponadto powszechne i zasadne praktyki handlowe, na przykład w dziedzinie reklamy, które są zgodne z mającym zastosowanie prawem, nie powinny być same w sobie uznawane za szkodliwe, polegające na manipulacji praktyki z wykorzystaniem AI***.

---

18 Dyrektywa Parlamentu Europejskiego i Rady 2005/29/WE z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy Parlamentu Europejskiego i Rady 97/7/WE, 98/27/WE i 2002/65/WE oraz rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 2006/2004 (dyrektywa o nieuczciwych praktykach handlowych) (Dz.U. L 149 z 11.6.2005, s. 22).

(30) ***Należy zakazać stosowania systemów kategoryzacji biometrycznej, które opierają się na danych biometrycznych osób fizycznych, takich jak twarz lub odciski palców danej osoby, w celu wydedukowania lub wywnioskowania informacji na temat opinii politycznych, przynależności do związków zawodowych, przekonań religijnych lub filozoficznych, rasy, życia seksualnego lub orientacji seksualnej danej osoby. Zakaz ten nie powinien obejmować zgodnego z prawem etykietowania, filtrowania lub kategoryzacji zbiorów danych biometrycznych, pozyskanych zgodnie z prawem Unii lub prawem krajowym, według danych biometrycznych, takiego jak sortowanie obrazów według koloru włosów lub koloru oczu, które można na przykład wykorzystać w obszarze ścigania przestępstw.***

(31) Systemy AI, które umożliwiają prowadzenie wobec osób fizycznych przez podmioty publiczne ***lub prywatne*** scoringu obywateli ▌ , 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 AI oceniają lub klasyfikują ***osoby fizyczne lub grupy osób fizycznych*** na podstawie ***wielu punktów danych dotyczących*** ich zachowań społecznych w wielu kontekstach lub na podstawie znanych***, wywnioskowanych*** lub przewidywanych cech osobistych lub cech osobowości ***w określonych przedziałach czasowych***. Ocena społeczna wystawiona przez takie systemy AI 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. Należy zatem zakazać ***systemów AI, w których stosuje się takie niedopuszczalne praktyki scoringu obywateli, które przynoszą tak szkodliwe lub niekorzystne skutki***. ***Zakaz ten nie powinien mieć wpływu na legalne praktyki oceny osób fizycznych, które są stosowane w konkretnym celu zgodnie z prawem Unii i prawem krajowym.***

(32) Wykorzystanie systemów AI do zdalnej identyfikacji biometrycznej osób fizycznych w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw szczególnie ingeruje w prawa i wolności zainteresowanych osób, ponieważ może to wpływać na życie prywatne dużej części społeczeństwa, wywoływać poczucie stałego nadzoru i pośrednio zniechęcać do korzystania z wolności zgromadzeń i innych praw podstawowych. ***Techniczne niedokładności systemów AI przeznaczonych do zdalnej identyfikacji biometrycznej osób fizycznych mogą prowadzić do nieobiektywnych wyników i wywoływać skutki w postaci dyskryminacji. Takie ewentualne nieobiektywne wyniki i skutki w postaci dyskryminacji są szczególnie istotne w odniesieniu do wieku, pochodzenia etnicznego, rasy, płci lub niepełnosprawności.*** 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.

(33) Wykorzystanie tych systemów w celu ścigania przestępstw powinno zatem być zabronione, z wyjątkiem zamkniętej listy wąsko zdefiniowanych sytuacji, w których wykorzystanie to jest absolutnie konieczne do realizacji istotnego interesu publicznego, którego waga przeważa nad ryzykiem. Sytuacje te obejmują poszukiwanie ***określonych*** ofiar przestępstw ▌, w tym ***osób*** zaginionych; zapobieganie niektórym zagrożeniom życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu; oraz lokalizowanie ***lub identyfikowanie*** sprawców przestępstw lub podejrzanych o popełnienie przestępstw, o których mowa w załączniku do niniejszego rozporządzenia***, w przypadku gdy*** przestępstwa te podlegają w danym państwie członkowskim, zgodnie z jego prawem, karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej ***cztery*** lata. 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 ***przestępstwa te opierają się na wykazie*** 32 przestępstw wymienionych w decyzji ramowej Rady 2002/584/WSiSW***[19], biorąc pod uwagę,*** że niektóre z tych przestępstw 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 lokalizowania ***lub identyfikowania*** 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. ***Bezpośrednie zagrożenie życia lub bezpieczeństwa fizycznego osób fizycznych może również wynikać z poważnego zakłócenia funkcjonowania infrastruktury krytycznej zdefiniowanej w art. 2 pkt 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557[20], w przypadku gdy zakłócenie lub zniszczenie takiej infrastruktury krytycznej spowodowałoby bezpośrednie zagrożenie życia lub bezpieczeństwa fizycznego danej osoby, w tym poprzez poważną szkodę w dostarczaniu podstawowych dostaw dla ludności lub w wykonywaniu podstawowych funkcji państwa. Ponadto niniejsze rozporządzenie powinno utrzymać możliwość przeprowadzania przez organy ścigania, organy kontroli granicznej, organy imigracyjne lub organy azylowe kontroli tożsamości w obecności danej osoby zgodnie z warunkami określonymi w prawie Unii i prawie krajowym w odniesieniu do takich kontroli. W szczególności organy ścigania, organy kontroli granicznej, organy imigracyjne lub organy azylowe powinny mieć możliwość korzystania z systemów informacyjnych, zgodnie z prawem Unii lub prawem krajowym – w celu zidentyfikowania osób, które podczas kontroli tożsamości odmawiają identyfikacji lub nie są w stanie podać lub dowieść swojej tożsamości – bez konieczności uzyskiwania uprzedniego zezwolenia na podstawie niniejszego rozporządzenia. Może to na przykład dotyczyć osoby mającej związek z przestępstwem, która nie chce lub – w wyniku wypadku lub z powodu stanu zdrowia – nie jest w stanie ujawnić swojej tożsamości organom ścigania.***

---

19 ***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).***

20 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022, s. 164).

(34) W celu zapewnienia, aby systemy te były wykorzystywane w sposób odpowiedzialny i proporcjonalny, należy również zastrzec, że w każdej z tych 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 w celu ścigania przestępstw powinno ***mieć miejsce jedynie, by potwierdzić tożsamość konkretnej poszukiwanej osoby, i nie powinno wykraczać poza to, co jest bezwzględnie konieczne w odniesieniu do przedziału czasowego, a także zakresu geograficznego i podmiotowego***, z uwzględnieniem w szczególności dowodów lub wskazówek dotyczących zagrożeń, ofiar lub sprawcy. ***Wykorzystanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej powinno być dozwolone tylko wtedy, gdy właściwy organ ścigania przeprowadził ocenę skutków w zakresie praw podstawowych oraz, o ile niniejsze rozporządzenie nie stanowi inaczej, zarejestrował system w bazie danych, jak określono w niniejszym rozporządzeniu.*** Referencyjna baza danych osób powinna być odpowiednia dla każdego przypadku użycia w każdej z wyżej wymienionych sytuacji.

(35) Każde użycie systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw powinno podlegać wyraźnemu i szczegółowemu zezwoleniu wydanemu w danym państwie członkowskim przez organ sądowy lub niezależny ***wydający wiążące decyzje*** organ administracyjny. Takie zezwolenie należy co do zasady uzyskać przed rozpoczęciem korzystania ***z systemu AI w celu zidentyfikowania osoby lub osób. Wyjątki od tej zasady powinny być dozwolone*** w należycie uzasadnionych sytuacjach nadzwyczajnych, to znaczy w sytuacjach, w których potrzeba skorzystania z danego systemu jest na tyle duża, że uzyskanie zezwolenia przed rozpoczęciem korzystania z tego systemu AI jest faktycznie i obiektywnie niemożliwe. W takich sytuacjach nadzwyczajnych wykorzystanie takiego systemu AI powinno być ograniczone do absolutnie niezbędnego minimum i powinno podlegać odpowiednim zabezpieczeniom i warunkom określonym w prawie krajowym i sprecyzowanym przez sam organ ścigania w kontekście każdego przypadku nadzwyczajnego użycia. Ponadto organ ścigania powinien w takich sytuacjach ***zwrócić się o takie*** zezwolenie ▌, podając powody, dla których nie był w stanie wystąpić o nie wcześniej***, bez zbędnej zwłoki i nie później niż w ciągu 24 godzin. W przypadku odmowy udzielenia takiego zezwolenia wykorzystywanie systemów identyfikacji biometrycznej w czasie rzeczywistym powiązanych z tym zezwoleniem powinno zostać wstrzymane ze skutkiem natychmiastowym, a wszystkie dane związane z takim wykorzystaniem powinny zostać odrzucone i usunięte. Dane takie obejmują dane wejściowe uzyskane bezpośrednio przez system AI w trakcie korzystania z takiego systemu, a także związane z tym zezwoleniem rezultaty i wyniki uzyskane podczas tego wykorzystania. Powyższe nie powinno mieć zastosowania do danych wejściowych uzyskanych legalnie zgodnie z innymi unijnymi lub krajowymi przepisami. W każdym przypadku żadnej decyzji wywołującej niepożądane skutki prawne dla danej osoby nie należy podejmować wyłącznie na podstawie wyników uzyskanych z systemu zdalnej identyfikacji biometrycznej***.

(36) Aby umożliwić odpowiednim organom nadzoru rynku i krajowym organom ochrony danych wykonywanie ich zadań zgodnie z wymogami określonymi w niniejszym rozporządzeniu oraz w przepisach krajowych, należy powiadamiać je o każdym wykorzystaniu systemu identyfikacji biometrycznej w czasie rzeczywistym. Krajowe organy nadzoru rynku i krajowe organy ochrony danych, które otrzymały powiadomienie, powinny przedkładać Komisji roczne sprawozdanie na temat wykorzystania systemów identyfikacji biometrycznej w czasie rzeczywistym.

(37) Ponadto należy zapewnić, z zastosowaniem wyczerpujących ram 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. ***Takie przepisy krajowe należy zgłosić Komisji w ciągu 30 dni od ich przyjęcia.***

(38) Wykorzystanie systemów AI do zdalnej identyfikacji biometrycznej osób fizycznych w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw 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 ścigania przestępstw – 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 ściganie przestępstw, w tym przez właściwe organy, nie powinno być jednak objęte szczegółowymi ramami dotyczącymi takiego wykorzystywania w celu ścigania przestępstw, określonymi w niniejszym rozporządzeniu. Takie wykorzystywanie do celów innych niż ściganie przestępstw nie powinno zatem podlegać wymogowi uzyskania zezwolenia na mocy niniejszego rozporządzenia i obowiązujących szczegółowych przepisów prawa krajowego, które mogą stanowić podstawę ubiegania się o takie zezwolenie.

(39) Wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane ze stosowaniem systemów AI do identyfikacji biometrycznej, inne niż w związku z wykorzystywaniem systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw zgodnie z przepisami niniejszego rozporządzenia, ***powinno nadal spełniać wszystkie wymogi wynikające z art. 10 dyrektywy (UE) 2016/680. Do*** celów ***innych*** niż ściganie przestępstw ▌ art. 9 ust. 1 rozporządzenia (UE) 2016/679 i art. 10 ust. 1 rozporządzenia (UE) 2018/1725 ***zakazują przetwarzania danych biometrycznych z uwzględnieniem ograniczonej liczby wyjątków określonych w tych artykułach. W ramach stosowania*** art. ***9 ust. 1 rozporządzenia (UE) 2016/679 wykorzystywanie zdalnej identyfikacji biometrycznej do celów innych niż ściganie przestępstw było już przedmiotem decyzji o zakazie wydawanych przez krajowe organy ochrony danych***.

(40) 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. c) – w takim zakresie, w jakim dotyczy on wykorzystania systemów kategoryzacji biometrycznej w odniesieniu do działań w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w art. 5 ust. 1 lit. e) i lit. f) – w takim zakresie, w jakim dotyczą one wykorzystania systemów AI objętych tymi przepisami,*** art. 5 ***ust 3–8 i w art. 26 ust. 10*** 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.

(41) 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. c) – w takim zakresie, w jakim dotyczy on wykorzystania systemów kategoryzacji biometrycznej w odniesieniu do działań w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w art. 5 ust. 1 lit. e) i lit. f) – w takim zakresie, w jakim dotyczą one wykorzystania systemów AI objętych tymi przepisami,*** art. 5 ***ust 3–8 i w art. 26 ust. 10*** 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.

(42) Zgodnie z domniemaniem niewinności osoby fizyczne w Unii powinny być zawsze oceniane na podstawie ich faktycznego zachowania. Osoby fizyczne nigdy nie powinny być oceniane na podstawie zachowań prognozowanych przez AI wyłącznie na podstawie poddania ich profilowaniu, na podstawie ich cech osobowości lub cech charakterystycznych, takich jak narodowość, miejsce urodzenia, miejsce zamieszkania, liczba dzieci, poziom zadłużenia lub rodzaj samochodu, bez uzasadnionego podejrzenia, że osoba ta jest zaangażowana w działalność przestępczą w oparciu o obiektywne możliwe do zweryfikowania fakty i bez ich oceny przez człowieka. W związku z tym należy zakazać ocen ryzyka przeprowadzanych w odniesieniu do osób fizycznych w celu oceny ryzyka popełnienia przez te osoby przestępstwa lub przewidywania wystąpienia faktycznego lub potencjalnego przestępstwa wyłącznie na podstawie przeprowadzonego wobec nich profilowania lub oceny ich cech osobistych i charakterystycznych. W każdym razie zakaz ten nie odnosi się do ani nie dotyczy analizy ryzyka, która nie opiera się na profilowaniu osób fizycznych ani na cechach osobistych i charakterystycznych osób fizycznych, w takich przypadkach jak wykorzystywanie przez systemy AI analizy ryzyka w celu oceny ryzyka nadużyć finansowych przez przedsiębiorstwa na podstawie podejrzanych transakcji lub narzędzi analizy ryzyka w celu przewidywania przez organy celne prawdopodobnej lokalizacji środków odurzających lub nielegalnych towarów, na przykład na podstawie znanych szlaków przemytu.

(43) Należy zakazać wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemów AI, które tworzą lub rozbudowują bazy danych służące rozpoznawaniu twarzy poprzez niecelowane pozyskiwanie (ang. scraping) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej, ponieważ praktyka ta zwiększa poczucie masowej inwigilacji i może prowadzić do poważnych naruszeń praw podstawowych, w tym prawa do prywatności.

(44) Istnieją poważne obawy co do podstaw naukowych systemów AI mających na celu rozpoznawanie emocji lub wyciąganie wniosków na temat emocji, zwłaszcza że wyrażanie emocji znacznie się różni w zależności od kultur i sytuacji, a nawet w przypadku pojedynczej osoby. Wśród głównych wad takich systemów znajdują się ograniczona wiarygodność, nieprecyzyjność i ograniczona możliwość uogólnienia. W związku z tym systemy AI rozpoznające emocje lub zamiary osób fizycznych lub wyciągające wnioski na temat emocji lub zamiarów na podstawie danych biometrycznych tych osób mogą prowadzić do dyskryminacyjnych wyników i mogą naruszać prawa i wolności zainteresowanych osób. Biorąc pod uwagę brak równowagi sił w kontekście pracy lub edukacji, w połączeniu z inwazyjnym charakterem tych systemów, systemy takie mogą prowadzić do krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup. W związku z tym należy zakazać wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów AI przeznaczonych do stosowania w celu wykrywania stanu emocjonalnego osób w sytuacjach związanych z miejscem pracy i edukacją. Zakaz ten nie powinien obejmować systemów AI wprowadzanych do obrotu wyłącznie ze względów medycznych lub bezpieczeństwa, takich jak systemy przeznaczone do użytku terapeutycznego.

(45) Niniejsze rozporządzenie nie powinno mieć wpływu na praktyki, które są zakazane na mocy prawa Unii, w tym prawa o ochronie danych, prawa o niedyskryminacji, prawa o ochronie konsumentów i prawa konkurencji.

(46) Systemy AI wysokiego ryzyka powinny być wprowadzane do obrotu w Unii**,** oddawane do użytku ***lub wykorzystywane*** wyłącznie wówczas, gdy spełniają określone obowiązkowe wymogi. Wymogi te powinny zapewniać, aby systemy AI 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. ***W oparciu o nowe ramy prawne, jak wyjaśniono w zawiadomieniu Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022”[21], ogólna zasada stanowi, że unijne prawodawstwo harmonizacyjne, takie jak rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745[22] i (UE) 2017/746[23] oraz dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady[24], może mieć zastosowanie do jednego produktu, ponieważ udostępnianie lub oddawanie do użytku może mieć miejsce tylko wtedy, gdy produkt jest zgodny z całością obowiązującego unijnego prawodawstwa harmonizacyjnego. Aby zapewnić spójność i uniknąć niepotrzebnych obciążeń administracyjnych lub niepotrzebnych kosztów, dostawcy produktu, który zawiera jeden system AI wysokiego ryzyka lub większą ich liczbę, do którego lub do których mają zastosowanie wymogi niniejszego rozporządzenia lub unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku do niniejszego rozporządzenia, powinni mieć dowolność w odniesieniu do decyzji operacyjnych dotyczących sposobu zapewnienia w optymalny sposób zgodności produktu zawierającego system AI lub większą ich liczbę ze wszystkimi mającymi zastosowanie wymogami unijnego prawodawstwa harmonizacyjnego.*** Jako systemy AI wysokiego ryzyka należy uznawać jedynie te systemy AI, 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.

---

21 ***Dz.U. C 247 z 29.6.2022, s. 1.***

22 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).

23 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).

24 Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE (Dz.U. L 157 z 9.6.2006, s. 24).

(47) Systemy AI mogą ***mieć*** niepożądany ***wpływ*** na zdrowie i bezpieczeństwo osób, w szczególności w przypadku gdy takie systemy funkcjonują jako elementy ***bezpieczeństwa***. 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 zagrożeniom dla bezpieczeństwa, które mogą być powodowane przez produkt jako całość ze względu na jego elementy cyfrowe, w tym systemy AI, a także ograniczanie tych zagrożeń. 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. ▌

(48) Przy klasyfikowaniu systemu AI jako systemu wysokiego ryzyka zasadnicze znaczenie ma, w jakim stopniu system AI wywiera niepożądany wpływ 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, prawo do edukacji, ochrona konsumentów, prawa pracownicze, prawa osób z niepełnosprawnościami, równość płci, prawa własności intelektualnej, 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 oraz w Konwencji ONZ o prawach dziecka, szerzej rozwinięte w opracowanym przez ONZ komentarzu ogólnym nr 25 w sprawie praw dziecka w środowisku cyfrowym, które to prawa wymagają uwzględnienia szczególnej wrażliwości 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 AI, w tym w odniesieniu do zdrowia i bezpieczeństwa osób.

(49) Jeżeli chodzi o systemy AI wysokiego ryzyka, które są związanymi z bezpieczeństwem elementami produktów lub systemów objętych zakresem rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008[25], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 167/2013[26], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013[27], dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE[28], dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/797[29], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858[30],

---

25 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).

26 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).

27 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).

28 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).

29 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).

30 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).

rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139[31] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2144[32] lub które same są takimi produktami lub systemami, wskazane jest wprowadzenie zmian do tych aktów w celu zapewnienia, aby przyjmując wszelkie stosowne 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 zarządzania, oceny zgodności i egzekwowania oraz w powołane na mocy tych aktów organy – obowiązkowe wymogi dotyczące systemów AI wysokiego ryzyka określone w niniejszym rozporządzeniu.

---

[31] 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).

[32] 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).

(50) W przypadku systemów AI, 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 procedurze oceny zgodności przez jednostkę oceniającą zgodność będącą stroną 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*.

(51) Klasyfikacja systemu AI jako systemu wysokiego ryzyka na podstawie niniejszego rozporządzenia nie powinna koniecznie oznaczać, że produkt, którego związanym z bezpieczeństwem elementem jest system AI, lub sam system AI jako produkt uznaje się za produkt „wysokiego ryzyka” zgodnie z kryteriami ustanowionymi w stosownym unijnym prawodawstwie harmonizacyjnym, które ma zastosowanie do tego produktu. Dotyczy to w szczególności rozporządzeń (UE) 2017/745 i (UE) 2017/746, w których ocenę zgodności przeprowadza strona trzecia w odniesieniu do produktów średniego i wysokiego ryzyka.

(52) Jeżeli chodzi o samodzielne systemy AI, tj. systemy AI 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 dotkliwość potencjalnych szkód, jak i prawdopodobieństwo ich wystąpienia, oraz jeżeli są one wykorzystywane w szeregu ściśle określonych z góry obszarów wskazanych w niniejszym rozporządzeniu. Identyfikacja tych systemów opiera się na tej samej metodyce i kryteriach przewidzianych również w odniesieniu do wszelkich przyszłych zmian w wykazie systemów AI wysokiego ryzyka***, do przyjmowania których – w drodze aktów delegowanych – powinna być uprawniona Komisja, aby uwzględniać szybkie tempo rozwoju technologicznego, a także potencjalne zmiany w wykorzystaniu systemów AI***.

(53) Ważne jest również wyjaśnienie, że mogą istnieć szczególne przypadki, w których systemy AI odnoszące się do z góry określonych obszarów wyszczególnionych w niniejszym rozporządzeniu nie prowadzą do znacznego ryzyka szkody dla interesów prawnych chronionych w tych obszarach, ponieważ nie mają istotnego wpływu na proces decyzyjny lub nie szkodzą tym interesom w istotny sposób. Do celów niniejszego rozporządzenia system AI, który nie ma istotnego wpływu na wynik procesu decyzyjnego, należy rozumieć jako system AI, który nie ma wpływu na istotę, a tym samym na wynik procesu decyzyjnego, zarówno przeprowadzanego przez człowieka, jak i w sposób zautomatyzowany. System AI, który nie ma istotnego wpływu na wynik procesu decyzyjnego, może obejmować sytuacje, w których spełniony jest co najmniej jeden z poniższych warunków. Pierwszym takim warunkiem powinno być to, aby system AI miał wykonywać wąskie zadanie proceduralne – chodzi np. o system AI, który przekształca nieustrukturyzowane dane w dane ustrukturyzowane, system AI kategoryzujący przychodzące dokumenty lub system AI wykorzystywany do wykrywania duplikatów w dużej liczbie zastosowań. Zadania te mają tak wąski i ograniczony charakter, że stwarzają jedynie ograniczone ryzyko, które nie wzrasta w wyniku wykorzystania ich w kontekście wymienionym w wykazie przypadków użycia wysokiego ryzyka zamieszczonym w załączniku do niniejszego rozporządzenia. Drugim warunkiem powinno być to, aby zadanie wykonywane przez system AI miało na celu poprawę wyników już zakończonego działania przeprowadzonego przez człowieka, które może być istotne w kontekście wykazu przypadków użycia wysokiego ryzyka. Biorąc pod uwagę te cechy, system AI uzupełnia jedynie działanie człowieka, co w konsekwencji wiąże się z niższym ryzykiem. Warunek ten miałby zastosowanie na przykład do systemów AI, które mają na celu językową korektę przygotowanych dokumentów, na przykład by wprowadzić profesjonalny ton, styl akademicki lub by dostosować tekst do określonego przekazu marki.

Trzecim warunkiem powinno być to, aby system AI miał na celu wykrywanie wzorców podejmowania decyzji lub odstępstw od wzorców podjętych uprzednio decyzji. W tym przypadku ryzyko byłoby mniejsze, ponieważ system AI stosuje się po przeprowadzeniu oceny przez człowieka i nie służy on temu, by ją zastąpić lub na nią wpłynąć bez przeprowadzenia właściwej weryfikacji przez człowieka. Takie systemy AI obejmują na przykład te, które – uwzględniając określony wzorzec oceniania stosowany przez nauczyciela – mogą być wykorzystywane ex post, by sprawdzić, czy nauczyciel nie odszedł od stosowanego wzorca, i w ten sposób wskazać potencjalne niespójności lub nieprawidłowości. Czwartym warunkiem powinno być to, by system AI był przeznaczony jedynie do wykonywania zadań przygotowawczych w kontekście oceny istotnej z punktu widzenia systemów AI wymienionych w załączniku do niniejszego rozporządzenia, co sprawi, że podczas mającej nastąpić oceny prawdopodobieństwo stwierdzenia ryzyka w kontekście wyników systemu będzie bardzo niskie. Mowa tu między innymi o inteligentnych rozwiązaniach w zakresie zarządzania plikami, które obejmują różne funkcje, takie jak indeksowanie, przeszukiwanie, przetwarzanie tekstów i mowy lub łączenie danych z innymi źródłami danych, lub o systemach AI wykorzystywanych do tłumaczenia dokumentów wstępnych. W każdym przypadku takie systemy AI wysokiego ryzyka należy uznać za stwarzające znaczące ryzyko szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych, jeżeli dany system AI wiąże się z profilowaniem w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679 lub art. 3 pkt 4 dyrektywy (UE) 2016/680 lub art. 3 pkt 5 rozporządzenia (UE) 2018/1725. Aby zapewnić identyfikowalność i przejrzystość, dostawca, który na podstawie powyższych warunków uważa, że system AI nie jest systemem wysokiego ryzyka, powinien sporządzić dokumentację oceny przed wprowadzeniem tego systemu do obrotu lub oddaniem go do użytku i na żądanie przekazać tę dokumentację właściwym organom krajowym. Taki dostawca powinien być zobowiązany do zarejestrowania systemu w unijnej bazie danych ustanowionej na mocy niniejszego rozporządzenia. By zapewnić dalsze wskazówki dotyczące praktycznego stosowania warunków, na jakich systemy AI wysokiego ryzyka wymienione w załączniku są, w drodze wyjątku, uznawane za nieobarczone wysokim ryzykiem, Komisja powinna, po konsultacji z Radą ds. AI, przedstawić wytyczne w sprawie tego praktycznego stosowania uzupełnione wyczerpującym wykazem praktycznych przypadków użycia systemów AI wysokiego ryzyka i systemów AI nieobarczonych wysokim ryzykiem.

▌

(54) Ponieważ dane biometryczne stanowią szczególną kategorię wrażliwych danych osobowych, kilka krytycznych przypadków użycia systemów biometrycznych należy zaklasyfikować jako obarczone wysokim ryzykiem, o ile ich wykorzystywanie jest dozwolone na mocy odpowiednich przepisów unijnych i krajowych. Techniczne niedokładności systemów AI przeznaczonych do zdalnej identyfikacji biometrycznej osób fizycznych mogą prowadzić do stronniczych wyników i wywoływać skutki w postaci dyskryminacji. Ryzyko wystąpienia takich stronniczych wyników i skutków w postaci dyskryminacji jest szczególnie istotne w odniesieniu do wieku, pochodzenia etnicznego, rasy, płci lub niepełnosprawności. Systemy zdalnej identyfikacji biometrycznej należy zatem klasyfikować jako systemy wysokiego ryzyka ze względu na ryzyko, jakie stwarzają. Do tej kategorii nie należą systemy AI przeznaczone do weryfikacji biometrycznej, w tym uwierzytelniania, prowadzonej jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie w celu uzyskania dostępu do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń. Ponadto jako systemy wysokiego ryzyka należy zaklasyfikować systemy AI przeznaczone do kategoryzacji biometrycznej na podstawie danych biometrycznych według wrażliwych atrybutów lub cech chronionych na podstawie art. 9 ust. 1 rozporządzenia (UE) 2016/679, o ile nie są one zakazane na mocy niniejszego rozporządzenia, oraz systemy rozpoznawania emocji, które nie są zakazane na mocy niniejszego rozporządzenia. Za systemy wysokiego ryzyka nie należy uznawać systemów biometrycznych, które mają być wykorzystywane wyłącznie, by umożliwić stosowanie środków cyberbezpieczeństwa i ochrony danych osobowych.

(55) Z punktu widzenia zarządzania infrastrukturą krytyczną i jej obsługi jako systemy wysokiego ryzyka należy klasyfikować systemy AI, które mają być użytkowane jako związane z bezpieczeństwem elementy procesów zarządzania ***krytyczną infrastrukturą cyfrową wymienioną w załączniku I pkt 8 dyrektywy (UE) 2022/2557,*** ruchem drogowym i procesów ich obsługi oraz związane z bezpieczeństwem elementy zaopatrzenia w wodę, gaz, ciepło i energię elektryczną, ponieważ ich awaria lub nieprawidłowe działanie mogą stanowić zagrożenie życia i zdrowia osób na dużą skalę i prowadzić do znacznych zakłóceń w zwykłym prowadzeniu działalności społecznej i gospodarczej. ***Związane z bezpieczeństwem elementy infrastruktury krytycznej, w tym krytycznej infrastruktury cyfrowej, to systemy, które są wykorzystywane do bezpośredniej ochrony fizycznej integralności infrastruktury krytycznej lub zdrowia i bezpieczeństwa osób i mienia, ale które nie są konieczne do funkcjonowania systemu. Awaria lub nieprawidłowe działanie takich elementów mogą bezpośrednio prowadzić do zagrożenia fizycznej integralności infrastruktury krytycznej, a co za tym idzie, do zagrożeń zdrowia i bezpieczeństwa osób i mienia. Elementów przeznaczonych do stosowania wyłącznie do celów cyberbezpieczeństwa nie należy kwalifikować jako elementy bezpieczeństwa. Przykładami elementów bezpieczeństwa takiej infrastruktury krytycznej są systemy monitorowania ciśnienia wody lub systemy sterowania alarmem przeciwpożarowym w centrach przetwarzania danych w chmurze.***

(56) ***Stosowanie systemów AI w edukacji jest ważne, by promować wysokiej jakości kształcenie i szkolenie cyfrowe oraz by umożliwić wszystkim osobom uczącym się i nauczycielom zdobywanie niezbędnych umiejętności i kompetencji cyfrowych, w tym umiejętności korzystania z mediów i krytycznego myślenia, oraz dzielenie się tymi umiejętnościami i kompetencjami, z myślą o aktywnym udziale w gospodarce, społeczeństwie i procesach demokratycznych. Jako systemy AI wysokiego ryzyka*** należy ***natomiast*** zaklasyfikować systemy AI wykorzystywane w obszarze edukacji lub szkolenia zawodowego – w szczególności przeznaczone do celów podejmowania decyzji o dostępie lub ***przyjęciu*** do instytucji edukacyjnych i instytucji szkolenia zawodowego lub ***programów edukacyjnych lub szkolenia zawodowego na wszystkich poziomach***, lub do nadawania osobom przydziału do tych instytucji lub programów***, oceniania odpowiedniego poziomu wykształcenia i istotnego oddziaływania na poziom wykształcenia i szkolenia, jaki dana osoba otrzyma lub do jakiego będzie mogła mieć dostęp, lub do monitorowania i wykrywania zabronionego zachowania uczniów podczas testów*** – ponieważ systemy te mogą 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 stosowane***, mogą być szczególnie inwazyjne i*** naruszać prawo do kształcenia i szkolenia, a także prawo do niedyskryminacji oraz 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***.

(57) Systemy AI wykorzystywane w obszarze zatrudnienia, zarządzania pracownikami i dostępu do samozatrudnienia, w szczególności do rekrutacji i wyboru kandydatów, do podejmowania decyzji ***mających wpływ na warunki stosunków pracy,*** decyzji o awansie i rozwiązaniu ***umownego stosunku pracy, do spersonalizowanego przydzielania zadań w oparciu o indywidualne zachowania, cechy osobowości i do*** 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, źródła utrzymania tych osób ***i prawa pracownicze***. Odnośne umowne stosunki pracy powinny w ***znaczący sposób*** obejmować pracowników i osoby pracujące za pośrednictwem platform internetowych, o czym mowa w programie prac Komisji na 2021 r. ▌ W całym procesie rekrutacji oraz w ramach oceny, awansu lub utrzymywania na stanowisku 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 lub o określonej orientacji seksualnej. Systemy AI wykorzystywane do monitorowania wydajności i zachowania tych osób mogą również ***podważać*** ich prawa ***podstawowe*** w zakresie ochrony danych i prywatności.

(58) Innym obszarem, w którym stosowanie systemów AI wymaga szczególnej uwagi, 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 ▌ osoby fizyczne ***ubiegające się o podstawowe świadczenia i usługi w ramach pomocy publicznej lub korzystające z takich świadczeń i usług zapewnianych przez organy publiczne, a mianowicie usług opieki zdrowotnej, świadczeń z zabezpieczenia społecznego, usług społecznych zapewniających ochronę w przypadkach takich jak macierzyństwo, choroba, wypadki przy pracy, zależność lub podeszły wiek oraz utrata zatrudnienia, a także z pomocy społecznej i mieszkaniowej,*** są zazwyczaj zależne od tych świadczeń i usług oraz znajdują się w słabszym położeniu względem odpowiedzialnych organów. Jeżeli systemy AI są wykorzystywane do ustalenia, czy organy powinny ***przyznać*** takie świadczenia i usługi, odmówić ich, ograniczyć je, cofnąć lub odzyskać***, w tym do stwierdzenia, czy świadczeniobiorcy są w świetle prawa uprawnieni do takich świadczeń lub usług, systemy te*** mogą 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 i 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 AI, pod warunkiem że systemy te nie stwarzają wysokiego ryzyka dla osób prawnych i fizycznych.

Ponadto jako systemy wysokiego ryzyka należy klasyfikować systemy AI wykorzystywane do przeprowadzania punktowej oceny kredytowej lub oceny zdolności kredytowej osób fizycznych, ponieważ systemy te decydują o dostępie tych osób do zasobów finansowych lub podstawowych usług, takich jak mieszkalnictwo, energia elektryczna i usługi telekomunikacyjne. Systemy AI wykorzystywane do tych celów mogą prowadzić do dyskryminacji osób lub grup i mogą utrwalać historyczne wzorce dyskryminacji, takie jak dyskryminacja ze względu na pochodzenie rasowe lub etniczne, płeć, niepełnosprawność, wiek, orientację seksualną, lub mogą powodować powstawanie nowych rodzajów dyskryminacji. Za systemy wysokiego ryzyka na mocy niniejszego rozporządzenia nie należy jednak uznawać systemów AI przewidzianych w prawie Unii do celów wykrywania oszustw w ramach oferowania usług finansowych oraz do celów ostrożnościowych do obliczania wymogów kapitałowych instytucji kredytowych i zakładów ubezpieczeń. Ponadto systemy AI przeznaczone do stosowania do oceny ryzyka w przypadku ubezpieczenia zdrowotnego i na życie dla osób fizycznych i ustalania cen tych ubezpieczeń mogą mieć również znaczący wpływ na źródła utrzymania osób, a jeżeli nie są odpowiednio zaprojektowane, opracowane i wykorzystywane, mogą naruszać ich prawa podstawowe i prowadzić do poważnych konsekwencji dla życia i zdrowia ludzi, w tym wykluczenia finansowego i dyskryminacji. Ponadto systemy AI ***wykorzystywane do oceny i klasyfikacji zgłoszeń alarmowych dokonywanych przez osoby fizyczne lub do*** wysyłania lub ustalania priorytetów w wysyłaniu służb pierwszej pomocy***, w tym policji, straży pożarnej, i pomocy medycznej oraz w ramach systemów oceny stanu zdrowia pacjentów w nagłych wypadkach,*** należy klasyfikować jako systemy wysokiego ryzyka, ponieważ służą one do podejmowania decyzji o krytycznym znaczeniu dla życia i zdrowia osób oraz ich mienia.

(59) ***Ze względu na rolę i odpowiedzialność*** organów ścigania ich działania związane z niektórymi zastosowaniami systemów AI charakteryzują się znacznym brakiem równowagi sił i mogą prowadzić do objęcia osoby fizycznej nadzorem, do jej aresztowania lub pozbawienia wolności, jak również do zaistnienia innych niepożądanych skutków dla przestrzegania praw podstawowych gwarantowanych w Karcie. W szczególności jeżeli system AI nie jest trenowany z wykorzystaniem danych wysokiej jakości, nie spełnia odpowiednich wymogów pod względem ***skuteczności,*** 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 AI nie są w wystarczającym stopniu przejrzyste, wyjaśnialne i udokumentowane. W związku z tym szereg systemów AI przeznaczonych do stosowania w kontekście ścigania przestępstw, w którym dokładność, wiarygodność i przejrzystość są szczególnie ważne dla uniknięcia niepożądanych skutków, zachowania zaufania publicznego oraz zapewnienia odpowiedzialności i skutecznego dochodzenia roszczeń, należy klasyfikować jako systemy wysokiego ryzyka, ***o ile ich wykorzystanie jest dozwolone zgodnie z właściwymi przepisami unijnymi i krajowymi***.

Ze względu na charakter przedmiotowych działań i związane z nimi ryzyko do takich systemów AI wysokiego ryzyka należy zaliczyć w szczególności systemy AI przeznaczone do wykorzystywania przez organy ścigania ***lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii wspierające organy ścigania do oceny ryzyka, że*** osoba fizyczna ***stanie się ofiarą przestępstwa, takie jak wariografy i podobne narzędzia,*** do oceny wiarygodności dowodów ***podczas prowadzenia postępowań przygotowawczych w sprawie przestępstw lub ich ścigania oraz, o ile nie jest to niedozwolone na mocy niniejszego rozporządzenia, do oceny ryzyka popełnienia przestępstwa lub ponownego popełnienia przestępstwa przez osobę fizyczną niewyłącznie na podstawie*** profilowania osób fizycznych lub do ***oceny*** cech osobowości i charakteru lub wcześniejszego zachowania przestępnego osób fizycznych lub grup, do profilowania w trakcie wykrywania przestępstw, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania ▌ . Systemów AI przeznaczonych specjalnie do stosowania w postępowaniach administracyjnych prowadzonych przez organy podatkowe i celne***, jak również przez jednostki analityki finansowej wykonujące zadania administracyjne dotyczące analizy informacji na podstawie unijnych przepisów dotyczących przeciwdziałania praniu pieniędzy,*** nie należy ***klasyfikować jako*** systemów AI wysokiego ryzyka wykorzystywanych przez organy ścigania do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. ***Stosowanie narzędzi sztucznej inteligencji przez organy ścigania nie powinno stać się czynnikiem powodującym nierówności lub wykluczenie. Nie należy ignorować wpływu stosowania narzędzi AI na prawo podejrzanych do obrony, w szczególności na trudności w uzyskaniu istotnych informacji na temat funkcjonowania tych systemów oraz wynikające z tego trudności w kwestionowaniu dostarczanych przez nie wyników przed sądem, w szczególności przez osoby fizyczne objęte postępowaniem przygotowawczym.***

(60) Systemy AI 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 AI 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. ***O ile ich wykorzystanie jest dozwolone zgodnie z właściwymi przepisami unijnymi i krajowymi,*** za systemy wysokiego ryzyka należy zatem uznać systemy AI przeznaczone do wykorzystywania przez właściwe organy publiczne ***lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii***, odpowiedzialne za wykonywanie zadań w dziedzinach zarządzania migracją, azylem i kontrolą graniczną, takie jak wariografy i podobne narzędzia***,*** gdy systemy te stosuje się do oceny niektórych zagrożeń stwarzanych przez osoby fizyczne wjeżdżające na terytorium państwa członkowskiego lub ubiegające się o wizę lub azyl***,*** do wspierania właściwych organów publicznych 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***, w tym przy powiązanej ocenie wiarygodności dowodów, do celów wykrywania, rozpoznawania lub identyfikacji osób fizycznych w kontekście zarządzania migracją, azylem i kontrolą graniczną, z wyjątkiem weryfikacji dokumentów podróży***.

Systemy AI w obszarze zarządzania migracją, azylem i kontrolą graniczną objęte niniejszym rozporządzeniem powinny być zgodne z odpowiednimi wymogami proceduralnymi określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 810/2009[33], dyrektywie Parlamentu Europejskiego i Rady 2013/32/UE[34] i w innych właściwych unijnych przepisach. ***Wykorzystanie systemów AI w zarządzaniu migracją, azylem i kontrolą graniczną nie powinno w żadnym wypadku być stosowane przez państwa członkowskie lub instytucje, organy i jednostki organizacyjne Unii jako sposób na obejście ich międzynarodowych zobowiązań wynikających z Konwencji ONZ dotyczącej statusu uchodźców sporządzonej w Genewie dnia 28 lipca 1951 r., zmienionej protokołem z dnia 31 stycznia 1967 r. Nie powinny być również wykorzystywane w żaden sposób do naruszania zasady non-refoulement ani do odmawiania bezpiecznych i skutecznych legalnych sposobów wjazdu na terytorium Unii, w tym prawa do ochrony międzynarodowej.***

---

33 ▌ 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).

34 ▌ 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).

(61) Niektóre systemy AI przeznaczone na potrzeby sprawowania wymiaru sprawiedliwości i procesów demokratycznych należy zaklasyfikować jako systemy wysokiego ryzyka, biorąc pod uwagę ich potencjalnie istotny wpływ na demokrację, praworządność, wolności osobiste, a także prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu. W szczególności, aby wyeliminować potencjalne ryzyko stronniczości, błędów i efektu czarnej skrzynki, jako systemy wysokiego ryzyka należy kwalifikować systemy AI, które mają ***być stosowane przez organy sądowe lub w ich imieniu, aby*** pomóc tym organom w badaniu i interpretacji faktów i przepisów oraz w stosowaniu tych przepisów do konkretnego stanu faktycznego. ***Systemy AI przeznaczone do wykorzystania w tych celach przez organy alternatywnego rozstrzygania sporów również należy uznać za systemy wysokiego ryzyka, jeżeli wyniki postępowania w sprawie alternatywnego rozstrzygania sporów wywołują skutki prawne dla stron. Stosowanie narzędzi AI może wspierać uprawnienia decyzyjne sędziów lub niezależność sądownictwa, ale nie powinno ich zastępować, gdyż podejmowanie ostatecznej decyzji musi pozostać działaniem kierowanym przez człowieka. Kwalifikacja systemów AI jako systemów AI wysokiego ryzyka*** nie powinna jednak rozciągać się na systemy AI 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 ▌.

(62) Bez uszczerbku dla przepisów ustanowionych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/...[35] [+] oraz aby zapobiec ryzyku nadmiernej zewnętrznej ingerencji w prawo do głosowania zapisane w art. 39 Karty oraz niepożądanemu wpływowi na demokrację i praworządność, systemy AI przeznaczone do wykorzystania, by wpływać na wynik wyborów lub referendum lub na zachowanie wyborcze osób fizycznych podczas głosowania w wyborach lub referendach, należy klasyfikować jako systemy AI wysokiego ryzyka, z wyjątkiem systemów AI, na których wyniki osoby fizyczne nie są bezpośrednio narażone, takich jak narzędzia wykorzystywane do organizowania, optymalizacji i strukturyzowania kampanii politycznych z administracyjnego i logistycznego punktu widzenia.

(63) Faktu, że dany system AI został zaklasyfikowany jako ***system AI*** wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, nie należy interpretować jako wskazującego na to, że korzystanie z tego systemu jest ▌ zgodne z prawem na gruncie innych aktów prawa Unii lub prawa krajowego zgodnego z prawem Unii, na przykład w zakresie ochrony danych osobowych, stosowania wariografów i podobnych narzędzi lub innych systemów służących wykrywaniu stanu emocjonalnego osób fizycznych. Każde takie wykorzystanie można 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***, o ile w niniejszym rozporządzeniu wyraźnie nie przewidziano inaczej***.

---

35 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... w sprawie przejrzystości i targetowania reklamy politycznej (Dz.U. L... z ..., ELI:...).

\+ Dz.U.: Proszę wstawić do tekstu numer rozporządzenia z dok. PE 90/23 (2021/0381 (COD)) oraz uzupełnić odpowiadający przypis.

(64) Aby ograniczyć ryzyko stwarzane przez systemy AI wysokiego ryzyka wprowadzone ***do obrotu lub*** oddawane do użytku ***oraz aby zapewnić wysoki poziom wiarygodności***, należy wprowadzić pewne obowiązkowe wymogi ***w odniesieniu do systemów AI wysokiego ryzyka***, z uwzględnieniem przeznaczenia systemu ***AI i kontekstu jego*** wykorzystania oraz zgodnie z systemem zarządzania ryzykiem, który ma zostać ustanowiony przez dostawcę. ***Środki przyjęte przez dostawców w celu spełnienia obowiązkowych wymogów niniejszego rozporządzenia powinny uwzględniać powszechnie uznany stan wiedzy technicznej w zakresie AI, być proporcjonalne i skuteczne do osiągnięcia celów niniejszego rozporządzenia. W oparciu o nowe ramy prawne, jak wyjaśniono w zawiadomieniu Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022", ogólna zasada stanowi, że unijne prawodawstwo harmonizacyjne może mieć zastosowanie do jednego produktu, ponieważ udostępnianie lub oddawanie do użytku może mieć miejsce tylko wtedy, gdy produkt jest zgodny z całością obowiązującego unijnego prawodawstwa harmonizacyjnego. Zagrożenia związane z systemami AI objętymi wymogami niniejszego rozporządzenia dotyczą innych aspektów niż istniejące unijne akty harmonizacyjne, w związku z czym wymogi niniejszego rozporządzenia uzupełnią istniejący zbiór unijnych aktów harmonizacyjnych. Na przykład maszyny lub wyroby medyczne zawierające system AI mogą stwarzać ryzyko, które nie zostało uwzględnione w zasadniczych wymogach w zakresie zdrowia i bezpieczeństwa określonych w odpowiednim unijnym prawodawstwie harmonizacyjnym, ponieważ to prawo sektorowe nie reguluje ryzyka specyficznego dla systemów AI.***

Wymaga to jednoczesnego i komplementarnego stosowania różnych aktów ustawodawczych. Aby zapewnić spójność i uniknąć niepotrzebnych obciążeń administracyjnych i niepotrzebnych kosztów, dostawcy produktu, który zawiera co najmniej jeden system AI wysokiego ryzyka, do którego mają zastosowanie wymogi niniejszego rozporządzenia i unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych wymienionego w załączniku do niniejszego rozporządzenia, powinni mieć dowolność w odniesieniu do decyzji operacyjnych dotyczących sposobu zapewnienia w optymalny sposób zgodności produktu zawierającego system AI lub większą ich liczbę ze wszystkimi mającymi zastosowanie wymogami unijnego prawodawstwa harmonizacyjnego. Elastyczność ta może oznaczać na przykład decyzję dostawcy o włączeniu części niezbędnych procesów testowania i sprawozdawczości, informacji i dokumentacji wymaganych na mocy niniejszego rozporządzenia do już istniejącej dokumentacji i procedur wymaganych na mocy obowiązującego unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych, wymienionego w załączniku do niniejszego rozporządzenia. Nie powinno to w żaden sposób podważać spoczywającego na dostawcy obowiązku spełnienia wszystkich mających zastosowanie wymogów.

(65) System zarządzania ryzykiem powinien obejmować ciągły, iteracyjny proces, który jest planowany i realizowany przez cały cykl życia systemu AI wysokiego ryzyka. Proces ten powinien mieć na celu identyfikację i ograniczenie istotnego ryzyka, jakie systemy AI stwarzają dla zdrowia, bezpieczeństwa i praw podstawowych. System zarządzania ryzykiem powinien podlegać regularnym przeglądom i aktualizacji, aby zapewnić jego stałą skuteczność, a także uzasadnienie i dokumentację wszelkich istotnych decyzji i działań podjętych zgodnie z niniejszym rozporządzeniem. Proces ten powinien zapewniać, aby dostawca identyfikował ryzyko lub niepożądane skutki oraz wdrażał środki ograniczające znane i racjonalnie przewidywalne ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych związane z systemami AI w świetle ich przeznaczenia i dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, w tym możliwego ryzyka wynikającego z interakcji między systemem AI a środowiskiem, w którym ten system działa. W systemie zarządzania ryzykiem należy przyjąć najbardziej odpowiednie – w świetle aktualnego stanu wiedzy technicznej w dziedzinie AI – środki zarządzania ryzykiem. Przy określaniu najbardziej odpowiednich środków zarządzania ryzykiem dostawca powinien udokumentować i wyjaśnić dokonane wybory oraz, w stosownych przypadkach, zaangażować ekspertów i zewnętrzne zainteresowane strony. Identyfikując dające się racjonalnie przewidzieć niewłaściwe wykorzystanie systemów AI wysokiego ryzyka, dostawca powinien uwzględnić zastosowania systemów AI, w odniesieniu do których można zasadnie oczekiwać, że będą one wynikać z łatwo przewidywalnego zachowania ludzkiego w kontekście szczególnych cech i wykorzystania danego systemu AI, chociaż zastosowań tych nie przewidziano w przeznaczeniu danego systemu ani w jego instrukcji obsługi.

Wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu AI wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, mogące powodować ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych, powinny zostać uwzględnione w instrukcji obsługi dostarczonej przez dostawcę. Ma to na celu zapewnienie, aby podmiot stosujący AI był ich świadomy i uwzględniał je przy korzystaniu z systemu AI wysokiego ryzyka. Określenie i wdrożenie – na podstawie niniejszego rozporządzenia – środków ograniczających ryzyko w odniesieniu dodającego się przewidzieć niewłaściwego wykorzystania nie powinno wymagać od dostawcy wprowadzenia szczególnych dodatkowych środków szkoleniowych, by zaradzić temu niewłaściwemu wykorzystaniu systemu AI wysokiego ryzyka. Zachęca się jednak dostawców do rozważenia takich dodatkowych środków szkoleniowych w celu ograniczenia dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, o ile będzie to konieczne i stosowne.

(66) Systemy AI wysokiego ryzyka powinny podlegać wymogom dotyczącym ***zarządzania ryzykiem,*** jakości ***i istotności*** wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji ***podmiotom stosującym AI***, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Wymogi te są konieczne, aby skutecznie ograniczyć ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych, ▌ gdy nie są racjonalnie dostępne inne środki, które powodowałyby mniejsze ograniczenia w handlu, co pozwoli uniknąć nieuzasadnionych ograniczeń w tym zakresie.

(67) ***Wysokiej jakości dane i dostęp do wysokiej*** jakości ***danych odgrywają kluczową rolę w zapewnianiu struktury i*** skuteczności działania wielu systemów AI, w szczególności w przypadku stosowania technik obejmujących trenowanie modeli, w celu zapewnienia, aby system AI 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 administrowania i zarządzania danymi***. ***Zbiory danych treningowych, walidacyjnych i testowych, w tym etykiety, muszą być adekwatne, wystarczająco reprezentatywne oraz w jak największym stopniu*** wolne od błędów i kompletne z punktu widzenia przeznaczenia systemu. ***Aby ułatwić przestrzeganie unijnych przepisów o ochronie danych, takich jak rozporządzenie (UE) 2016/679, praktyki w zakresie administrowania i zarządzania danymi powinny przewidywać, w przypadku danych osobowych, zapewnianie przejrzystości pierwotnego celu gromadzenia danych. Te zbiory danych*** powinny również charakteryzować się odpowiednimi właściwościami statystycznymi, w tym w odniesieniu do osób lub grup osób***, wobec których*** system AI wysokiego ryzyka ma być wykorzystywany***, ze szczególnym uwzględnieniem ograniczania ewentualnej stronniczości w zbiorach danych, która może mieć wpływ na zdrowie i bezpieczeństwo osób, negatywnie oddziaływać na prawa podstawowe lub prowadzić do dyskryminacji zakazanej na mocy prawa Unii, zwłaszcza w przypadku gdy dane wyjściowe wpływają na dane wejściowe wykorzystywane na potrzeby przyszłych operacji (sprzężenie zwrotne). Stronniczość może być na przykład nieodłączną cechą źródłowych zbiorów danych, szczególnie jeżeli używa się danych historycznych lub wygenerowanych na etapie wdrażania systemów w warunkach rzeczywistych.***

Na wyniki generowane przez systemy AI może wpływać taka nieodłączna stronniczość, która z zasady stopniowo zwiększa się, a tym samym utrwala i pogłębia istniejącą dyskryminację, zwłaszcza w odniesieniu do osób szczególnie wrażliwych należących do niektórych grup, w tym grup rasowych lub etnicznych. Wymóg, aby zbiory danych były w jak największym stopniu kompletne i wolne od błędów, nie powinien wpływać na stosowanie technik ochrony prywatności w kontekście opracowywania i testowania systemów AI. W szczególności zbiory danych powinny uwzględniać – w zakresie wymaganym z uwagi na ich przeznaczenie – cechy, właściwości lub elementy, które są specyficzne dla określonego otoczenia geograficznego, ***kontekstualnego,*** behawioralnego lub funkcjonalnego, w którym dany system AI ma być wykorzystywany. ***Wymogi związane z zarządzaniem danymi można spełnić, korzystając z usług stron trzecich, które oferują certyfikowane usługi w zakresie zgodności, w tym weryfikację zarządzania danymi i integralności zbioru danych oraz praktyki w zakresie trenowania, walidacji i testowania danych, o ile zapewniona jest zgodność z wymogami dotyczącymi danych określonymi w niniejszym rozporządzeniu.***

(68) Przy opracowywaniu i ***ocenie*** systemów AI wysokiego ryzyka niektóre podmioty, takie jak dostawcy, jednostki notyfikowane i inne odpowiednie podmioty, takie jak europejskie centra innowacji cyfrowych, ośrodki testowo-doświadczalne i naukowcy, powinny mieć możliwość uzyskania dostępu do wysokiej jakości zbiorów danych i korzystania z nich w wykonywanych przez te podmioty 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 AI. Na przykład w dziedzinie zdrowia europejska przestrzeń danych dotyczących zdrowia ułatwi niedyskryminacyjny dostęp do danych dotyczących zdrowia oraz trenowanie algorytmów AI na tych zbiorach danych w sposób bezpieczny, terminowy, przejrzysty, wiarygodny i zapewniający ochronę prywatności oraz z odpowiednim zarządzaniem 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 AI.

(69) Prawo do prywatności i ochrony danych osobowych musi być zagwarantowane przez cały cykl życia systemu AI. W tym względzie, gdy przetwarzane są dane osobowe, zastosowanie mają zasady minimalizacji danych oraz uwzględnienia ochrony danych już w fazie projektowania i domyślnej ochrony danych, które określono w unijnych przepisach o ochronie danych. Środki podejmowane przez dostawców w celu zapewnienia zgodności z tymi zasadami mogą obejmować nie tylko anonimizację i szyfrowanie, ale również wykorzystanie technologii, która umożliwia wprowadzanie algorytmów do danych i umożliwia trenowanie systemów AI bez przekazywania między stronami lub kopiowania samych surowych lub ustrukturyzowanych danych, bez uszczerbku dla wymogów dotyczących zarządzania danymi przewidzianych w niniejszym rozporządzeniu.

(70) W celu ochrony praw innych osób przed dyskryminacją, która może wynikać ze stronniczości systemów AI, dostawcy powinni wyjątkowo, w zakresie, w jakim jest to absolutnie niezbędne do celów zapewnienia wykrywania i korygowania stronniczości w odniesieniu do systemów AI wysokiego ryzyka – z zastrzeżeniem odpowiednich zabezpieczeń w zakresie podstawowych praw i wolności osób fizycznych oraz po spełnieniu wszystkich mających zastosowanie warunków określonych w niniejszym rozporządzeniu, w uzupełnieniu warunków określonych w rozporządzeniach (UE) 2016/679 i (UE) 2018/1725 oraz w dyrektywie (UE) 2016/680 – mieć możliwość przetwarzania również szczególnych kategorii danych osobowych w związku z istotnym interesem publicznym w rozumieniu art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679 i art. 10 ust. 2 lit. g) rozporządzenia (UE) 2018/1725.

(71) Dysponowanie ***zrozumiałymi*** informacjami na temat tego, w jaki sposób opracowano systemy AI wysokiego ryzyka i jak działają one w całym ***cyklu życia***, ma zasadnicze znaczenie dla ***umożliwienia identyfikowalności tych systemów,*** weryfikacji zgodności z wymogami określonymi w niniejszym rozporządzeniu***, a także dla monitorowania ich działania i monitorowania po wprowadzeniu do obrotu***. W tym celu konieczne jest prowadzenie rejestrów zdarzeń oraz zapewnienie dostępności dokumentacji technicznej zawierającej informacje niezbędne do oceny zgodności systemu AI z odpowiednimi wymogami ***i do ułatwienia monitorowania po wprowadzeniu do obrotu***. Informacje takie powinny ***być podane w jasnej i kompleksowej formie i*** obejmować ogólne właściwości, zdolności i ograniczenia systemu, algorytmy, dane, procesy związane z trenowaniem, testowaniem i walidacją, a także dokumentację dotyczącą odpowiedniego systemu zarządzania ryzykiem. Dokumentacja techniczna powinna podlegać ***odpowiedniej aktualizacji w całym cyklu życia systemu AI***. ***Ponadto w systemach AI wysokiego ryzyka powinno być technicznie możliwe automatyczne rejestrowanie zdarzeń – za pomocą rejestrów zdarzeń – w całym cyklu życia systemu.***

(72) Aby zająć się ***kwestiami związanymi z*** efektem czarnej skrzynki i ***złożonością*** niektórych systemów AI i ***pomóc podmiotom stosującym AI w wypełnianiu ich obowiązków wynikających z niniejszego rozporządzenia,*** od systemów AI wysokiego ryzyka należy wymagać określonego stopnia przejrzystości ***przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku. Systemy AI wysokiego ryzyka*** należy ***projektować w taki sposób, aby umożliwić podmiotom stosującym AI zrozumienie funkcjonowania*** systemu ***AI, ocenę jego funkcjonalności oraz zrozumienie jego mocnych stron i ograniczeń.*** Systemom AI ***wysokiego ryzyka*** powinny ▌ towarzyszyć ***odpowiednie informacje w formie*** instrukcji obsługi. ***Takie informacje powinny*** obejmować ***cechy, zdolności i ograniczenia skuteczności działania systemu AI. Takie elementy obejmowałyby*** informacje ***na temat ewentualnych znanych lub przewidywalnych okoliczności związanych z wykorzystaniem systemu AI wysokiego ryzyka,*** w tym działań ***podmiotu stosującego AI, które mogą wpływać na zachowanie i skuteczność systemu, i w których to okolicznościach system AI może powodować*** ryzyko dla ***zdrowia, bezpieczeństwa i*** praw podstawowych***; a także informacje na temat zmian, które zostały z góry zaplanowane i ocenione pod kątem zgodności przez dostawcę, oraz na temat odpowiednich środków nadzoru ze strony człowieka, w tym środków ułatwiających podmiotom stosującym AI interpretację wyników działania systemu AI. Przejrzystość, w tym towarzyszące instrukcje obsługi, powinny pomóc podmiotom stosującym AI w korzystaniu z systemu i wspierać podejmowanie przez te podmioty świadomych decyzji. Na przykład podmioty stosujące AI powinny być lepiej przygotowane, by dokonać właściwego wyboru systemu, z którego zamierzają korzystać w świetle mających do nich zastosowanie obowiązków, mieć wiedzę na temat zamierzonych i wykluczonych zastosowań oraz prawidłowo i odpowiednio korzystać z systemu AI. Aby zwiększyć czytelność i dostępność informacji zawartych w instrukcji obsługi,*** w stosownych przypadkach ***należy uwzględnić konkretne przykłady, takie jak przykłady ograniczeń czy zamierzonych i wykluczonych zastosowań systemu AI***. ***Dostawcy powinni zapewnić, aby wszelka dokumentacja, w tym instrukcje obsługi, zawierała istotne, wyczerpujące, dostępne i zrozumiałe informacje, z uwzględnieniem potrzeb docelowych podmiotów stosujących AI i prawdopodobnie posiadanej przez te podmioty wiedzy. Instrukcje obsługi powinny być udostępniane w języku łatwo zrozumiałym dla docelowych podmiotów stosujących AI, określonym przez zainteresowane państwo członkowskie.***

(73) Systemy AI wysokiego ryzyka należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie***, zapewniać, by ich wykorzystanie było zgodne z przeznaczeniem oraz zapewniać reagowanie na skutki ich stosowania w całym cyklu życia systemu***. W tym celu przed wprowadzeniem systemu do obrotu lub oddaniem go 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. ***W stosownych przypadkach istotne jest także zapewnienie, aby systemy AI wysokiego ryzyka obejmowały mechanizmy udzielania wskazówek i informacji osobom fizycznym, którym powierzono nadzór ze strony człowieka, aby mogły one podejmować świadome decyzje, czy, kiedy i w jaki sposób należy interweniować w celu uniknięcia negatywnych konsekwencji lub zagrożeń lub zatrzymać system, jeżeli nie działa on zgodnie z przeznaczeniem. Zważywszy na istotne konsekwencje dla osób fizycznych w przypadku nieprawidłowego dopasowania przez niektóre systemy identyfikacji biometrycznej, należy wprowadzić wymóg sprawowania w odniesieniu do tych systemów wzmocnionego nadzoru ze strony człowieka, tak aby podmiot stosujący AI nie mógł podejmować żadnych działań ani decyzji na podstawie identyfikacji wynikającej z systemu, dopóki nie zostało to odrębnie zweryfikowane i potwierdzone przez co najmniej dwie osoby fizyczne. Osoby te mogą pochodzić z różnych podmiotów i mogą to być osoby obsługujące system lub z niego korzystające. Wymóg ten nie powinien powodować niepotrzebnych obciążeń ani opóźnień i powinno wystarczyć, że odrębne weryfikacje dokonywane przez różne osoby będą automatycznie rejestrowane w wygenerowanych przez system rejestrach zdarzeń. Biorąc pod uwagę specyfikę obszarów ścigania przestępstw, migracji, kontroli granicznej i azylu, powyższy wymóg nie powinien mieć zastosowania, jeżeli na mocy prawa Unii lub prawa krajowego stosowanie tego wymogu uznaje się za nieproporcjonalne.***

(74) Systemy AI wysokiego ryzyka powinny działać w sposób spójny w całym cyklu życia i charakteryzować się odpowiednim poziomem dokładności, solidności i cyberbezpieczeństwa – ***w świetle ich przeznaczenia i*** zgodnie z powszechnie uznawanym stanem wiedzy technicznej. ***Komisję oraz właściwe organizacje i zainteresowane strony zachęca się, by należycie uwzględniały ograniczanie ryzyka i negatywnych skutków związanych ze stosowaniem systemu AI. Oczekiwany*** poziom ***wskaźników skuteczności należy zadeklarować w załączonej instrukcji obsługi. Dostawców wzywa się, by przekazywali te informacje podmiotom stosującym AI w jasny i łatwo zrozumiały sposób, wolny od dwuznaczności i stwierdzeń wprowadzających w błąd. Prawo Unii dotyczące metrologii prawnej, w tym dyrektywy Parlamentu Europejskiego i Rady 2014/31/UE[36] i 2014/32/UE[37], ma na celu zapewnienie dokładności pomiarów oraz wspieranie przejrzystości i uczciwości transakcji handlowych. W tym kontekście, we współpracy z odpowiednimi zainteresowanymi stronami i organizacjami, takimi jak organy ds. metrologii i organy ds. analizy porównawczej, Komisja powinna w stosownych przypadkach zachęcać do opracowywania poziomów odniesienia i metod pomiaru dotyczących systemów AI. Komisja powinna przy tym współpracować z partnerami międzynarodowymi pracującymi nad metrologią i odpowiednimi wskaźnikami pomiarowymi związanymi z AI oraz uwzględniać ich działania.***

---

36 Dyrektywa Parlamentu Europejskiego i Rady 2014/31/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku wag nieautomatycznych (Dz.U. L 96 z 29.3.2014, s. 107).

37 Dyrektywa Parlamentu Europejskiego i Rady 2014/32/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych (Dz.U. L 096 z 29.3.2014, s. 149).

(75) Kluczowym wymogiem dotyczącym systemów AI wysokiego ryzyka jest solidność techniczna. Powinny one być odporne ***na szkodliwe lub w inny sposób niepożądane zachowania, które mogą wynikać z*** ograniczeń w ***systemach lub z środowiska, w którym te systemy działają*** (np. błędy, usterki, niespójności, nieoczekiwane sytuacje)***. W związku z tym należy wprowadzić środki techniczne i organizacyjne, by zapewnić solidność systemów AI wysokiego ryzyka, na przykład poprzez projektowanie i opracowywanie odpowiednich rozwiązań technicznych w celu zapobiegania*** szkodliwym lub innym niepożądanym zachowaniom ***lub ich ograniczania***. ***Takie rozwiązania techniczne mogą obejmować na przykład mechanizmy umożliwiające bezpieczne przerwanie działania systemu (przejście systemu w stan bezpieczny – tzw. „fail-safe"), jeśli zaistnieją pewne nieprawidłowości lub gdy działanie wykracza poza określone z góry granice.*** Brak ochrony przed tymi zagrożeniami może mieć konsekwencje dla bezpieczeństwa lub negatywnie wpłynąć na prawa podstawowe, na przykład z powodu błędnych decyzji lub nieprawidłowych lub stronniczych wyników działania generowanych przez system AI.

(76) Cyberbezpieczeństwo odgrywa kluczową rolę w zapewnianiu odporności systemów AI na próby modyfikacji ich zastosowania, zachowania, skuteczności działania lub obejścia ich zabezpieczeń przez działające w złej wierze osoby trzecie wykorzystujące słabe punkty systemu. Cyberataki na systemy AI mogą polegać na wykorzystaniu konkretnych zasobów AI, takich jak zbiory danych treningowych (np. zatruwanie danych) lub trenowane modele (np. ataki kontradyktoryjne ***lub ataki z wywnioskowaniem przynależności***), lub wykorzystaniu słabych punktów w zasobach cyfrowych systemu AI lub w bazowej infrastrukturze ICT. Aby zapewnić poziom cyberbezpieczeństwa odpowiedni do ryzyka, dostawcy systemów AI wysokiego ryzyka powinni zatem wdrożyć odpowiednie środki***, takie jak mechanizmy kontroli bezpieczeństwa,*** uwzględniając również w stosownych przypadkach infrastrukturę ICT, na której opiera się dany system.

(77) Bez uszczerbku dla wymogów związanych z solidnością i dokładnością określonych w niniejszym rozporządzeniu systemy AI wysokiego ryzyka, które wchodzą w zakres rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/...[38] [+], zgodnie z art. 8 tego rozporządzenia mogą wykazać zgodność z wymogami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu w drodze spełnienia zasadniczych wymogów w zakresie cyberbezpieczeństwa zawartych w art. 10 rozporządzenia (UE) 2024/...[+] oraz w załączniku I do tego rozporządzenia. W przypadku gdy systemy AI wysokiego ryzyka spełniają zasadnicze wymogi rozporządzenia (UE) 2024/...[++], należy uznać, że wykazują zgodność z wymogami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu w zakresie, w jakim wypełnienie tych wymogów wykazano w deklaracji zgodności UE lub w jej częściach wydanych zgodnie z rozporządzeniem (UE) 2024/...[++]. W tym celu ocena ryzyka w cyberprzestrzeni związanego z produktem z elementami cyfrowymi, które zaklasyfikowano jako system AI wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, przeprowadzana na podstawie rozporządzenia (UE) 2024/...[++], powinna uwzględniać ryzyko dla cyberodporności systemu AI w odniesieniu do podejmowanych przez nieupoważnione osoby trzecie prób zmiany jego zastosowania, zachowania lub skuteczności działania, w tym uwzględniać charakterystyczne dla AI słabe punkty, takie jak ryzyko zatruwania danych lub ataki kontradyktoryjne, a także, w stosownych przypadkach, uwzględniać ryzyko dla przestrzegania praw podstawowych zgodnie z wymogami niniejszego rozporządzenia.

---

38 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/… z dnia … w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020 (Dz.U. L z ...., ELI: ...).

\+ Dz.U.: Proszę wstawić do tekstu numer rozporządzenia z dok. PE XX/RR (2022/0272 (COD)) oraz uzupełnić odpowiadający przypis.

(78) Procedura oceny zgodności przewidziana w niniejszym rozporządzeniu powinna mieć zastosowanie do zasadniczych wymogów w zakresie cyberbezpieczeństwa produktu z elementami cyfrowymi objętego rozporządzeniem (UE) 2024/...[+] i zaklasyfikowanego jako system AI wysokiego ryzyka na podstawie niniejszego rozporządzenia. Zasada ta nie powinna jednak powodować zmniejszenia niezbędnego poziomu bezpieczeństwa w odniesieniu do produktów krytycznych z elementami cyfrowymi objętych rozporządzeniem (UE) 2024/...[+]. W związku z tym, na zasadzie odstępstwa od tej zasady, systemy AI wysokiego ryzyka, które wchodzą w zakres niniejszego rozporządzenia i są również kwalifikowane jako ważne i krytyczne produkty z elementami cyfrowymi zgodnie z rozporządzeniem (UE) 2024/...[+] i do których ma zastosowanie procedura oceny zgodności oparta na kontroli wewnętrznej określona w załączniku do niniejszego rozporządzenia, podlegają przepisom dotyczącym oceny zgodności zawartym w rozporządzeniu (UE) 2024/...[+] w zakresie, w jakim dotyczy to zasadniczych wymogów w zakresie cyberbezpieczeństwa określonych w tym rozporządzeniu. W tym przypadku do wszystkich pozostałych aspektów objętych niniejszym rozporządzeniem należy stosować odpowiednie przepisy dotyczące oceny zgodności opierającej się na kontroli wewnętrznej określone w załączniku do niniejszego rozporządzenia. By wykorzystać wiedzę teoretyczną i fachową ENISA w zakresie polityki cyberbezpieczeństwa i w oparciu o zadania powierzone ENISA na podstawie rozporządzenia (UE) 2019/1020, Komisja powinna współpracować z ENISA w kwestiach związanych z cyberbezpieczeństwem systemów AI.

[+] Dz.U.: Proszę wstawić numer rozporządzenia z dok. PE XX/RR (2022/0272 (COD)).

()

(79) Należy zapewnić, aby odpowiedzialność za wprowadzenie do obrotu lub oddanie do użytku systemu AI 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.

(80) ***Jako sygnatariusze Konwencji ONZ o prawach osób niepełnosprawnych Unia i państwa członkowskie są prawnie zobowiązane do ochrony osób z niepełnosprawnościami przed dyskryminacją i do propagowania ich równości, do zapewnienia im dostępu na równych zasadach z innymi osobami do technologii i systemów informacyjno-komunikacyjnych oraz do zapewnienia poszanowania ich prywatności. Z uwagi na rosnące znaczenie i stosowanie systemów sztucznej inteligencji stosowanie zasad projektowania uniwersalnego do wszystkich nowych technologii i usług powinno zapewniać pełny i równy dostęp dla wszystkich osób, których potencjalnie dotyczą technologie sztucznej inteligencji lub które je stosują, w tym osób z niepełnosprawnościami, w sposób uwzględniający w pełni ich przyrodzoną godność i różnorodność. Istotne jest zatem, aby dostawcy zapewniali pełną zgodność z wymogami dostępności, w tym z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/2102[39] i dyrektywą (UE) 2019/882. Dostawcy powinni zapewnić zgodność z tymi wymogami już na etapie projektowania. W związku z tym w projektowaniu systemu AI wysokiego ryzyka należy w jak największym stopniu uwzględnić niezbędne środki.***

---

39 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.U. L 327 z 2.12.2016, s. 1).

(81) 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. ***Dostawcy systemów AI wysokiego ryzyka, którzy podlegają obowiązkom dotyczącym systemów zarządzania jakością na mocy odpowiednich sektorowych przepisów Unii, powinni mieć możliwość włączenia elementów systemu zarządzania jakością przewidzianego w niniejszym rozporządzeniu do istniejącego systemu zarządzania jakością przewidzianego w innych sektorowych przepisach Unii. Komplementarność między niniejszym rozporządzeniem a obowiązującymi sektorowymi przepisami Unii powinna być również brana pod uwagę w przyszłych działaniach normalizacyjnych lub wytycznych przyjmowanych przez Komisję.*** Organy publiczne, które oddają do użytku systemy AI wysokiego ryzyka do celów własnych, mogą – w ramach przyjętego, odpowiednio, na szczeblu krajowym lub regionalnym systemu zarządzania jakością – przyjąć i wdrożyć zasady dotyczące systemu zarządzania jakością, z uwzględnieniem specyfiki sektora oraz kompetencji i organizacji danego organu publicznego.

(82) W celu umożliwienia egzekwowania niniejszego rozporządzenia i stworzenia równych warunków działania dla operatorów, a także uwzględniając różne formy udostępniania produktów cyfrowych, należy zapewnić, aby w każdych okolicznościach znajdowała się w Unii mająca w niej siedzibę osoba, która będzie w stanie przekazać organom wszystkie niezbędne informacje dotyczące zgodności danego systemu AI. W związku z tym ▌ dostawcy mający siedzibę w państwach trzecich przed udostępnieniem swoich systemów AI w Unii są zobowiązani wyznaczyć – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego siedzibę w Unii. ***Ten upoważniony przedstawiciel odgrywa kluczową rolę w zapewnianiu zgodności systemów AI wysokiego ryzyka wprowadzanych do obrotu lub oddawanych do użytku w Unii przez dostawców, którzy nie mają siedziby w Unii, oraz w pełnieniu funkcji ich osoby kontaktowej mającej siedzibę w Unii.***

(83) W świetle charakteru i złożoności łańcucha wartości systemów AI oraz zgodnie z nowymi ramami prawnymi konieczne jest zapewnienie pewności prawa i ułatwienie zgodności z niniejszym rozporządzeniem. W związku z tym konieczne jest wyjaśnienie roli i konkretnych obowiązków odpowiednich operatorów w całym łańcuchu wartości, takich jak importerzy i dystrybutorzy, którzy mogą przyczyniać się do rozwoju systemów AI. W niektórych sytuacjach operatorzy ci mogą odgrywać więcej niż jedną rolę jednocześnie i w związku z tym powinni łącznie wypełniać wszystkie odpowiednie obowiązki związane z tymi rolami. Na przykład operator może występować jednocześnie jako dystrybutor i importer.

(84) ***Aby zapewnić pewność prawa, należy wyjaśnić, że w pewnych*** określonych ***warunkach każdego dystrybutora, importera, podmiot stosujący AI lub inną stronę trzecią należy uznać za dostawcę systemu AI wysokiego ryzyka i w związku z tym powinni oni przyjąć na siebie wszystkie związane z tym*** obowiązki. ***Miałoby to miejsce w przypadku, gdy strona ta umieszcza swoją nazwę lub znak towarowy w systemie AI wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku, bez uszczerbku dla ustaleń umownych przewidujących, że podział zawartych w nich obowiązków następuje w inny sposób, lub jeżeli strona ta dokonuje istotnej zmiany w systemie AI wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku, w taki sposób, że pozostaje on systemem AI wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, lub jeżeli zmodyfikuje przeznaczenie systemu AI, w tym systemu AI ogólnego przeznaczenia, który nie został zaklasyfikowany jako system wysokiego ryzyka i został już wprowadzony do obrotu lub oddany do użytku, w taki sposób, że ten system AI staje się systemem wysokiego ryzyka zgodnie z niniejszym rozporządzeniem. Przepisy te powinny mieć zastosowanie bez uszczerbku dla bardziej szczegółowych przepisów określonego unijnego prawodawstwa harmonizacyjnego opartego o nowe ramy prawne, wraz z którymi niniejsze rozporządzenie powinno być stosowane łącznie. Na przykład do systemów AI wysokiego ryzyka będących wyrobami medycznymi w rozumieniu rozporządzenia (UE) 2017/745,*** powinien ***nadal mieć zastosowanie art. 16 ust. 2 tego rozporządzenia stwierdzający, że niektórych zmian nie należy uznawać za modyfikację wyrobu mogącą wpłynąć na jego zgodność z obowiązującymi wymogami***.

(85) ***Systemy AI ogólnego przeznaczenia mogą być wykorzystywane jako samodzielne systemy AI wysokiego ryzyka lub stanowić element innych systemów AI wysokiego ryzyka. W związku z tym z uwagi na ich szczególny charakter i aby zapewnić sprawiedliwy podział obowiązków na całej długości łańcucha wartości AI, dostawcy systemów AI ogólnego przeznaczenia, niezależnie od tego, czy ich systemy są wykorzystywane jako systemy AI wysokiego ryzyka przez innych dostawców czy jako elementy systemów tego rodzaju, powinni ściśle współpracować – chyba że w niniejszym rozporządzeniu przewidziano inaczej – z dostawcami odpowiednich systemów AI wysokiego ryzyka, aby umożliwić im wypełnianie odpowiednich obowiązków wynikających z niniejszego rozporządzenia, oraz z właściwymi organami ustanowionymi na podstawie niniejszego rozporządzenia.***

(86) ***W przypadku gdy zgodnie z warunkami ustanowionymi w niniejszym rozporządzeniu dostawcy, który pierwotnie wprowadził system AI do obrotu lub oddał go do użytku, nie należy już uznawać za dostawcę do celów niniejszego rozporządzenia, a dostawca ten nie wykluczył wyraźnie, że system AI może stać się systemem AI wysokiego ryzyka, ten pierwszy dostawca powinien nadal ściśle współpracować i udostępniać niezbędne informacje oraz zapewniać dostęp techniczny i inną pomoc, których można zasadnie oczekiwać i które są wymagane do wypełnienia obowiązków określonych w niniejszym rozporządzeniu, w szczególności w zakresie wymogów dotyczących oceny zgodności systemów AI wysokiego ryzyka.***

(87) Ponadto w przypadku gdy system AI wysokiego ryzyka będący elementem bezpieczeństwa produktu, który wchodzi w zakres unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych, nie jest wprowadzany do obrotu ani oddawany do użytku niezależnie od tego produktu, producent produktu – w rozumieniu wspomnianych przepisów – powinien wypełniać obowiązki dostawcy ustanowione w niniejszym rozporządzeniu, a w szczególności zapewnić zgodność systemu AI wbudowanego w produkt końcowy z wymogami niniejszego rozporządzenia.

(88) Na całej długości łańcucha wartości AI wiele podmiotów często dostarcza systemy AI, narzędzia i usługi, ale również elementy lub procesy, które są włączane przez dostawcę do systemu AI w różnych celach, w tym trenowania modelu, przekwalifikowania modelu, testowania i oceny modelu, integracji z oprogramowaniem lub innych aspektów rozwoju modelu. Podmioty te mają do odegrania ważną rolę w łańcuchu wartości w stosunku do dostawcy systemu AI wysokiego ryzyka, z którym to systemem zintegrowane są ich systemy AI, narzędzia, usługi, elementy lub procesy; podmioty te powinny zapewnić temu dostawcy w drodze pisemnej umowy niezbędne informacje, zdolności, dostęp techniczny i inną pomoc w oparciu o powszechnie uznany stan wiedzy technicznej, aby umożliwić dostawcy pełne wypełnianie obowiązków określonych w niniejszym rozporządzeniu, bez uszczerbku dla ich własnych praw własności intelektualnej lub tajemnic przedsiębiorstwa.

(89) Strony trzecie udostępniające publicznie narzędzia, usługi, procesy lub elementy AI, inne niż modele AI ogólnego przeznaczenia, nie są zobowiązane do przestrzegania wymogów dotyczących obowiązków na całej długości łańcucha wartości AI, w szczególności wobec dostawcy, który je wykorzystał lub zintegrował, jeżeli te narzędzia, usługi, procesy lub elementy AI są udostępniane na podstawie bezpłatnej i otwartej licencji. Należy zachęcać twórców bezpłatnych i otwartych narzędzi, usług, procesów lub elementów AI, innych niż modele AI ogólnego przeznaczenia, do wdrażania powszechnie przyjętych praktyk w zakresie dokumentacji, takich jak karta modelu i karta charakterystyki, jako sposobu na przyspieszenie wymiany informacji w całym łańcuchu wartości AI, co umożliwi promowanie godnych zaufania systemów AI w Unii.

(90) Komisja mogłaby opracować dobrowolne modelowe postanowienia umowne między dostawcami systemów AI wysokiego ryzyka a stronami trzecimi dostarczającymi narzędzia, usługi, elementy lub procesy, które są wykorzystywane w systemach AI wysokiego ryzyka lub z nimi zintegrowane, i zalecać stosowanie tych modelowych postanowień, aby ułatwić współpracę na całej długości łańcucha wartości. Przy opracowywaniu dobrowolnych modelowych postanowień umownych, Komisja powinna też brać pod uwagę wymogi umowne, które mogą mieć zastosowanie w określonych sektorach lub przypadkach biznesowych.

(91) Ze względu na charakter systemów AI oraz ryzyko dla bezpieczeństwa i praw podstawowych, jakie może wiązać się z ich wykorzystywaniem, ***uwzględniając*** przy tym potrzebę zapewnienia właściwego monitorowania skuteczności działania systemu AI w warunkach rzeczywistych, należy określić szczególne obowiązki ***podmiotów stosujących AI***. ***Podmioty stosujące AI*** powinny w szczególności ***wprowadzić odpowiednie środki techniczne i organizacyjne w celu zapewnienia,*** aby systemy AI wysokiego ryzyka były wykorzystywane przez nich zgodnie z instrukcjami obsługi, a w stosownych przypadkach należy przewidzieć określone inne obowiązki w odniesieniu do monitorowania funkcjonowania systemów AI oraz rejestrowania zdarzeń. ***Ponadto podmioty stosujące AI powinny zapewnić, aby osoby wyznaczone do wdrożenia instrukcji obsługi i nadzoru ze strony człowieka, zgodnie z niniejszym rozporządzeniem, posiadały niezbędne kompetencje, w szczególności odpowiedni poziom kompetencji w zakresie AI oraz odpowiedni poziom przeszkolenia i uprawnień, aby właściwie wykonywać te zadania. Obowiązki te powinny pozostawać bez uszczerbku dla innych wynikających z prawa Unii lub prawa krajowego obowiązków podmiotów stosujących AI w odniesieniu do systemów AI wysokiego ryzyka.***

(92) ***Niniejsze rozporządzenie pozostaje bez uszczerbku dla obowiązków pracodawców w zakresie informowania pracowników lub ich przedstawicieli i konsultowania się z nimi na podstawie krajowego lub unijnego prawa i krajowej lub unijnej praktyki, w tym dyrektywy 2002/14/WE Parlamentu Europejskiego i Rady[40] w sprawie ogólnych ramowych warunków informowania i przeprowadzania konsultacji z pracownikami, na temat decyzji o oddaniu do użytku lub korzystaniu z systemów AI. Nadal konieczne jest zapewnienie pracownikom i ich przedstawicielom informacji na temat planowanego wdrożenia systemów AI wysokiego ryzyka w miejscu pracy, w przypadku gdy warunki dotyczące tych obowiązków w zakresie informowania lub informowania i przeprowadzania konsultacji określone w innych instrumentach prawnych nie są spełnione. Ponadto takie prawo do informacji ma charakter pomocniczy i konieczny w stosunku do leżącego u podstaw niniejszego rozporządzenia celu, jakim jest ochrona praw podstawowych. W związku z tym w niniejszym rozporządzeniu należy ustanowić wymóg informowania w tym zakresie, nie naruszając żadnych istniejących praw pracowników.***

---

40 Dyrektywa 2002/14/WE Parlamentu Europejskiego i Rady z dnia 11 marca 2002 r. ustanawiająca ogólne ramowe warunki informowania i przeprowadzania konsultacji z pracownikami we Wspólnocie Europejskiej – Wspólna deklaracja Parlamentu Europejskiego, Rady i Komisji w sprawie reprezentacji pracowników (Dz.U. L 80 z 23.3.2002, s. 29).

(93) ***Ryzyko związane z systemami AI może wynikać ze sposobu projektowania takich systemów, jak również ze sposobu korzystania z nich. Podmioty stosujące systemy AI wysokiego ryzyka odgrywają zatem kluczową rolę w zapewnianiu ochrony praw podstawowych w uzupełnieniu obowiązków dostawcy podczas opracowywania systemu AI. Podmioty stosujące systemy AI najlepiej rozumieją, jak konkretnie stosowany będzie system AI wysokiego ryzyka, i mogą w związku z tym zidentyfikować potencjalne poważne ryzyko, które nie zostało przewidziane na etapie opracowywania, dzięki bardziej precyzyjnej wiedzy na temat kontekstu stosowania, osób lub grup osób, na które system może wywierać wpływ, w tym grup szczególnie wrażliwych. Podmioty stosujące systemy AI wysokiego ryzyka wymienione w załączniku do niniejszego rozporządzenia również odgrywają kluczową rolę w informowaniu osób fizycznych i powinny – gdy podejmują decyzje lub pomagają w podejmowaniu decyzji dotyczących osób fizycznych, w stosownych przypadkach, informować osoby fizyczne, że podlegają one korzystaniu z systemu AI wysokiego ryzyka. Taka informacja powinna obejmować przeznaczenie systemu i typ podejmowanych przez niego decyzji. Podmiot stosujący AI informuje również osobę fizyczną o przysługującym jej prawie do uzyskania wyjaśnienia, które przewiduje niniejsze rozporządzenie. W odniesieniu do systemów AI wysokiego ryzyka wykorzystywanych do celów ścigania przestępstw obowiązek ten należy realizować zgodnie z art. 13 dyrektywy (UE) 2016/680.***

(94) ***Wszelkie przetwarzanie danych biometrycznych związane z wykorzystywaniem systemów AI do identyfikacji biometrycznej do celów ścigania przestępstw musi być zgodne z art. 10 dyrektywy (UE) 2016/680, który zezwala na takie przetwarzanie wyłącznie wtedy, jeżeli jest to bezwzględnie niezbędne, z zastrzeżeniem odpowiednich zabezpieczeń dla praw i wolności osoby, której dane dotyczą, oraz jeżeli jest to dopuszczone prawem Unii lub prawem państwa członkowskiego. Takie wykorzystanie, jeżeli jest dozwolone, musi być również zgodne z zasadami określonymi w art. 4 ust. 1 dyrektywy (UE) 2016/680, w tym zasadami zgodności z prawem, rzetelności i przejrzystości, celowości, dokładności i ograniczenia przechowywania.***

(95) ***Bez uszczerbku dla mającego zastosowanie prawa Unii, w szczególności rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680, biorąc pod uwagę inwazyjny charakter systemów zdalnej identyfikacji biometrycznej* post factum*, korzystanie z takich systemów podlega zabezpieczeniom. Systemy identyfikacji biometrycznej* post factum *powinny być zawsze wykorzystywane w sposób proporcjonalny, zgodny z prawem i jeżeli jest to bezwzględnie niezbędne, a tym samym ukierunkowane na osoby, które mają zostać zidentyfikowane, na określoną lokalizację i zakres czasowy, oraz opierać się na zamkniętym zbiorze danych pochodzących z legalnie uzyskanych materiałów wideo. W żadnym wypadku systemy zdalnej identyfikacji biometrycznej* post factum *nie powinny być wykorzystywane w ramach ścigania przestępstw w celu prowadzenia masowej inwigilacji. Warunki zdalnej identyfikacji biometrycznej* post factum *nie powinny w żadnym wypadku stanowić podstawy do obchodzenia warunków zakazu i ścisłych wyjątków dotyczących zdalnej identyfikacji biometrycznej w czasie rzeczywistym.***

(96) Aby skutecznie zapewnić ochronę praw podstawowych, podmioty stosujące systemy AI wysokiego ryzyka będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne i operatorzy wdrażający niektóre systemy AI wysokiego ryzyka wymienione w załączniku do niniejszego rozporządzenia, tacy jak podmioty bankowe lub ubezpieczeniowe, powinni przed wprowadzeniem tych systemów do użytku przeprowadzić ocenę skutków w zakresie praw podstawowych. Usługi o charakterze publicznym ważne dla osób fizycznych mogą być również świadczone przez podmioty prywatne. Podmioty prywatne świadczące takie usługi o charakterze publicznym działają w powiązaniu z zadaniami świadczonymi w interesie publicznym, takimi jak edukacja, opieka zdrowotna, usługi społeczne, mieszkalnictwo, sprawowanie wymiaru sprawiedliwości. Celem oceny skutków w zakresie praw podstawowych jest zidentyfikowanie przez podmiot stosujący AI konkretnych rodzajów ryzyka dla praw osób lub grup osób, na które to osoby AI może mieć wpływ, oraz określenie środków, które należy podjąć w przypadku urzeczywistnienia się tego ryzyka. Ocena skutków powinna odnosić się do pierwszego wykorzystania systemu AI wysokiego ryzyka i powinna być aktualizowana, gdy podmiot stosujący AI uzna, że którykolwiek z istotnych czynników uległ zmianie. W ocenie skutków należy określić odpowiednie procesy prowadzone przez podmiot stosujący AI, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem; powinna ona przedstawiać informacje o okresie, w którym system ma być wykorzystywany, i o częstotliwości jego stosowania, a także opis konkretnych kategorii osób fizycznych i grup, na które AI może mieć wpływ w tym konkretnym kontekście użytkowania.

Ocena powinna również obejmować określenie szczególnego ryzyka szkody, które może mieć wpływ na prawa podstawowe tych osób lub grup. Przeprowadzając tę ocenę, podmiot stosujący AI powinien uwzględnić informacje istotne dla właściwej oceny skutków, w tym między innymi informacje podane przez dostawcę systemu AI wysokiego ryzyka w instrukcji obsługi. W świetle zidentyfikowanego ryzyka podmioty stosujące AI powinny określić środki, które należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym na przykład rozwiązania dotyczące zarządzania w tym konkretnym kontekście użytkowania np. dotyczące nadzoru ze strony człowieka zgodnie z instrukcją obsługi lub procedury rozpatrywania skarg i dochodzenia roszczeń, ponieważ mogą one odegrać zasadniczą rolę w ograniczaniu ryzyka dla praw podstawowych w konkretnych przypadkach użycia. Po przeprowadzeniu tej oceny skutków podmiot stosujący AI powinien powiadomić właściwy organ nadzoru rynku. W stosownych przypadkach w celu zebrania odpowiednich informacji niezbędnych do przeprowadzenia oceny skutków podmioty stosujące system AI wysokiego ryzyka, w szczególności gdy systemy AI są wykorzystywane w sektorze publicznym, mogą angażować odpowiednie zainteresowane strony, w tym przedstawicieli grup osób, na które system AI może mieć wpływ, niezależnych ekspertów i organizacje społeczeństwa obywatelskiego w przeprowadzanie takich ocen skutków i opracowywanie środków, które należy wprowadzić w przypadku urzeczywistnienia się ryzyka. Europejski Urząd ds. Sztucznej Inteligencji („Urząd ds. AI”) powinien opracować wzór kwestionariusza, by ułatwić przestrzeganie przepisów i zmniejszyć obciążenia administracyjne dla podmiotów stosujących AI.

(97) ***Należy jasno zdefiniować pojęcie modeli AI ogólnego przeznaczenia i oddzielić je od pojęcia systemów AI, aby zapewnić pewność prawa. Definicja powinna opierać się na kluczowych cechach funkcjonalnych modelu AI ogólnego przeznaczenia, w szczególności na ogólnym charakterze i zdolności do kompetentnego wykonywania szerokiego zakresu różnych zadań. Modele te są zazwyczaj trenowane w oparciu o dużą ilość danych za pomocą różnych metod, takich jak uczenie się samodzielnie nadzorowane, nienadzorowane lub uczenie przez wzmacnianie. Modele AI ogólnego przeznaczenia mogą być wprowadzane do obrotu na różne sposoby, w tym za pośrednictwem bibliotek, interfejsów programowania aplikacji (API), przez bezpośrednie pobieranie lub w wersji fizycznej. Modele te mogą być dalej modyfikowane lub dostosowywane jako baza do tworzenia nowych modeli. Chociaż modele AI są zasadniczymi elementami systemów AI, nie stanowią same w sobie systemów AI. Aby model AI mógł stać się systemem AI należy dodać do niego dodatkowe elementy, takie jak na przykład interfejs użytkownika. Modele AI są zwykle zintegrowane z systemami AI i stanowią ich część. Niniejsze rozporządzenie ustanawia przepisy szczegółowe dotyczące modeli AI ogólnego przeznaczenia oraz modeli AI ogólnego przeznaczenia, które stwarzają ryzyko systemowe, a przepisy te powinny mieć zastosowanie również wtedy, gdy modele te są zintegrowane z systemem AI lub stanowią jego część. Należy rozumieć, że obowiązki dostawców modeli AI ogólnego przeznaczenia powinny mieć zastosowanie od momentu wprowadzenia do obrotu modeli AI ogólnego przeznaczenia.***

W przypadku gdy dostawca modelu AI ogólnego przeznaczenia zintegruje własny model z własnym systemem AI, który jest udostępniany na rynku lub oddany do użytku, model ten należy uznać za wprowadzony do obrotu i w związku z tym obowiązki dotyczące modeli określone w niniejszym rozporządzeniu powinny nadal mieć zastosowanie obok obowiązków dotyczących systemów AI. Obowiązki określone w odniesieniu do modeli nie powinny w żadnym przypadku mieć zastosowania, jeżeli model własny jest stosowany w czysto wewnętrznych procesach, które nie są niezbędne do dostarczania produktu lub usługi osobom trzecim, a prawa osób fizycznych nie są naruszone. Biorąc pod uwagę ich potencjalne znacząco negatywne skutki, modele AI ogólnego przeznaczenia z ryzykiem systemowym powinny zawsze podlegać odpowiednim obowiązkom wynikającym z niniejszego rozporządzenia. Definicja nie powinna obejmować modeli AI wykorzystywanych przed wprowadzeniem ich do obrotu wyłącznie do celów działalności badawczo-rozwojowej i tworzenia prototypów. Pozostaje to bez uszczerbku dla obowiązku przestrzegania niniejszego rozporządzenia w przypadku wprowadzenia do obrotu danego modelu w następstwie takich działań.

(98) Mając na uwadze, że ogólny charakter modelu można określić między innymi na podstawie liczby parametrów, należy uznać, że modele o co najmniej miliardzie parametrów i trenowane w oparciu o dużą ilość danych z wykorzystaniem nadzoru własnego na dużą skalę są bardzo ogólne i kompetentnie wykonują szeroki zakres różnych zadań.

(99) Duże generatywne modele AI są typowym przykładem modelu AI ogólnego przeznaczenia, biorąc pod uwagę, że umożliwiają elastyczne generowanie treści, np. w postaci tekstu, dźwięku, obrazów lub materiałów wideo i mogą z łatwością wykonywać szeroki zakres różnych zadań.

(100) Jeżeli model AI ogólnego przeznaczenia jest zintegrowany z systemem AI lub stanowi jego część, system ten należy uznać za system AI ogólnego przeznaczenia, jeżeli w wyniku zintegrowania modelu system ten może służyć różnym celom. System AI ogólnego przeznaczenia może być wykorzystywany bezpośrednio lub być zintegrowany z innymi systemami AI.

(101) Dostawcy modeli AI ogólnego przeznaczenia odgrywają szczególną rolę i ponoszą szczególną odpowiedzialność na całej długości łańcucha wartości AI, ponieważ modele, które oferują, mogą stanowić podstawę szeregu systemów niższego szczebla, często zapewnianych przez dostawców niższego szczebla, które to systemy wymagają dobrego zrozumienia modeli i ich zdolności, zarówno by umożliwić integrację takich modeli z ich produktami, jak i by wypełnić obowiązki wynikające z niniejszego rozporządzenia lub innych przepisów. W związku z tym należy ustanowić proporcjonalne środki w zakresie przejrzystości, w tym sporządzanie i aktualizowanie dokumentacji oraz dostarczanie informacji na temat modelu AI ogólnego przeznaczenia do jego stosowania przez dostawców niższego szczebla. Dostawca modelu AI ogólnego przeznaczenia powinien przygotować i aktualizować dokumentację techniczną w celu udostępnienia jej na żądanie Urzędowi ds. AI i właściwym organom krajowym. Minimalny zestaw elementów do uwzględnienia w takiej dokumentacji należy określić w załącznikach do niniejszego rozporządzenia. Komisja powinna być uprawniona do zmiany tych załączników w drodze aktów delegowanych w świetle postępu technicznego.

(102) Oprogramowanie i dane, w tym modele, wydawane na podstawie bezpłatnej i otwartej licencji, która umożliwia ich ogólne upowszechnianie i zezwala użytkownikom na swobodny dostęp do nich, ich wykorzystywanie, modyfikację i ich redystrybucję lub ich zmodyfikowanych wersji, mogą przyczynić się do badań naukowych i innowacji na rynku oraz zapewnić gospodarce Unii znaczne możliwości wzrostu. Należy uznać, że modele AI ogólnego przeznaczenia udostępniane na podstawie bezpłatnych i otwartych licencji zapewniają wysoki poziom przejrzystości i otwartości, jeżeli ich parametry, w tym wagi, informacje na temat architektury modelu oraz informacje na temat wykorzystania modelu, są publicznie dostępne. Licencję należy uznać za bezpłatną i otwartą również wtedy, gdy umożliwia użytkownikom obsługę, kopiowanie, dystrybucję, badanie, zmianę i ulepszanie oprogramowania i danych, w tym modeli, pod warunkiem że umieszcza się wzmiankę o pierwotnym dostawcy modelu i że przestrzega się identycznych lub porównywalnych warunków dystrybucji.

(103) Bezpłatne i otwarte elementy AI obejmują oprogramowanie i dane, w tym modele i modele AI ogólnego przeznaczenia, narzędzia, usługi lub procesy systemu AI. Bezpłatne i otwarte elementy AI mogą być dostarczane za pośrednictwem różnych kanałów, w tym opracowywane w otwartych repozytoriach. Do celów niniejszego rozporządzenia elementy AI, które są dostarczane odpłatnie lub w inny sposób monetyzowane, w tym poprzez zapewnianie wsparcia technicznego lub innych usług związanych z elementem AI, np. poprzez platformy oprogramowania, lub wykorzystywanie danych osobowych z powodów innych niż wyłącznie poprawa bezpieczeństwa, kompatybilności lub interoperacyjności oprogramowania, z wyjątkiem transakcji między mikroprzedsiębiorstwami, nie powinny korzystać ze zwolnień przewidzianych w odniesieniu do bezpłatnych i otwartych elementów AI. Fakt udostępniania elementów AI w otwartych repozytoriach nie powinien sam w sobie stanowić monetyzacji.

(104) ***Dostawcy modeli AI ogólnego przeznaczenia, które są udostępniane na podstawie bezpłatnej i otwartej licencji i których parametry, w tym wagi, informacje o architekturze modelu oraz informacje na temat korzystania z modelu, są udostępniane publicznie, powinni podlegać zwolnieniom w odniesieniu do wymogów związanych z przejrzystością nałożonych na modele AI ogólnego przeznaczenia, chyba że można uznać, że modele te stwarzają ryzyko systemowe, w którym to przypadku przejrzystość modelu i fakt, że towarzyszy mu licencja otwartego oprogramowania, nie jest wystarczającym powodem zwolnienia ze zgodności z obowiązkami wynikającymi z niniejszego rozporządzenia. W każdym razie, biorąc pod uwagę, że udostępnianie modeli AI ogólnego przeznaczenia na podstawie bezpłatnej i otwartej licencji niekoniecznie prowadzi do ujawnienia istotnych informacji na temat zbioru danych wykorzystywanego do trenowania lub dostosowywania modelu oraz na temat sposobu zapewnienia tym samym zgodności z prawem autorskim, przewidziane w odniesieniu do modeli AI ogólnego przeznaczenia zwolnienie z obowiązku zgodności z wymogami związanymi z przejrzystością nie powinno dotyczyć obowiązku sporządzenia streszczenia dotyczącego treści wykorzystywanych do trenowania modeli oraz obowiązku wprowadzenia polityki zgodnej z unijnym prawem autorskim, w szczególności w celu zidentyfikowania i zastosowania się do zastrzeżenia praw zgodnie z art. 4 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790[41].***

---

41 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.U. L 130 z 17.5.2019, s. 92).

(105) Modele ogólnego przeznaczenia, w szczególności duże modele generatywne, zdolne do generowania tekstów, obrazów i innych treści, stwarzają wyjątkowe możliwości w zakresie innowacji, ale także wyzwania dla artystów, autorów i innych twórców oraz w odniesieniu do sposobu tworzenia, rozpowszechniania, wykorzystywania i konsumowania ich treści kreatywnych. Opracowanie i trenowanie takich modeli wymaga dostępu do ogromnych ilości tekstów, obrazów, materiałów wideo i innych danych. Techniki eksploracji tekstów i danych mogą być w tym kontekście szeroko wykorzystywane do wyszukiwania i analizy takich treści, które mogą być chronione prawem autorskim i prawami pokrewnymi. Każde wykorzystanie treści chronionych prawem autorskim wymaga zezwolenia danego podmiotu praw, chyba że zastosowanie mają odpowiednie wyjątki i ograniczenia dotyczące praw autorskich. Na mocy dyrektywy (UE) 2019/790 wprowadzono wyjątki i ograniczenia umożliwiające, pod pewnymi warunkami, zwielokrotnianie i pobieranie utworów lub innych przedmiotów objętych ochroną do celów eksploracji tekstów i danych. Zgodnie z tymi przepisami podmioty uprawnione mogą zastrzec swoje prawa do swoich utworów lub innych przedmiotów objętych ochroną, aby zapobiec eksploracji tekstów i danych, chyba że odbywa się to do celów badań naukowych. W przypadku gdy prawo do wyłączenia z eksploracji zostało w odpowiedni sposób wyraźnie zastrzeżone, dostawcy modeli AI ogólnego przeznaczenia muszą uzyskać zezwolenie od podmiotów uprawnionych, jeżeli chcą dokonywać eksploracji tekstów i danych odnośnie do takich utworów.

(106) Dostawcy wprowadzający modele AI ogólnego przeznaczenia do obrotu w Unii powinni zapewnić zgodność z odpowiednimi obowiązkami określonymi w niniejszym rozporządzeniu. W tym celu dostawcy modeli AI ogólnego przeznaczenia powinni wprowadzić politykę w celu uzyskania zgodności z prawem Unii dotyczącym prawa autorskiego i praw pokrewnych, w szczególności w celu identyfikacji i przestrzegania zastrzeżeń praw wyrażonych przez podmioty uprawnione zgodnie z art. 4 ust. 3 dyrektywy (UE) 2019/790. Każdy dostawca wprowadzający do obrotu w Unii model AI ogólnego przeznaczenia powinien przestrzegać tego obowiązku, niezależnie od jurysdykcji, w której mają miejsce czynności regulowane prawem autorskim stanowiące podstawę trenowania tych modeli AI ogólnego przeznaczenia. Jest to konieczne do zapewnienia równych warunków działania dostawcom modeli AI ogólnego przeznaczenia, tak aby żaden dostawca nie mógł uzyskać przewagi konkurencyjnej na rynku unijnym poprzez stosowanie niższych standardów praw autorskich niż normy przewidziane w Unii.

(107) W celu zwiększenia przejrzystości dotyczącej danych wykorzystywanych do wstępnego trenowania i trenowania modeli AI ogólnego przeznaczenia, w tym w zakresie tekstów i danych chronionych prawem autorskim, właściwe jest, aby dostawcy takich modeli sporządzali i udostępniali publicznie wystarczająco szczegółowe streszczenie na temat treści wykorzystywanych do trenowania modelu ogólnego przeznaczenia. Przy należytym uwzględnieniu potrzeby ochrony tajemnic przedsiębiorstwa i poufnych informacji handlowych streszczenie to nie powinno skupiać się na szczegółach technicznych, lecz mieć zasadniczo kompleksowy charakter, aby ułatwić stronom mającym uzasadnione interesy, w tym posiadaczom praw autorskich, wykonywanie i egzekwowanie swoich praw wynikających z prawa Unii; streszczenie to powinno więc na przykład wymieniać główne zbiory danych, które wykorzystano do trenowania modelu, takie jak duże prywatne lub publiczne bazy lub archiwa danych, oraz powinno zawierać opisowe wyjaśnienie innych wykorzystanych źródeł danych. Urząd ds. AI powinien przedstawić wzór streszczenia, który powinien być prosty i skuteczny oraz umożliwiać dostawcy przedstawienie wymaganego streszczenia w formie opisowej.

(108) Urząd ds. AI powinien monitorować, czy dostawca wypełnił obowiązki nałożone na dostawców modeli AI ogólnego przeznaczenia dotyczące wprowadzenia polityki w celu uzyskania zgodności z unijnym prawem autorskim i podania do wiadomości publicznej streszczenia na temat treści wykorzystywanych do trenowania, jednak nie powinien weryfikować danych treningowych pod kątem przestrzegania praw autorskich ani przystępować do oceny tych danych w podziale na poszczególne utwory. Niniejsze rozporządzenie nie wpływa na egzekwowanie przepisów dotyczących praw autorskich przewidzianych w prawie Unii.

(109) Wypełnianie obowiązków mających zastosowanie do dostawców modeli AI ogólnego przeznaczenia powinno być współmierne i proporcjonalne do rodzaju dostawcy modeli, z wyłączeniem konieczności ich wypełniania przez osoby, które opracowują lub wykorzystują modele do celów pozazawodowych lub badań naukowych – osoby te należy jednak zachęcać do dobrowolnego spełniania tych wymogów. Bez uszczerbku dla unijnego prawa autorskiego wypełnianie tych obowiązków powinno odbywać się przy należytym uwzględnieniu wielkości dostawcy i być realizowane w oparciu o uproszczone sposoby przestrzegania przepisów dla MŚP, w tym przedsiębiorstw typu start-up, które nie powinny wiązać się z nadmiernymi kosztami i zniechęcać do korzystania z takich modeli. W przypadku modyfikacji lub dostosowywania modelu obowiązki dostawców powinny być ograniczone do tej modyfikacji lub dostosowania modelu, na przykład poprzez uzupełnienie już istniejącej dokumentacji technicznej o informacje na temat modyfikacji, w tym nowych źródeł danych treningowych, w celu wypełnienia obowiązków związanych z łańcuchem wartości przewidzianych w niniejszym rozporządzeniu.

(110) Modele AI ogólnego przeznaczenia mogą stwarzać ryzyko systemowe, które obejmuje między innymi wszelkie rzeczywiste lub dające się racjonalnie przewidzieć negatywne skutki poważnych awarii, zakłóceń w sektorach krytycznych oraz poważne konsekwencje dla zdrowia i bezpieczeństwa publicznego; wszelkie rzeczywiste lub dające się racjonalnie przewidzieć negatywne skutki dla procesów demokratycznych, bezpieczeństwa publicznego i gospodarczego; rozpowszechnianie nielegalnych, fałszywych lub dyskryminujących treści. Należy rozumieć, że ryzyko systemowe wzrasta wraz ze zdolnościami i zasięgiem modelu, może wystąpić w całym cyklu życia modelu i jest uzależnione od warunków niewłaściwego wykorzystania, niezawodności, uczciwości i bezpieczeństwa modelu, stopnia jego autonomii, dostępu do narzędzi, stosowania nowatorskich lub połączonych metod, strategii udostępniania i dystrybucji, ewentualnych możliwości w zakresie usuwania zabezpieczeń i innych czynników. W szczególności podejścia międzynarodowe do tej pory wskazywały na potrzebę zwrócenia uwagi na zagrożenia wynikające z potencjalnego umyślnego niewłaściwego wykorzystania lub niezamierzonych dotyczących kontroli kwestii związanych z dostosowaniem się do zamiaru człowieka; zagrożenia chemiczne, biologiczne, radiologiczne i jądrowe, takie jak sposoby obniżania barier wejścia na rynek, w tym w zakresie opracowywania, projektowania, nabywania lub stosowania broni; ofensywne zdolności w zakresie cyberbezpieczeństwa, takie jak sposoby wykrywania, wykorzystywania lub operacyjnego stosowania podatności; skutki interakcji i wykorzystania narzędzi, w tym na przykład zdolność do kontrolowania systemów fizycznych i zakłócania infrastruktury krytycznej; ryzyko związane ze sporządzaniem kopii własnych przez modele lub samoreplikacji lub wynikające z trenowania innych modeli przez dany model; sposoby, w jakie modele mogą powodować szkodliwą stronniczość i dyskryminację zagrażające jednostkom, społecznościom lub społeczeństwom; ułatwianie dezinformacji lub naruszanie prywatności, co przedstawia zagrożenie dla wartości demokratycznych i praw człowieka; ryzyko, że dane wydarzenie może spowodować reakcję łańcuchową o znacznych negatywnych skutkach, które mogą mieć wpływ nawet na całe miasta, obszary działań lub całe społeczności.

(111) Należy ustanowić metodykę klasyfikacji modeli AI ogólnego przeznaczenia jako modeli AI ogólnego przeznaczenia z ryzykiem systemowym. Ponieważ ryzyko systemowe wynika ze szczególnie wysokich zdolności, należy uznać, że model AI ogólnego przeznaczenia stwarza ryzyko systemowe, jeżeli wykazuje on zdolności dużego oddziaływania, oceniane na podstawie odpowiednich narzędzi i metod technicznych, lub jeżeli ze względu na swój zasięg ma znaczący wpływ na rynek wewnętrzny. Zdolności dużego oddziaływania w przypadku modeli AI ogólnego przeznaczenia oznaczają zdolności, które dorównują zdolnościom zapisanym w najbardziej zaawansowanych modelach AI ogólnego przeznaczenia lub je przewyższają. Pełny zakres zdolności danego modelu można lepiej zrozumieć po jego udostępnieniu na rynku lub po tym, jak użytkownicy wejdą w interakcję z modelem. Zgodnie z aktualnym stanem wiedzy technicznej w momencie wejścia w życie niniejszego rozporządzenia jednym ze sposób przybliżonego określenia zdolności modelu jest łączna liczba obliczeń wykorzystanych do trenowania modelu AI ogólnego zastosowania wyrażona w operacjach zmiennoprzecinkowych („FLOP”). Liczba obliczeń wykorzystanych do trenowania obejmuje obliczenia stosowane w odniesieniu do wszystkich działań i metod, które mają na celu zwiększenie zdolności modelu przed wdrożeniem, takich jak trenowanie wstępne, generowanie danych syntetycznych i dostosowywania. W związku z tym należy określić próg minimalny FLOP, który, jeżeli zostanie spełniony przez model AI ogólnego przeznaczenia, pozwoli założyć, że model ten jest modelem AI ogólnego przeznaczenia z ryzykiem systemowym. Próg ten powinien być z czasem dostosowywany w celu odzwierciedlenia zmian technologicznych i przemysłowych, takich jak ulepszenia algorytmiczne lub większa wydajność sprzętu, i powinien zostać uzupełniony o poziomy odniesienia i wskaźniki dotyczące zdolności modelu.

W tym celu Urząd ds. AI powinien współpracować ze środowiskiem naukowym, przemysłem, społeczeństwem obywatelskim i innymi ekspertami. Progi, a także narzędzia i poziomy odniesienia na potrzeby oceny zdolności dużego oddziaływania powinny zapewniać mocne podstawy przewidywania ogólnego charakteru, zdolności i związanego z nimi ryzyka systemowego modeli AI ogólnego przeznaczenia – mogą też rzutować na sposób, w jaki model zostanie wprowadzony do obrotu lub na liczbę użytkowników, na które model ten może mieć wpływ. Aby uzupełnić te mechanizmy, Komisja powinna mieć możliwość podejmowania indywidualnych decyzji w sprawie uznania modelu AI ogólnego przeznaczenia za model AI ogólnego przeznaczenia z ryzykiem systemowym, jeżeli okaże się, że zdolności lub wpływ takiego modelu są równoważne z tymi, które określa ustalony próg. Decyzję tę należy podjąć na podstawie ogólnej oceny kryteriów do celów uznawania modeli AI ogólnego przeznaczenia za modele z ryzykiem systemowym, określonych w załączniku do niniejszego rozporządzenia, takich jak jakość lub wielkość zbioru danych treningowych, liczba użytkowników biznesowych i końcowych, format danych wejściowych i wyjściowych modelu, stopień autonomii i skalowalności lub narzędzia, do których ma dostęp. Na uzasadniony wniosek dostawcy, którego model został uznany za model AI ogólnego przeznaczenia z ryzykiem systemowym, Komisja powinna odnieść się do tego wniosku i może podjąć decyzję o ponownej ocenie, czy model AI ogólnego przeznaczenia nadal można uznać za stwarzający ryzyko systemowe.

(112) Konieczne jest również doprecyzowanie procedury klasyfikacji modelu AI ogólnego zastosowania z ryzykiem systemowym. Model AI ogólnego przeznaczenia, do którego ma zastosowanie próg dotyczący zdolności dużego oddziaływania, należy uznać za model AI ogólnego przeznaczenia z ryzykiem systemowym. Dostawca powinien powiadomić Urząd ds. AI najpóźniej dwa tygodnie od momentu spełnienia kryteriów lub po uzyskaniu wiedzy, że model AI ogólnego przeznaczenia będzie spełniał kryteria prowadzące do takiego założenia. Jest to szczególnie istotne w odniesieniu do progu wyrażonego liczbą FLOP, ponieważ trenowanie modeli AI ogólnego przeznaczenia wymaga znacznego planowania, co obejmuje przydział z góry zasobów obliczeniowych, w związku z czym dostawcy modeli AI ogólnego przeznaczenia są w stanie stwierdzić, czy ich model osiągnąłby ten próg przed zakończeniem trenowania. W kontekście tego zgłoszenia dostawca powinien móc wykazać, że ze względu na swoje szczególne cechy model AI ogólnego przeznaczenia wyjątkowo nie stwarza ryzyka systemowego, a zatem nie powinien być zaklasyfikowany jako model AI ogólnego przeznaczenia z ryzykiem systemowym. Zgłoszenia te to cenne informacje, które umożliwiają Urzędowi ds. AI przewidywanie, że modele AI sztucznej inteligencji ogólnego przeznaczenia z ryzykiem systemowym zostaną wprowadzone do obrotu, dostawcy mogą zatem rozpocząć współpracę z Urzędem ds. AI na wczesnym etapie. Informacje te są szczególnie ważne w odniesieniu do modeli AI ogólnego przeznaczenia, które mają zostać udostępnione jako otwarte oprogramowanie, zważywszy na to, że wdrożenie środków niezbędnych do zapewnienia zgodności z obowiązkami wynikającymi z niniejszego rozporządzenia może być trudniejsze po udostępnieniu modelu otwartego oprogramowania.

(113) Jeżeli Komisja dowie się o tym, że model AI ogólnego przeznaczenia spełnia kryteria, by zostać zaklasyfikowany jako model o ogólnym przeznaczeniu z ryzykiem systemowym, czego wcześniej nie było wiadomo lub w przypadku gdy właściwy dostawca nie wywiązał się z obowiązku powiadomienia o tym Komisji, Komisja powinna być uprawniona do uznania tego modelu za model o ogólnym przeznaczeniu z ryzykiem systemowym. Obok działań monitorujących prowadzonych przez Urząd ds. AI powinien istnieć mechanizm, w ramach którego panel naukowy za pośrednictwem ostrzeżeń kwalifikowanych informuje Urząd ds. AI o modelach AI ogólnego przeznaczenia, które należy ewentualnie zaklasyfikować jako modele AI ogólnego przeznaczenia z ryzykiem systemowym.

(114) Dostawcy modeli AI ogólnego przeznaczenia stwarzających ryzyko systemowe powinni podlegać nie tylko obowiązkom nałożonym na dostawców modeli AI ogólnego przeznaczenia, ale także obowiązkom mającym na celu identyfikację i ograniczenie ryzyka systemowego oraz zapewnienie odpowiedniego poziomu ochrony cyberbezpieczeństwa, niezależnie od tego, czy modele te są dostarczane jako samodzielne modele czy wbudowane w system AI lub w produkt. Aby osiągnąć te cele, w niniejszym rozporządzeniu należy zobowiązać dostawców do przeprowadzania niezbędnych ocen modeli, w szczególności przed ich pierwszym wprowadzeniem do obrotu, w tym przeprowadzania wobec modeli i dokumentowania testów kontradyktoryjnych, również, w stosownych przypadkach, w drodze wewnętrznych lub niezależnych testów zewnętrznych. Ponadto dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym powinni stale oceniać i ograniczać ryzyko systemowe, w tym na przykład poprzez wprowadzanie strategii zarządzania ryzykiem, takich jak procesy rozliczalności i zarządzania, wdrażanie monitorowania po wprowadzeniu do obrotu, podejmowanie odpowiednich środków w całym cyklu życia modelu oraz współpracę z odpowiednimi podmiotami na całej długości łańcucha wartości AI.

(115) Dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym powinni oceniać i ograniczać to ewentualne ryzyko systemowe. Jeżeli pomimo wysiłków na rzecz zidentyfikowania ryzyka związanego z modelem AI ogólnego przeznaczenia, który może stwarzać ryzyko systemowe, i pomimo wysiłków na rzecz zapobieżenia mu, w wyniku opracowania lub zastosowania modelu wystąpi poważny incydent, dostawca modelu AI ogólnego przeznaczenia powinien bez zbędnej zwłoki zacząć śledzić jego przebieg i zgłosić wszelkie istotne informacje i możliwe środki naprawcze Komisji i właściwym organom krajowym. Ponadto dostawcy powinni zapewnić odpowiedni poziom ochrony cyberbezpieczeństwa w odniesieniu do modelu i jego infrastruktury fizycznej, w stosownych przypadkach, w całym cyklu życia modelu. Ochrona cyberbezpieczeństwa w kontekście ryzyka systemowego związanego ze złośliwym wykorzystaniem lub atakami powinna należycie uwzględniać przypadkowe przecieki modelu, nieuprawnione przypadki udostępnienia, obchodzenie środków bezpieczeństwa oraz ochronę przed cyberatakami, nieuprawnionym dostępem lub kradzieżą modelu. Ochronę tę można ułatwić poprzez zabezpieczenie wag modeli, algorytmów, serwerów i zbiorów danych, na przykład za pomocą operacyjnych środków bezpieczeństwa na rzecz bezpieczeństwa informacji, konkretnych polityk cyberbezpieczeństwa, odpowiednich rozwiązań technicznych i ustanowionych rozwiązań oraz kontroli dostępu fizycznego i w cyberprzestrzeni, odpowiednio do danych okoliczności i związanego z nimi ryzyka.

(116) Urząd ds. AI powinien wspierać i ułatwiać opracowywanie, przegląd i dostosowywanie kodeksów praktyk, z uwzględnieniem podejść międzynarodowych. Do udziału można by zaprosić wszystkich dostawców modeli AI ogólnego przeznaczenia. W celu zapewnienia, aby kodeksy praktyk odzwierciedlały aktualny stan wiedzy technicznej i należycie uwzględniały różne punkty widzenia, przy opracowania takich kodeksów Urząd ds. AI powinien współpracować z odpowiednimi właściwymi organami krajowymi i mógłby, w stosownych przypadkach, konsultować się z organizacjami społeczeństwa obywatelskiego i innymi odpowiednimi zainteresowanymi stronami i ekspertami, w tym z panelem naukowym. Kodeksy praktyk powinny obejmować obowiązki dostawców modeli AI ogólnego przeznaczenia i modeli ogólnego przeznaczenia stwarzających ryzyko systemowe. Ponadto w odniesieniu do ryzyka systemowego kodeksy praktyk powinny pomóc w ustanowieniu na poziomie Unii klasyfikacji tego ryzyka pod względem jego różnych rodzajów i charakteru, w tym jego źródeł. Kodeksy praktyk powinny również koncentrować się na konkretnych środkach oceny i ograniczania ryzyka.

(117) ***Kodeksy praktyk powinny stanowić jedno z głównych narzędzi służących zapewnieniu właściwej zgodności z obowiązkami przewidzianymi w niniejszym rozporządzeniu w odniesieniu do dostawców modeli AI ogólnego przeznaczenia. Dostawcy powinni móc polegać na kodeksach praktyk w celu wykazania zgodności z obowiązkami. W drodze aktów wykonawczych Komisja może podjąć decyzję o zatwierdzeniu kodeksu praktyk i nadaniu mu ogólnej ważności w Unii lub ewentualnie o ustanowieniu wspólnych zasad dotyczących wdrażania odpowiednich obowiązków, jeżeli do czasu rozpoczęcia stosowania niniejszego rozporządzenia prace nad kodeksem praktyk nie mogą zostać sfinalizowane lub jeśli Urząd ds. AI uzna, że kodeks ten nie jest wystarczający. Po opublikowaniu normy zharmonizowanej i po tym jak Urząd ds. AI oceni ją jako właściwą, by objąć odpowiednie obowiązki, spełnienie wymogów europejskiej normy zharmonizowanej powinno w odniesieniu do dostawców oznaczać domniemanie zgodności. Dostawcy modeli AI ogólnego przeznaczenia powinni ponadto być w stanie wykazać zgodność za pomocą odpowiednich alternatywnych środków, jeżeli kodeksy praktyk lub normy zharmonizowane nie są dostępne lub jeśli zdecydują się na nich nie polegać.***

(118) Niniejsze rozporządzenie reguluje systemy i modele AI, nakładając określone wymogi i obowiązki na odpowiednie podmioty rynkowe, które wprowadzają je do obrotu, oddają do użytku lub wykorzystują w Unii, i uzupełnia w ten sposób obowiązki dostawców usług pośrednich, którzy włączają takie systemy lub modele do swoich usług regulowanych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2065[42]. W zakresie, w jakim takie systemy lub modele są wbudowane we wskazane bardzo duże platformy internetowe lub bardzo duże wyszukiwarki internetowe, podlegają one ramom zarządzania ryzykiem przewidzianym w rozporządzeniu (UE) 2022/2065. W związku z tym należy domniemywać, że odpowiednie obowiązki wynikające z niniejszego rozporządzenia zostały spełnione, chyba że w takich modelach pojawi się i zostanie zidentyfikowane znaczące ryzyko systemowe nieobjęte rozporządzeniem (UE) 2022/2065. W tych ramach dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych są zobowiązani do oceny potencjalnego ryzyka systemowego wynikającego z projektu, funkcjonowania i wykorzystania ich usług, w tym tego, w jaki sposób projekt systemów algorytmicznych wykorzystywanych w danej usłudze może przyczynić się do powstania takiego ryzyka, a także ryzyka systemowego wynikającego z potencjalnego nadużywania ich usług. Dostawcy ci są również zobowiązani podjąć odpowiednie środki ograniczające to ryzyko z poszanowaniem praw podstawowych.

---

42 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), (Dz.U. L 277 z 27.10.2022, s. 1.).

(119) Biorąc pod uwagę szybkie tempo innowacji i rozwój technologiczny usług cyfrowych objętych różnymi instrumentami prawa Unii, w szczególności mając na uwadze wykorzystanie tych usług oraz zrozumienie, kto jest ich odbiorcą, systemy AI podlegające niniejszemu rozporządzeniu mogą być oferowane jako usługi pośrednie lub ich części w rozumieniu rozporządzenia (UE) 2022/2065, które należy postrzegać w sposób neutralny pod względem technologicznym. Na przykład systemy AI mogą być wykorzystywane w roli wyszukiwarek internetowych, w szczególności w zakresie, w jakim system AI, taki jak chatbot internetowy, zasadniczo przeprowadza wyszukiwanie wszystkich stron internetowych, a następnie włącza wyniki do swojej istniejącej wiedzy i wykorzystuje zaktualizowaną wiedzę do wygenerowania jednego wyniku, który łączy różne źródła informacji.

(120) Ponadto obowiązki nałożone w niniejszym rozporządzeniu na dostawców i podmioty stosujące niektóre systemy AI, by umożliwić wykrywanie i ujawnianie, że wyniki tych systemów są sztucznie generowane lub zmanipulowane, są szczególnie istotne dla ułatwienia skutecznego wdrożenia rozporządzenia (UE) 2022/2065. Dotyczy to w szczególności obowiązków dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych w zakresie identyfikowania i ograniczania ryzyka systemowego, które może wynikać z rozpowszechniania treści sztucznie wygenerowanych lub zmanipulowanych, w szczególności ryzyka faktycznego lub przewidywalnego negatywnego wpływu na procesy demokratyczne, dyskurs obywatelski i procesy wyborcze, w tym poprzez stosowanie dezinformacji.

(121) Kluczową rolę w dostarczaniu dostawcom rozwiązań technicznych ***– zgodnie z aktualnym stanem wiedzy technicznej –*** w celu zapewnienia zgodności z niniejszym rozporządzeniem powinna odgrywać normalizacja***, tak aby promować innowacje oraz konkurencyjność i wzrost gospodarczy na jednolitym rynku***. Zgodność z normami zharmonizowanymi określonymi w art. 2 pkt 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012[43]***, które z założenia mają odzwierciedlać stan wiedzy technicznej,*** powinna stanowić dla dostawców sposób wykazania zgodności z wymogami niniejszego rozporządzenia. ***Należy zatem zachęcać do zrównoważonej reprezentacji interesów przy angażowaniu w opracowywanie norm wszystkich zainteresowanych stron, w szczególności MŚP, organizacji konsumenckich oraz zainteresowanych stron działających na rzecz ochrony środowiska i społeczeństwa zgodnie z art. 5 i 6 rozporządzenia (UE) nr 1025/2012. Aby ułatwić osiąganie zgodności, wnioski o normalizację powinny być wydawane przez Komisję bez zbędnej zwłoki. Przygotowując wniosek o normalizację, Komisja powinna skonsultować się z forum doradczym i Radą ds. AI, aby zebrać odpowiednią wiedzę fachową.*** Jednakże w ***przypadku braku odpowiednich odniesień do norm zharmonizowanych*** Komisja ***powinna mieć możliwość ustanowienia, w drodze aktów wykonawczych i po konsultacji z forum doradczym, wspólnych specyfikacji dotyczących niektórych wymogów określonych w niniejszym rozporządzeniu.***

---

43 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).

Ta wspólna ***specyfikacja powinna stanowić wyjątkowe rozwiązanie awaryjne ułatwiające dostawcy spełnienie wymogów niniejszego rozporządzenia, w przypadku gdy wniosek o normalizację nie został zaakceptowany przez żadną z europejskich organizacji normalizacyjnych lub gdy odpowiednie normy zharmonizowane w niewystarczającym stopniu uwzględniają obawy dotyczące praw podstawowych lub gdy normy*** zharmonizowane ***nie są zgodne z wnioskiem, lub gdy występują opóźnienia w przyjęciu odpowiedniej normy zharmonizowanej***. ***Jeżeli opóźnienie w przyjęciu normy zharmonizowanej wynika ze złożoności technicznej danej normy, Komisja powinna to uwzględnić, zanim zacznie rozważać ustanowienie wspólnych specyfikacji. Przy opracowywaniu wspólnych specyfikacji zachęca się Komisję do współpracy z partnerami międzynarodowymi i międzynarodowymi organami normalizacyjnymi.***

(122) Bez uszczerbku dla stosowania norm zharmonizowanych i wspólnych specyfikacji należy zakładać, że dostawcy systemu AI wysokiego ryzyka, który został wytrenowany i przetestowany w oparciu o dane odzwierciedlające określone otoczenie geograficzne, behawioralne, kontekstualne lub funkcjonalne, w którym dany system AI ma być wykorzystywany, stosują odpowiedni środek przewidziany w ramach wymogu dotyczącego zarządzania danymi określonego w niniejszym rozporządzeniu. Bez uszczerbku dla wymogów dotyczących solidności i dokładności określonych w niniejszym rozporządzeniu, zgodnie z art. 54 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881[44] należy domniemywać, że systemy AI wysokiego ryzyka, które zostały certyfikowane lub w odniesieniu do których wydano deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa na podstawie tego rozporządzenia i do których to poświadczeń opublikowano odniesienia w Dzienniku Urzędowym Unii Europejskiej, spełniają wymóg cyberbezpieczeństwa określony w niniejszym rozporządzeniu w zakresie, w jakim certyfikat cyberbezpieczeństwa lub deklaracja zgodności lub ich części obejmują wymóg cyberbezpieczeństwa określony w niniejszym rozporządzeniu. Pozostaje to bez uszczerbku dla dobrowolnego charakteru tego programu certyfikacji cyberbezpieczeństwa.

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

---

44 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. 15).

(124) Aby zminimalizować obciążenie dla operatorów i uniknąć ewentualnego powielania działań, zgodność z wymogami niniejszego rozporządzenia w przypadku systemów AI wysokiego ryzyka powiązanych z produktami, które są objęte zakresem stosowania obowiązującego unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych, 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 unijnym prawodawstwie harmonizacyjnym. ▌

(125) Biorąc pod uwagę ***złożoność systemów AI wysokiego ryzyka i związane z nimi ryzyko, ważne jest opracowanie odpowiedniego systemu procedury oceny zgodności dla systemów AI wysokiego ryzyka z udziałem jednostek notyfikowanych, tzw. oceny zgodności przeprowadzanej przez stronę trzecią. Zważywszy jednak na dotychczasowe*** doświadczenie, jakie zawodowe podmioty zajmujące się certyfikacją przed wprowadzeniem do obrotu mają w dziedzinie bezpieczeństwa produktów, oraz odmienny charakter odnośnego ryzyka, zakres stosowania oceny zgodności przeprowadzanej przez stronę trzecią należy ograniczyć, przynajmniej na początkowym etapie stosowania niniejszego rozporządzenia, w przypadku systemów AI wysokiego ryzyka innych niż systemy powiązane z produktami. W związku z tym ocena zgodności takich systemów powinna być co do zasady przeprowadzana przez dostawcę na jego własną odpowiedzialność, z wyjątkiem systemów AI przeznaczonych do wykorzystania do celów ***biometrycznych***.

(126) Do celów ***oceny*** zgodności przeprowadzanej przez stronę trzecią***, jeśli jest ona wymagana,*** właściwe organy krajowe powinny ***notyfikować*** na podstawie niniejszego rozporządzenia jednostki notyfikowane, pod warunkiem że jednostki te spełniają szereg wymogów, w szczególności dotyczących niezależności, kompetencji, braku konfliktu interesów ***i odpowiednich wymogów cyberbezpieczeństwa***. ***Notyfikacja tych jednostek powinna zostać przesłana Komisji i pozostałym państwom członkowskim przez właściwe organy krajowe za pomocą systemu notyfikacji elektronicznej opracowanego i zarządzanego przez Komisję zgodnie z art. R23 załącznika I do decyzji nr 768/2008/WE.***

(127) Zgodnie ze zobowiązaniami Unii wynikającymi z Porozumienia Światowej Organizacji Handlu w sprawie barier technicznych w handlu właściwe jest ułatwienie wzajemnego uznawania wyników oceny zgodności sporządzonych przez właściwe jednostki oceniające zgodność, niezależnie od terytorium, na którym mają siedzibę, pod warunkiem że te jednostki oceniające zgodność ustanowione na mocy prawa państwa trzeciego spełniają mające zastosowanie wymogi niniejszego rozporządzenia, a Unia zawarła w tym zakresie umowę. W tym kontekście Komisja powinna aktywnie szukać rozwiązań w postaci ewentualnych służących temu celowi instrumentów międzynarodowych, a w szczególności dążyć do zawarcia umów o wzajemnym uznawaniu z państwami trzecimi.

(128) Zgodnie z powszechnie ugruntowanym pojęciem istotnej zmiany w odniesieniu do produktów regulowanych unijnym prawodawstwem harmonizacyjnym, należy ▌ – za każdym razem, gdy dokonuje się zmiany, która może wpłynąć na zgodność danego systemu ***AI wysokiego ryzyka*** z niniejszym rozporządzeniem ***(np. zmiana systemu operacyjnego lub architektury oprogramowania),*** lub gdy zmienia się przeznaczenie danego systemu **–** ***uznać ten system AI za nowy system AI, który powinien zostać poddany nowej ocenie zgodności. Za istotną zmianę nie należy jednak uznawać zmian w algorytmie oraz w skuteczności działania*** systemu AI, który po wprowadzeniu do obrotu lub oddaniu do użytku nadal się „uczy", tzn. ▌ automatycznie ***dostosowuje*** sposób wykonywania funkcji***, pod warunkiem że zmiany te*** zostały z góry zaplanowane przez dostawcę i ocenione w momencie przeprowadzania oceny zgodności ▌ .

(129) Systemy AI wysokiego ryzyka powinny posiadać oznakowanie CE świadczące o ich zgodności z niniejszym rozporządzeniem, aby umożliwić ich swobodny przepływ na rynku wewnętrznym. ***W przypadku systemów AI wysokiego ryzyka wbudowanych w produkt należy umieścić fizyczne oznakowanie CE, które może zostać uzupełnione cyfrowym oznakowaniem CE. W przypadku systemów AI wysokiego ryzyka dostarczanych wyłącznie w formie cyfrowej należy stosować cyfrowe oznakowanie CE.*** Państwa członkowskie nie powinny stwarzać nieuzasadnionych przeszkód dla wprowadzania do obrotu lub oddawania do użytku systemów AI wysokiego ryzyka zgodnych z wymogami ustanowionymi w niniejszym rozporządzeniu i posiadających oznakowanie CE.

(130) W pewnych warunkach szybka dostępność innowacyjnych technologii może być kluczowa dla zdrowia i bezpieczeństwa osób***, ochrony środowiska i zmiany klimatu*** oraz dla całego społeczeństwa. Jest zatem właściwe, aby w przypadku wystąpienia nadzwyczajnych względów dotyczących ***bezpieczeństwa publicznego lub*** ochrony zdrowia i życia osób fizycznych***, ochrony środowiska*** oraz ochrony ***kluczowych aktywów przemysłowych i infrastrukturalnych, organy nadzoru rynku*** mogły zezwolić na wprowadzenie do obrotu lub oddanie do użytku systemów AI, które nie przeszły oceny zgodności. ***W należycie uzasadnionych sytuacjach przewidzianych w niniejszym rozporządzeniu organy ścigania lub organy ochrony ludności mogą oddać do użytku określony system AI wysokiego ryzyka bez zezwolenia organu nadzoru rynku, pod warunkiem że o takie zezwolenie wystąpiono bez zbędnej zwłoki w trakcie jego wykorzystania lub po wykorzystaniu.***

(131) Aby ułatwić pracę Komisji i państw członkowskich w dziedzinie AI, jak również zwiększyć przejrzystość wobec ogółu społeczeństwa, dostawców systemów AI wysokiego ryzyka innych niż systemy powiązane z produktami objętymi zakresem odpowiedniego istniejącego unijnego prawodawstwa harmonizacyjnego***, a także dostawców, którzy uznają, że w związku z odstępstwem system AI wysokiego ryzyka objęty wykazem w załączniku do niniejszego rozporządzenia nie jest systemem wysokiego ryzyka***, należy zobowiązać, by dokonali ***swojej*** rejestracji ***oraz rejestracji informacji na temat swoich*** systemów AI w unijnej bazie danych, która zostanie utworzona i będzie zarządzana przez Komisję. ***Przed zastosowaniem takiego systemu AI wysokiego ryzyka będące publicznymi organami, agencjami lub jednostkami organizacyjnymi podmioty stosujące systemy AI wysokiego ryzyka powinny dokonać swojej rejestracji w tej bazie danych i wybrać system, z którego zamierzają skorzystać.***

Inne podmioty stosujące AI powinny być uprawnione do zrobienia tego dobrowolnie. Ta sekcja bazy danych powinna być publicznie dostępna, nieodpłatna, informacje powinny być łatwe do odnalezienia, zrozumiałe i nadające się do odczytu maszynowego. Ta baza danych powinna być również przyjazna dla użytkownika, na przykład poprzez zapewnienie funkcji wyszukiwania, w tym za pomocą słów kluczowych, co umożliwi ogółowi społeczeństwa znalezienie istotnych informacji, które przedkłada się przy rejestracji systemów AI wysokiego ryzyka, oraz informacji na temat systemów AI wysokiego ryzyka, określonych w załącznikach do niniejszego rozporządzenia, których kategoriom odpowiadają poszczególne systemy AI wysokiego ryzyka. W unijnej bazie danych powinno się też rejestrować wszelkie istotne zmiany systemów sztucznej inteligencji wysokiego ryzyka. W przypadku systemów AI wysokiego ryzyka w obszarze ścigania przestępstw, zarządzania migracją, azylem i kontrolą graniczną obowiązkowej rejestracji należy dokonać w bezpiecznej niepublicznej sekcji bazy danych. Dostęp do tej bezpiecznej, niepublicznej sekcji powinna posiadać tylko i wyłącznie Komisja i organy nadzoru rynku w odniesieniu do ich krajowej sekcji tej bazy danych. Systemy AI wysokiego ryzyka w obszarze infrastruktury krytycznej powinny być rejestrowane wyłącznie na szczeblu krajowym. Komisja powinna być administratorem ***unijnej*** bazy danych zgodnie z rozporządzeniem (UE) 2018/1725. Aby zapewnić pełną funkcjonalność tej bazy danych po jej wdrożeniu, procedura ustanawiania bazy danych powinna obejmować opracowanie przez Komisję specyfikacji funkcjonalnych oraz sprawozdanie z niezależnego audytu. ***Wykonując swoje zadania jako administrator danych unijnej bazy danych, Komisja powinna wziąć pod uwagę cyberbezpieczeństwo i ryzyko związane z zagrożeniami. Aby zmaksymalizować dostępność i wykorzystywanie bazy danych przez społeczeństwo, baza danych, w tym udostępniane za jej pośrednictwem informacje, powinna być zgodna z wymogami określonymi w dyrektywie (UE) 2019/882.***

(132) Niektóre systemy AI przeznaczone do wchodzenia w interakcję z osobami fizycznymi lub generowania 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 określonych dla systemów AI wysokiego ryzyka, ***przy zastosowaniu ukierunkowanych wyjątków, aby uwzględnić szczególne potrzeby w zakresie ścigania przestępstw***. W szczególności osoby fizyczne powinny być informowane o tym, że prowadzą interakcję z systemem AI, chyba że jest to oczywiste z ***punktu widzenia osoby fizycznej, która jest dostatecznie poinformowana, uważna i ostrożna, z uwzględnieniem*** okoliczności i kontekstu korzystania. ***Przy realizacji takiego obowiązku należy uwzględniać cechy osób należących do grup osób szczególnie wrażliwych ze względu na wiek lub niepełnosprawność – w zakresie, w jakim system AI ma również wchodzić w interakcję z tymi grupami. Ponadto osoby fizyczne powinny być powiadamiane, jeżeli są poddawane działaniu systemów, które poprzez przetwarzanie ich danych biometrycznych mogą zidentyfikować lub wywnioskować emocje lub zamiary tych*** osób ***lub przypisać je do określonych kategorii. Te określone kategorie mogą dotyczyć takich aspektów jak płeć, wiek, kolor włosów, kolor oczu, tatuaże, cechy osobowości, pochodzenie etniczne, osobiste preferencje i zainteresowania. Tego rodzaju informacje i powiadomienia należy przekazywać w formatach dostępnych dla osób z niepełnosprawnościami***.

(133) Różne systemy AI mogą generować duże ilości treści syntetycznych, które stają się coraz trudniejsze do odróżnienia od treści generowanych przez człowieka i treści autentycznych. Szeroka dostępność i coraz większe zdolności tych systemów mają znaczący wpływ na integralność ekosystemu informacyjnego i zaufanie do niego, stwarzając nowe rodzaje ryzyka polegające na podawaniu informacji wprowadzających w błąd i na manipulacji na dużą skalę, oszustwach, podszywaniu się pod inne osoby i wprowadzaniu w błąd konsumentów. W świetle tych skutków, a także szybkiego tempa technologicznego oraz zapotrzebowania na nowe metody i techniki śledzenia pochodzenia informacji należy zobowiązać dostawców tych systemów do wbudowania rozwiązań technicznych, które umożliwiają oznakowanie w formacie nadającym się do odczytu maszynowego i wykrywanie, że wyniki zostały wygenerowane lub zmanipulowane przez system AI, a nie przez człowieka. Takie techniki i metody powinny być wystarczająco niezawodne, interoperacyjne, skuteczne i solidne, o ile jest to technicznie wykonalne, z uwzględnieniem dostępnych technik lub kombinacji takich technik, takich jak znaki wodne, identyfikacja metadanych, metody kryptograficzne służące do potwierdzania pochodzenia i autentyczności treści, metody rejestracji zdarzeń, odciski palców lub inne techniki, stosownie do przypadku. Przy wdrażaniu tego obowiązku dostawcy powinni uwzględniać specyfikę i ograniczenia różnych rodzajów treści oraz istotne postępy technologiczne i rynkowe w tym obszarze, które odzwierciedla powszechnie uznany stan wiedzy technicznej. Takie techniki i metody można wdrażać na poziomie danego systemu lub na poziomie modelu, w tym modeli AI ogólnego przeznaczenia generujących treści, a tym samym ułatwiać wypełnienie tego obowiązku przez dostawcę niższego szczebla danego systemu AI. Aby zachować proporcjonalność, należy przewidzieć, że ten obowiązek oznakowania nie powinien obejmować systemów AI pełniących przede wszystkim funkcję wspomagającą w zakresie standardowej edycji lub systemów AI, które nie zmieniają w istotny sposób przekazywanych przez podmiot stosujący AI danych wejściowych ani ich semantyki.

(134) Oprócz rozwiązań technicznych wykorzystywanych przez dostawców systemu, podmioty stosujące AI, które wykorzystują system AI do generowania obrazów, treści dźwiękowych lub wideo lub manipulowania nimi, tak by łudząco przypominały istniejące osoby, miejsca lub wydarzenia i które to treści mogą niesłusznie zostać uznane przez odbiorcę za autentyczne („deepfake"), powinny również jasno i wyraźnie ujawnić – poprzez odpowiednie oznakowanie wyniku sztucznej inteligencji i ujawnienie, że źródłem jest AI – że treści te zostały sztucznie wygenerowane lub poddane manipulacji. Zgodność z obowiązkiem w zakresie przejrzystości nie oznacza, że korzystanie z systemu lub jego wyników ogranicza prawo do wolności wypowiedzi i prawo do wolności sztuki i nauki zagwarantowane w Karcie, w szczególności w przypadku, gdy treści te stanowią część dzieła lub programu mającego wyraźnie charakter twórczy, satyryczny, artystyczny lub fikcyjny, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich. W takich przypadkach określony w niniejszym rozporządzeniu obowiązek w zakresie przejrzystości dotyczący treści typu deepfake ogranicza się do ujawniania informacji o istnieniu takich generowanych lub poddanych manipulacji treści w odpowiedni sposób, który nie utrudnia wyświetlania utworu lub docenienia go, w tym jego normalnego wykorzystania i użytkowania, przy jednoczesnym zachowaniu użyteczności i jakości utworu. Ponadto należy również przewidzieć podobny obowiązek ujawniania w odniesieniu do tekstu generowanego przez AI lub tekstu poddanego manipulacji w zakresie, w jakim jest on publikowany w celu informowania opinii publicznej o sprawach leżących w interesie publicznym, chyba że treści generowane przez AI zostały poddane procesowi weryfikacji przez człowieka lub kontroli redakcyjnej, a osoba fizyczna lub prawna ponosi odpowiedzialność redakcyjną za publikację treści.

(135) Aby zapewnić spójne wdrażanie, należy upoważnić Komisję do przyjmowania aktów wykonawczych w zakresie stosowania przepisów dotyczących oznakowania i wykrywania sztucznie wygenerowanych lub poddanych manipulacji treści. Bez uszczerbku dla obowiązkowego charakteru i pełnego stosowania obowiązków w zakresie przejrzystości Komisja może również zachęcać do opracowywania kodeksów praktyk na poziomie Unii i ułatwiać ich opracowywanie, aby ułatwić skuteczne wykonywanie obowiązków dotyczących wykrywania i oznakowania sztucznie wygenerowanych lub poddanych manipulacji treści, w tym aby wspierać praktyczne rozwiązania dotyczące udostępniania, stosownie do przypadku, mechanizmów wykrywania i ułatwiania współpracy z innymi podmiotami na całej długości łańcucha wartości, które rozpowszechniają treści lub sprawdzają ich autentyczność i pochodzenie, aby umożliwić ogółowi społeczeństwa skuteczne rozróżnianie treści generowanych przez AI.

(136) Obowiązki nałożone w niniejszym rozporządzeniu na dostawców i podmioty stosujące niektóre systemy AI w celu umożliwienia wykrywania i ujawniania, że wyniki tych systemów są sztucznie generowane lub poddane manipulacji, są szczególnie istotne dla ułatwienia skutecznego wdrożenia rozporządzenia (UE) 2022/2065. Dotyczy to w szczególności obowiązków dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych w zakresie identyfikowania i ograniczania ryzyka systemowego, które może wynikać z rozpowszechniania treści sztucznie wygenerowanych lub zmanipulowanych, w szczególności ryzyka faktycznego lub przewidywalnego negatywnego wpływu na procesy demokratyczne, dyskurs obywatelski i procesy wyborcze, w tym poprzez stosowanie dezinformacji. Wymóg oznakowania treści generowanych przez systemy AI na podstawie niniejszego rozporządzenia pozostaje bez uszczerbku dla określonego w art. 16 ust. 6 rozporządzenia (UE) 2022/2065 obowiązku rozpatrywania przez dostawców usług hostingu zgłoszeń dotyczących nielegalnych treści otrzymanych na podstawie art. 16 ust. 1 tego rozporządzenia i nie powinien mieć wpływu na ocenę i decyzję w sprawie niezgodności z prawem konkretnych treści. Ocena ta powinna być dokonywana wyłącznie w odniesieniu do przepisów regulujących zgodność treści z prawem.

(137) Przestrzeganie obowiązków w zakresie przejrzystości w odniesieniu do systemów AI objętych niniejszym rozporządzeniem nie powinno być interpretowane jako wskazanie, że korzystanie z systemu lub jego wyników jest zgodne z prawem na podstawie niniejszego rozporządzenia lub innych przepisów prawa Unii i prawa państw członkowskich, i powinno pozostawać bez uszczerbku dla innych obowiązków w zakresie przejrzystości ustanowionych w prawie Unii lub prawie krajowym wobec podmiotów stosujących AI.

(138) AI jest szybko rozwijającą się grupą technologii, wymagającą nadzoru regulacyjnego oraz bezpiecznej i ***kontrolowanej*** przestrzeni do eksperymentów, przy jednoczesnym zapewnieniu odpowiedzialnej innowacji oraz uwzględnieniu odpowiednich zabezpieczeń etycznych i środków zmniejszających ryzyko. Aby zapewnić ramy prawne ***wspierające innowacje,*** nieulegające dezaktualizacji i uwzględniające przełomowe technologie, ***państwa członkowskie powinny zapewnić, by ich właściwe organy krajowe ustanowiły co najmniej jedną*** piaskownicę regulacyjną w zakresie AI ***na szczeblu krajowym***, aby ułatwić rozwijanie i testowanie innowacyjnych systemów AI pod ścisłym nadzorem regulacyjnym przed ich wprowadzeniem do obrotu lub oddaniem do użytku w inny sposób. ***Państwa członkowskie mogłyby również wypełnić ten obowiązek, uczestnicząc w już istniejących piaskownicach regulacyjnych lub ustanawiając piaskownicę wspólnie z co najmniej jednym właściwym organem innego państwa członkowskiego, o ile udział ten zapewnia uczestniczącym państwom członkowskim równoważny poziom zasięgu krajowego. Piaskownice regulacyjne mogą być tworzone w formie fizycznej, cyfrowej lub hybrydowej i mogą obejmować zarówno produkty fizyczne, jak i cyfrowe. Organy ustanawiające piaskownice regulacyjne powinny również zapewnić, aby dysponowały one odpowiednimi do ich funkcjonowania zasobami, w tym zasobami finansowymi i ludzkimi.***

(139) Piaskownice regulacyjne w zakresie ***AI*** powinny mieć na celu: wspieranie innowacji w zakresie AI poprzez ustanowienie kontrolowanego środowiska doświadczalnego i testowego w fazie rozwojowej i przed wprowadzeniem do obrotu, z myślą o zapewnieniu zgodności innowacyjnych systemów AI z niniejszym rozporządzeniem oraz z innymi odnośnymi przepisami unijnymi i krajowymi***,*** 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 ze stosowaniem AI, ***ułatwienie organom i przedsiębiorstwom uczenia się działań regulacyjnych, w tym z myślą o przyszłym dostosowaniu ram prawnych, wspieranie współpracy i wymiany najlepszych praktyk z organami zaangażowanymi w piaskownicę regulacyjną w zakresie AI*** oraz przyspieszenie dostępu do rynków, w tym poprzez usuwanie barier dla MŚP***, w tym*** przedsiębiorstw typu start-up. ***Piaskownice regulacyjne powinny być powszechnie dostępne w całej*** Unii***, a szczególną uwagę należy zwrócić na ich dostępność dla MŚP, w tym dla przedsiębiorstw typu start-up. Uczestnictwo w piaskownicy*** regulacyjnej w ***zakresie AI powinno koncentrować się na kwestiach, które powodują niepewność prawa dla dostawców i potencjalnych dostawców w zakresie innowacji czy eksperymentowania z AI w Unii, oraz powinno przyczyniać się do opartego na dowodach uczenia się działań regulacyjnych.*** Nadzór nad ***systemami AI w piaskownicy regulacyjnej w zakresie AI*** powinien ***zatem obejmować ich opracowywanie, trenowanie, testowanie i walidację przed wprowadzeniem tych systemów do obrotu lub oddaniem do użytku, a także pojęcie i występowanie istotnych zmian, które mogą wymagać nowej procedury oceny zgodności. Wykrycie jakiegokolwiek istotnego ryzyka na etapie opracowywania i testowania takich*** systemów AI ***powinno powodować konieczność właściwego ograniczenia tego ryzyka, a w przypadku jego nieusunięcia – skutkować zawieszeniem procesu opracowywania i testowania systemu.***

W stosownych przypadkach właściwe organy krajowe ustanawiające piaskownice regulacyjne w zakresie AI ***powinny współpracować z innymi odpowiednimi organami, w tym organami nadzorującymi ochronę praw podstawowych, i powinny umożliwiać zaangażowanie innych podmiotów funkcjonujących w ekosystemie AI, takich jak krajowe lub europejskie organizacje normalizacyjne, jednostki notyfikowane, ośrodki testowo-doświadczalne, laboratoria badawcze i doświadczalne, europejskie centra innowacji cyfrowych oraz organizacje zrzeszające odpowiednie zainteresowane strony i społeczeństwo obywatelskie. Aby zapewnić jednolite wdrożenie w całej Unii oraz osiągnąć korzyści skali,*** należy ***ustanowić wspólne przepisy regulujące uruchamianie piaskownic regulacyjnych oraz ramy współpracy między odpowiednimi*** organami ***uczestniczącymi w nadzorze nad piaskownicami regulacyjnymi. Piaskownice regulacyjne w zakresie AI ustanowione na mocy niniejszego rozporządzenia powinny pozostawać bez uszczerbku dla innych przepisów, które umożliwiają tworzenie innych piaskownic mających na celu zapewnienie przestrzegania innych niż niniejsze rozporządzenie unijnych przepisów. W stosownych przypadkach odpowiednie właściwe organy odpowiedzialne za te inne piaskownice regulacyjne powinny przeanalizować korzyści płynące ze stosowania tych piaskownic również do celów zapewnienia zgodności systemów AI z niniejszym rozporządzeniem. Po osiągnięciu porozumienia pomiędzy*** właściwymi organami ***krajowymi oraz uczestnikami piaskownicy regulacyjnej w zakresie AI w ramach takiej piaskownicy regulacyjnej można również prowadzić i nadzorować testy w warunkach rzeczywistych***.

(140) Niniejsze rozporządzenie powinno zapewniać dostawcom i potencjalnym dostawcom uczestniczącym w piaskownicy regulacyjnej w zakresie AI podstawę prawną do wykorzystywania danych osobowych zebranych w innych celach do opracowywania – w ramach piaskownicy regulacyjnej w zakresie AI – określonych systemów AI w interesie publicznym, tylko pod określonymi warunkami, zgodnie z art. 6 ust. 4 i art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679 i art. 5, 6 i 10 rozporządzenia (UE) 2018/1725 i nie naruszając przepisów art. 4 ust. 2 i art. 10 dyrektywy (UE) 2016/680. Nadal mają zastosowanie wszystkie pozostałe obowiązki administratorów danych i prawa osób, których dane dotyczą, wynikające z rozporządzeń (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywy (UE) 2016/680. W szczególności niniejsze rozporządzenie nie powinno stanowić podstawy prawnej w rozumieniu art. 22 ust. 2 lit. b) rozporządzenia (UE) 2016/679 i art. 24 ust. 2 lit. b) rozporządzenia (UE) 2018/1725. Dostawcy i potencjalni dostawcy w 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 właściwego ograniczenia wszelkiego zidentyfikowanego istotnego ryzyka dla bezpieczeństwa, zdrowia i praw podstawowych, jakie może powstać w trakcie opracowywania produktów oraz prowadzenia działań testowych i doświadczalnych w ramach piaskownicy regulacyjnej.

(141) Aby przyspieszyć proces opracowywania i wprowadzania do obrotu systemów AI wysokiego ryzyka wymienionych w załączniku do niniejszego rozporządzenia, ważne jest, aby dostawcy lub potencjalni dostawcy takich systemów mogli korzystać ze specjalnego mechanizmu testowania tych systemów w warunkach rzeczywistych, bez udziału w piaskownicy regulacyjnej w zakresie AI. Jednak w takich przypadkach oraz uwzględniając potencjalne konsekwencje takiego testowania dla obywateli, należy zapewnić, by niniejsze rozporządzenie wprowadzało odpowiednie i wystarczające zabezpieczenia i warunki dotyczące dostawców lub potencjalnych dostawców. Takie gwarancje powinny obejmować między innymi wymóg udzielenia świadomej zgody przez osoby fizyczne, które mają brać udział w testach w warunkach rzeczywistych, z wyjątkiem organów ścigania, gdy konieczność wystąpienia o świadomą zgodę uniemożliwiłaby testowanie systemu AI. Zgoda podmiotów testów na udział w takich testach na podstawie niniejszego rozporządzenia ma odrębny charakter i pozostaje bez uszczerbku dla zgody osób, których dane dotyczą, na przetwarzanie ich danych osobowych na podstawie odpowiedniego prawa ochrony danych.

Ważne jest również, aby zminimalizować ryzyko i umożliwić nadzór ze strony właściwych organów, a zatem zobowiązać potencjalnych dostawców do: przedstawienia właściwemu organowi nadzoru rynku planu testów w warunkach rzeczywistych, rejestrowania testów w specjalnych sekcjach unijnej bazy danych (z pewnymi ograniczonymi wyjątkami), ustalenia ograniczeń co do okresu, w jakim można przeprowadzać testy, oraz wymagania dodatkowych zabezpieczeń w odniesieniu do osób szczególnie wrażliwych, w tym grup osób szczególnie wrażliwych, a także pisemnej umowy określającej role i obowiązki potencjalnych dostawców i podmiotów stosujących AI oraz skutecznego nadzoru ze strony kompetentnego personelu zaangażowanego w testy w warunkach rzeczywistych. Ponadto należy przewidzieć dodatkowe zabezpieczenia w celu zapewnienia, aby predykcje, zalecenia lub decyzje wygenerowane przez system AI mogły zostać skutecznie odwrócone i nie były brane pod uwagę oraz aby dane osobowe były chronione i usuwane, gdy uczestnicy wycofają swoją zgodę na udział w testach, bez uszczerbku dla ich praw jako osób, których dane dotyczą, wynikających z unijnego prawa o ochronie danych. W odniesieniu do przekazywania danych należy także przewidzieć, by dane zebrane i przetwarzane do celów testów w warunkach rzeczywistych przekazywano do państw trzecich wyłącznie pod warunkiem wdrożenia odpowiednich zabezpieczeń mających zastosowanie na podstawie prawa Unii, w szczególności zgodnie z podstawami przekazywania danych osobowych na mocy prawa Unii dotyczącego ochrony danych osobowych, a w odniesieniu do danych nieosobowych wprowadzono odpowiednie zabezpieczenia zgodnie z prawem Unii, takim jak rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868[45] ***i*** (UE) 2023/2854[46]**.**

---

45 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. L 152 z 3.6.2022, s. 1).

46 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.U. L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) W celu zapewnienia, aby AI przynosiła korzyści dla społeczeństwa i środowiska, zachęca się państwa członkowskie do wspierania i promowania badań i rozwoju w dziedzinie rozwiązań w zakresie AI wspierających takie korzyści społeczne i środowiskowe, np. opartych na AI rozwiązań, które zwiększają dostępność dla osób z niepełnosprawnościami, przeciwdziałają nierównościom społeczno-gospodarczym lub służą osiągnięciu celów środowiskowych, przez przydzielanie wystarczających zasobów, w tym finansowania publicznego i unijnego, oraz, w stosownych przypadkach i pod warunkiem spełnienia kryteriów kwalifikowalności i wyboru, przez priorytetowe traktowanie projektów, które służą realizacji takich celów. Projekty takie powinny opierać się na zasadzie współpracy międzydyscyplinarnej między twórcami AI, ekspertami ds. nierówności i niedyskryminacji, dostępności, praw konsumentów, praw środowiskowych i cyfrowych oraz przedstawicielami środowiska akademickiego.

(143) W celu promowania i ochrony innowacji ważne jest szczególne uwzględnienie interesów ***MŚP, w tym przedsiębiorstw typu start-up, które są dostawcami*** systemów AI ***lub podmiotami stosującymi systemy AI***. W tym celu państwa członkowskie powinny opracować inicjatywy skierowane do tych operatorów, w tym inicjatywy służące podnoszeniu świadomości i przekazywaniu informacji. ***Państwa członkowskie zapewniają MŚP, w tym przedsiębiorstwom typu start-up, mającym siedzibę statutową lub oddział w Unii, priorytetowy dostęp do piaskownic regulacyjnych w zakresie AI, pod warunkiem że przedsiębiorstwa te spełniają warunki kwalifikowalności i kryteria wyboru – w sposób, który nie uniemożliwia innym dostawcom i potencjalnym dostawcom dostępu do piaskownic, pod warunkiem spełnienia przez nich tych samych warunków i kryteriów. Państwa członkowskie korzystają z istniejących kanałów komunikacji, a w stosownych przypadkach tworzą nowy specjalny kanał komunikacji z MŚP, przedsiębiorstwami typu start-up, podmiotami stosującymi AI i innymi innowacyjnymi podmiotami, a w stosownych przypadkach, z lokalnymi organami publicznymi, aby wspierać MŚP w rozwoju poprzez udzielanie im wskazówek i odpowiadanie na ich pytania dotyczące wdrażania niniejszego rozporządzenia. W stosownych przypadkach kanały te współpracują ze sobą, by uzyskać synergię i czuwać nad jednolitością wskazówek dla MŚP, w tym przedsiębiorstw typu start-up, i podmiotów stosujących AI. Dodatkowo państwa członkowskie powinny ułatwiać udział MŚP i innych odpowiednich stron w procesie opracowywania norm.*** Ponadto przy ustalaniu przez jednostki notyfikowane wysokości opłat z tytułu oceny zgodności ***należy*** uwzględnić szczególne interesy i potrzeby ***MŚP, w tym przedsiębiorstw typu start-up,*** będących dostawcami. ***Komisja powinna regularnie oceniać koszty certyfikacji i przestrzegania przepisów ponoszone przez MŚP, w tym przedsiębiorstwa typu start-up, w drodze przejrzystych konsultacji z podmiotami stosującymi AI, oraz współpracować z państwami członkowskimi na rzecz obniżenia tych kosztów.***

Przykładowo koszty tłumaczeń związane z prowadzeniem obowiązkowej dokumentacji i komunikacji z organami mogą stanowić istotny koszt dla dostawców i innych operatorów, w szczególności tych działających na mniejszą skalę. Państwa członkowskie powinny w miarę możliwości zapewnić, aby jednym z języków wskazanych i akceptowanych przez nie do celów dokumentacji sporządzanej przez odpowiednich dostawców oraz komunikacji z operatorami był język powszechnie rozumiany przez możliwie największą liczbę ***podmiotów stosujących AI*** w wymiarze transgranicznym. ***Aby zaspokoić szczególne potrzeby MŚP, w tym przedsiębiorstw typu start-up, Komisja powinna na wniosek Rady ds. AI zapewnić ujednolicone wzory dokumentacji dla obszarów objętych niniejszym rozporządzeniem. Ponadto Komisja powinna w uzupełnieniu wysiłków państw członkowskich dostarczyć jednolitą platformę informacyjną zawierającą łatwe w użyciu informacje dotyczące niniejszego rozporządzenia dla wszystkich dostawców i podmiotów stosujących AI, organizować odpowiednie kampanie informacyjne w celu podnoszenia świadomości na temat obowiązków wynikających z niniejszego rozporządzenia oraz oceniać i promować zbieżność najlepszych praktyk w procedurach udzielania zamówień publicznych w odniesieniu do systemów AI. Przedsiębiorstwa, które niedawno przekształciły się z małych w średnie, w rozumieniu załącznika do zalecenia Komisji 2003/361/WE[47], powinny mieć dostęp do tych środków wsparcia, ponieważ w niektórych przypadkach te nowe średnie przedsiębiorstwa mogą nie posiadać zasobów prawnych i szkoleniowych niezbędnych do zapewnienia właściwego zrozumienia i przestrzegania niniejszego rozporządzenia***.

---

47 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).

(144) W celu promowania i ochrony innowacji do realizacji celów niniejszego rozporządzenia powinny przyczyniać się, w stosownych przypadkach, platforma „Sztuczna inteligencja na żądanie", wszystkie odpowiednie finansowane przez Unię programy i projekty, takie jak program „Cyfrowa Europa", „Horyzont Europa", wdrażane przez Komisję i państwa członkowskie na szczeblu unijnym lub krajowym.

(145) ***W szczególności,*** aby zminimalizować zagrożenia dla wdrożenia wynikające z braku wiedzy o rynku i jego znajomości, a także aby ułatwić dostawcom***, zwłaszcza MŚP, w tym przedsiębiorstwom typu start-up,*** i jednostkom notyfikowanym wykonywanie obowiązków ustanowionych w niniejszym rozporządzeniu, platforma „Sztuczna inteligencja na żądanie", europejskie centra innowacji cyfrowych oraz ośrodki testowo-doświadczalne ustanowione przez Komisję i państwa członkowskie na szczeblu unijnym lub krajowym powinny przyczyniać się do wdrożenia niniejszego rozporządzenia. W ramach swoich zadań i obszarów kompetencji platforma „Sztuczna inteligencja na żądanie", europejskie centra innowacji cyfrowych oraz ośrodki testowo-doświadczalne są w stanie zapewnić w szczególności wsparcie techniczne i naukowe dostawcom i jednostkom notyfikowanym.

(146) Ponadto, biorąc pod uwagę bardzo mały rozmiar niektórych operatorów i aby zapewnić proporcjonalność w odniesieniu do kosztów innowacji, należy zezwolić mikroprzedsiębiorstwom na uproszczone wypełnienie jednego z najbardziej kosztownych obowiązków, a mianowicie ustanowienia systemu zarządzania jakością, co zmniejszy obciążenie administracyjne i koszty ponoszone przez te przedsiębiorstwa bez wpływu na poziom ochrony oraz konieczność zapewnienia zgodności z wymogami dotyczącymi systemów AI wysokiego ryzyka. Komisja powinna opracować wytyczne w celu określenia, które z elementów systemu zarządzania jakością mają być realizowane w ten uproszczony sposób przez mikroprzedsiębiorstwa.

(147) 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 rozporządzeń (UE) 2017/745 i (UE) 2017/746.

(148) ***W niniejszym rozporządzeniu należy ustanowić ramy zarządzania, które umożliwiają koordynację i wspieranie stosowania niniejszego rozporządzenia na szczeblu krajowym, a także budowanie zdolności na szczeblu unijnym i zaangażowanie zainteresowanych stron w dziedzinę AI. Skuteczne wdrożenie i egzekwowanie niniejszego rozporządzenia wymaga ram zarządzania, które umożliwią koordynację i gromadzenie centralnej wiedzy fachowej na szczeblu Unii. Misją Urzędu ds. AI, który został ustanowiony decyzją Komisji[48], jest rozwijanie unijnej wiedzy fachowej i unijnych zdolności w dziedzinie AI oraz przyczynianie się do wdrażania prawa Unii dotyczącego AI. Państwa członkowskie powinny ułatwiać Urzędowi ds. AI wykonywanie zadań z myślą o wspieraniu rozwoju unijnej wiedzy fachowej i unijnych zdolności oraz wzmacnianiu funkcjonowania jednolitego rynku cyfrowego. Ponadto należy ustanowić Radę ds. AI składającą się z przedstawicieli państw członkowskich, panel naukowy w celu zaangażowania środowiska naukowego oraz forum doradcze w celu wnoszenia przez zainteresowane strony wkładu we wdrażanie niniejszego rozporządzenia na szczeblu unijnym i krajowym. Rozwój unijnej wiedzy fachowej i unijnych zdolności powinien również obejmować wykorzystanie istniejących zasobów i wiedzy fachowej, w szczególności poprzez synergię ze strukturami zbudowanymi w kontekście egzekwowania innych przepisów na szczeblu Unii oraz synergię z powiązanymi inicjatywami na szczeblu Unii, takimi jak Wspólne Przedsięwzięcie EuroHPC i ośrodki testowo-doświadczalne w dziedzinie AI w ramach programu „Cyfrowa Europa”.***

---

48 Decyzja Komisji z dnia 24 stycznia 2024 r. ustanawiająca Europejski Urząd ds. Sztucznej Inteligencji C(2024) 390.

(149) Aby ułatwić sprawne, skuteczne i zharmonizowane wdrażanie niniejszego rozporządzenia, należy ustanowić Radę ds. AI. Rada ds. AI powinna ***odzwierciedlać różne interesy ekosystemu AI i składać się z przedstawicieli państw członkowskich. Rada ds. AI powinna*** odpowiadać za szereg zadań doradczych, w tym wydawanie opinii lub zaleceń oraz udzielanie porad lub ***udział w tworzeniu*** wskazówek w dziedzinach związanych z wdrażaniem niniejszego rozporządzenia, także w ***kwestiach egzekwowania***, specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w niniejszym rozporządzeniu, jak również za udzielanie porad ***Komisji oraz państwom członkowskim i ich właściwym organom krajowym*** w konkretnych kwestiach związanych z AI. ***Aby zapewnić państwom członkowskim pewną elastyczność w wyznaczaniu swoich przedstawicieli do Rady ds. AI, takimi przedstawicielami mogą być wszelkie osoby należące do podmiotów publicznych, które powinny mieć odpowiednie kompetencje i uprawnienia, aby ułatwiać koordynację na szczeblu krajowym i przyczyniać się do realizacji zadań Rady ds. AI. Rada ds. AI powinna ustanowić dwie stałe podgrupy służące jako platforma współpracy i wymiany między organami nadzoru rynku i organami notyfikującymi w zakresie kwestii dotyczących odpowiednio nadzoru rynku i jednostek notyfikowanych. Stała podgrupa ds. nadzoru rynku powinna do celów niniejszego rozporządzenia pełnić rolę grupy ds. współpracy administracyjnej (ADCO) w rozumieniu art. 30 rozporządzenia (UE) 2019/1020. Zgodnie z art. 33 wspomnianego powyżej rozporządzenia Komisja powinna wspierać działania stałej podgrupy ds. nadzoru rynku poprzez przeprowadzanie ocen lub badań rynku, w szczególności w celu zidentyfikowania aspektów niniejszego rozporządzenia wymagających szczególnej i pilnej koordynacji między organami nadzoru rynku. W stosownych przypadkach Rada ds. AI może również tworzyć inne stałe lub tymczasowe podgrupy na potrzeby zbadania konkretnych kwestii. Rada ds. AI powinna również w stosownych przypadkach współpracować z odpowiednimi unijnymi organami, grupami ekspertów i sieciami działającymi w kontekście odpowiedniego prawa Unii, w tym w szczególności z tymi, które działają na podstawie odpowiednich unijnych przepisów dotyczących danych oraz produktów i usług cyfrowych.***

(150) Aby zapewnić zaangażowanie zainteresowanych stron we wdrażanie i stosowanie niniejszego rozporządzenia, należy ustanowić forum doradcze, które będzie doradzać Radzie ds. AI i Komisji oraz zapewniać im fachową wiedzę techniczną. Aby zapewnić zróżnicowaną i zrównoważoną reprezentację zainteresowanych stron z uwzględnieniem interesów handlowych i niehandlowych oraz w ramach kategorii interesów handlowych – w odniesieniu do MŚP i innych przedsiębiorstw, forum doradcze powinno obejmować m.in. przemysł, przedsiębiorstwa typu start-up, MŚP, środowisko akademickie, społeczeństwo obywatelskie, w tym partnerów społecznych, a także Agencję Praw Podstawowych, Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Europejski Komitet Normalizacyjny (CEN), Europejski Komitet Normalizacyjny Elektrotechniki (CENELEC) i Europejski Instytut Norm Telekomunikacyjnych (ETSI).

(151) Aby wspierać wdrażanie i egzekwowanie niniejszego rozporządzenia, w szczególności działania monitorujące prowadzone przez Urząd ds. AI w odniesieniu do modeli AI ogólnego przeznaczenia, należy ustanowić panel naukowy złożony z niezależnych ekspertów. Niezależni eksperci tworzący panel naukowy powinni być wybierani na podstawie aktualnej wiedzy naukowej lub technicznej w dziedzinie AI i powinni wykonywać swoje zadania w sposób bezstronny i obiektywny oraz zapewniać poufność informacji i danych uzyskanych w trakcie wykonywania swoich zadań i działań. Aby umożliwić wzmocnienie krajowych zdolności niezbędnych do skutecznego egzekwowania niniejszego rozporządzenia, państwa członkowskie powinny mieć możliwość zwrócenia się o wsparcie do zespołu ekspertów wchodzących w skład panelu naukowego w odniesieniu do ich działań w zakresie egzekwowania przepisów.

(152) Aby wspierać odpowiednie egzekwowanie przepisów w odniesieniu do systemów AI i wzmocnić zdolności państw członkowskich, należy ustanowić unijne struktury wsparcia w zakresie testowania AI i udostępnić je państwom członkowskim.

(153) Państwa członkowskie odgrywają kluczową rolę w stosowaniu i egzekwowaniu niniejszego rozporządzenia. W tym zakresie każde państwo członkowskie powinno wyznaczyć ***co najmniej jedną jednostkę notyfikującą i co najmniej jeden organ nadzoru ryku jako*** właściwe organy krajowe do celów sprawowania nadzoru nad stosowaniem i wdrażaniem niniejszego rozporządzenia. ***Państwa członkowskie mogą podjąć decyzję o wyznaczeniu dowolnego rodzaju podmiotu publicznego do wykonywania zadań właściwych organów krajowych w rozumieniu niniejszego rozporządzenia, zgodnie z ich określonymi krajowymi cechami organizacyjnymi i potrzebami.*** Aby zwiększyć efektywność organizacyjną po stronie państw członkowskich oraz ustanowić ***pojedynczy*** punkt kontaktowy dla ogółu społeczeństwa oraz innych partnerów na szczeblu państw członkowskich i na szczeblu unijnym, ▌ każde państwo członkowskie ***powinno wyznaczyć organ nadzoru rynku, który pełniłby funkcję pojedynczego punktu kontaktowego***.

(154) Właściwe organy krajowe powinny wykonywać swoje uprawnienia w sposób niezależny, bezstronny i wolny od uprzedzeń, aby zagwarantować przestrzeganie zasady obiektywności swoich działań i zadań oraz zapewnić stosowanie i wdrażanie niniejszego rozporządzenia. Członkowie tych organów powinni powstrzymać się od wszelkich działań niezgodnych z ich obowiązkami i powinni podlegać zasadom poufności na mocy niniejszego rozporządzenia.

(155) W celu zapewnienia, aby dostawcy systemów AI wysokiego ryzyka mogli wykorzystywać doświadczenia związane ze stosowaniem systemów AI 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. ***W stosownych przypadkach monitorowanie po wprowadzeniu do obrotu powinno obejmować analizę interakcji z innymi systemami AI, w tym z innymi urządzeniami i oprogramowaniem. Monitorowanie po wprowadzeniu do obrotu nie obejmuje wrażliwych danych operacyjnych podmiotów stosujących AI, które są organami ścigania.*** System ten ma również zasadnicze znaczenie dla zapewnienia skuteczniejszego i terminowego przeciwdziałania możliwym zagrożeniom związanym z systemami AI, które nadal „uczą się" po wprowadzeniu do obrotu lub oddaniu do użytku. W tym kontekście dostawcy powinni być również zobowiązani do posiadania systemu zgłaszania odpowiednim organom wszelkich poważnych incydentów ***zaistniałych w związku ze stosowaniem ich systemów AI, tj. incydentu lub nieprawidłowego działania prowadzącego do śmierci lub poważnej szkody dla zdrowia, poważnych i nieodwracalnych zakłóceń w zarządzaniu infrastrukturą krytyczną i jej obsłudze, naruszeń obowiązków wynikających z*** prawa Unii ***mających na celu ochronę*** praw podstawowych ***lub poważnych szkód majątkowych lub środowiskowych***.

(156) Aby zapewnić odpowiednie i skuteczne egzekwowanie wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, które należy do unijnego prawodawstwa harmonizacyjnego, pełne zastosowanie powinien mieć system nadzoru rynku i zgodności produktów ustanowiony rozporządzeniem (UE) 2019/1020. ***Organy nadzoru rynku wyznaczone zgodnie z niniejszym rozporządzeniem powinny mieć wszystkie uprawnienia w zakresie egzekwowania przepisów wynikające z niniejszego rozporządzenia oraz z rozporządzenia (UE) 2019/1020 i powinny wykonywać*** swoje ***uprawnienia i obowiązki w sposób niezależny, bezstronny i wolny od uprzedzeń. Chociaż większość systemów AI nie podlega szczególnym wymogom i obowiązkom na podstawie niniejszego rozporządzenia,*** organy ***nadzoru rynku mogą przyjmować środki w odniesieniu do wszystkich systemów AI, jeżeli zgodnie z niniejszym rozporządzeniem stwarzają one ryzyko. Z uwagi na szczególny charakter instytucji, organów i*** jednostek organizacyjnych ***Unii objętych zakresem stosowania niniejszego rozporządzenia, należy wyznaczyć Europejskiego Inspektora Ochrony Danych jako właściwy dla nich organ nadzoru rynku. Powinno to pozostawać bez uszczerbku dla wyznaczenia właściwych organów krajowych przez państwa członkowskie. Działania w zakresie nadzoru rynku nie*** powinny ***wpływać na zdolność nadzorowanych podmiotów do niezależnego wypełniania ich zadań, w przypadku gdy taka niezależność jest wymagana prawem Unii***.

(157) ***Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji, zadań, uprawnień i niezależności odpowiednich krajowych organów lub podmiotów publicznych, które nadzorują stosowanie prawa Unii w zakresie ochrony praw podstawowych, w tym organów ds. równości i organów ochrony danych. W przypadku gdy jest to niezbędne do wykonywania ich mandatu, te krajowe organy lub podmioty publiczne powinny również mieć dostęp do wszelkiej dokumentacji sporządzonej na podstawie niniejszego rozporządzenia. Należy ustanowić specjalną procedurę w sprawie środków ochronnych, aby zapewnić odpowiednie i terminowe egzekwowanie przepisów niniejszego rozporządzenia w odniesieniu do systemów AI stwarzających ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych. Procedurę dotyczącą takich systemów AI stwarzających ryzyko należy stosować w odniesieniu do systemów AI wysokiego ryzyka stwarzających ryzyko, zakazanych systemów, które zostały wprowadzone do obrotu, oddane do użytku lub są wykorzystywane z naruszeniem zasad dotyczących zakazanych praktyk ustanowionych w niniejszym rozporządzeniu, oraz systemów AI, które zostały udostępnione z naruszeniem ustanowionych w niniejszym rozporządzeniu wymogów przejrzystości i które stwarzają ryzyko.***

(158) Przepisy Unii dotyczące usług finansowych obejmują zasady i wymogi dotyczące zarządzania wewnętrznego i zarządzania ryzykiem, które mają zastosowanie do regulowanych instytucji finansowych podczas świadczenia tych usług, w tym wówczas, gdy korzystają one z systemów AI. Aby zapewnić spójne stosowanie i egzekwowanie obowiązków ustanowionych w niniejszym rozporządzeniu oraz odpowiednich zasad i wymogów ustanowionych w unijnych aktach prawnych dotyczących usług finansowych, ***właściwe organy*** do celów nadzoru nad przepisami dotyczącymi usług finansowych i ich egzekwowania, w szczególności ***właściwe organy zdefiniowane w rozporządzeniu Parlamentu*** Europejskiego ***i Rady (UE) nr 575/2013***[49] ***oraz dyrektywach Parlamentu Europejskiego i Rady 2008/48/WE***[50]***, 2009/138/WE***[51]***, 2013/36/UE***[52]***, 2014/17/UE***[53] ***i (UE) 2016/97***[54] należy wyznaczyć ***w ramach ich odpowiednich kompetencji*** jako właściwe organy do celów nadzoru nad wdrażaniem niniejszego rozporządzenia, w tym do celów działań związanych z nadzorem rynku, w odniesieniu do systemów AI dostarczanych lub wykorzystywanych przez objęte regulacją i nadzorem instytucje finansowe***, chyba że państwa członkowskie zdecydują się wyznaczyć inny organ do wypełniania tych zadań związanych z nadzorem rynku.***

---

49 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1).

50 Dyrektywa Parlamentu Europejskiego i Rady nr 2008/48/WE z dnia 23 kwietnia 2008 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrektywę Rady 87/102/EWG (Dz.U. L 133 z 22.5.2008, s. 66).

51 Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 335 z 17.12.2009, s. 1).

52 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).

53 Dyrektywa Parlamentu Europejskiego i Rady 2014/17/UE z dnia 4 lutego 2014 r. w sprawie konsumenckich umów o kredyt związanych z nieruchomościami mieszkalnymi i zmieniająca dyrektywy 2008/48/WE i 2013/36/UE oraz rozporządzenie (UE) nr 1093/2010 (Dz.U. L 60 z 28.2.2014, s. 34).

54 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń (Dz.U. L 26 z 2.2.2016, s. 19).

Te właściwe organy powinny mieć wszystkie uprawnienia wynikające z niniejszego rozporządzenia i rozporządzenia (UE) 2019/1020 w celu egzekwowania wymogów i obowiązków wynikających z niniejszego rozporządzenia, w tym uprawnienia do prowadzenia działań ex post w zakresie nadzoru rynku, które można w stosownych przypadkach włączyć do ich istniejących mechanizmów i procedur nadzorczych na podstawie odpowiednich unijnych przepisów dotyczących usług finansowych. Należy przewidzieć, że –występując w charakterze organów nadzoru rynku na podstawie niniejszego rozporządzenia – odpowiedzialne za nadzór instytucji kredytowych uregulowanych na podstawie dyrektywy 2013/36/UE krajowe organy uczestniczące w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem Rady (UE) nr 1024/2013[55] powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zidentyfikowane w trakcie prowadzonych przez siebie działań z zakresu nadzoru rynku, które potencjalnie mogą mieć znaczenie dla Europejskiego Banku Centralnego z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego.

---

55 Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz.U. L 287 z 29.10.2013, s. 63).

Aby dodatkowo zwiększyć spójność między niniejszym rozporządzeniem a przepisami mającymi zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy 2013/36/UE, 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 prowadzonego przez dostawców oraz obowiązku monitorowania nałożonego na ***podmioty stosujące*** systemy AI wysokiego ryzyka w zakresie, w jakim mają one zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy 2013/36/UE. ***Ten sam system powinien mieć zastosowanie do zakładów ubezpieczeń i zakładów reasekuracji oraz ubezpieczeniowych spółek holdingowych na podstawie dyrektywy 2009/138/WE oraz pośredników ubezpieczeniowych na mocy dyrektywy (UE) 2016/97, a także do innych rodzajów instytucji finansowych objętych wymogami dotyczącymi ich systemu zarządzania wewnętrznego, uzgodnień lub procedur ustanowionych zgodnie z odpowiednimi unijnymi przepisami dotyczącymi usług finansowych, w celu zapewnienia spójności i równego traktowania w sektorze finansowym.***

(159) Każdy organ nadzoru rynku ds. systemów AI wysokiego ryzyka w obszarze danych biometrycznych, wymienionych w załączniku do niniejszego rozporządzenia, o ile systemy te są wykorzystywane do celów ścigania przestępstw, zarządzania migracją, azylem i kontrolą graniczną lub do celów sprawowania wymiaru sprawiedliwości i procesów demokratycznych, powinien dysponować skutecznymi uprawnieniami do prowadzenia postępowań i uprawnieniami naprawczymi, w tym co najmniej uprawnieniami do uzyskania dostępu do wszystkich przetwarzanych danych osobowych oraz do wszelkich informacji niezbędnych do wykonywania jego zadań. Organy nadzoru rynku powinny mieć możliwość wykonywania swoich uprawnień, działając w sposób całkowicie niezależny. Wszelkie ograniczenia dostępu tych organów do wrażliwych danych operacyjnych na mocy niniejszego rozporządzenia powinny pozostawać bez uszczerbku dla uprawnień przyznanych im na mocy dyrektywy (UE) 2016/680. Żadne wyłączenie dotyczące ujawniania danych krajowym organom ochrony danych na mocy niniejszego rozporządzenia nie powinno mieć wpływu na obecne lub przyszłe uprawnienia tych organów wykraczające poza zakres niniejszego rozporządzenia.

(160) Organy nadzoru rynku państw członkowskich i Komisja powinny mieć możliwość proponowania wspólnych działań, w tym wspólnych postępowań, które mają być prowadzone przez organy nadzoru rynku lub organy nadzoru rynku wspólnie z Komisją, których celem jest promowanie zgodności, wykrywanie niezgodności, podnoszenie świadomości i zapewnianie wytycznych dotyczących niniejszego rozporządzenia w odniesieniu do konkretnych kategorii systemów AI wysokiego ryzyka, w przypadku których stwierdzono, że stwarzają poważne ryzyko w co najmniej dwóch państwach członkowskich. Wspólne działania na rzecz promowania zgodności należy prowadzić zgodnie z art. 9 rozporządzenia (UE) 2019/1020. Urząd ds. AI powinien zapewniać wsparcie w zakresie koordynacji wspólnych postępowań.

(161) Konieczne jest wyjaśnienie obowiązków i kompetencji na szczeblu unijnym i krajowym w odniesieniu do systemów AI, które opierają się na modelach AI ogólnego przeznaczenia. Aby uniknąć nakładania się kompetencji, w przypadku gdy system AI opiera się na modelu AI ogólnego przeznaczenia, a model i system są dostarczone przez tego samego dostawcę, nadzór powinien odbywać się na poziomie Unii za pośrednictwem Urzędu ds. AI, który w tym celu powinien posiadać uprawnienia organu nadzoru rynku w rozumieniu rozporządzenia (UE) 2019/1020. We wszystkich innych przypadkach krajowe organy nadzoru rynku pozostają odpowiedzialne za nadzór nad systemami AI. Natomiast w przypadku systemów AI ogólnego przeznaczenia, które mogą być wykorzystywane bezpośrednio przez podmioty stosujące AI do co najmniej jednego celu sklasyfikowanego jako cel wysokiego ryzyka, organy nadzoru rynku powinny współpracować z Urzędem ds. AI przy prowadzeniu ocen zgodności i by odpowiednio informować Radę ds. AI i inne organy nadzoru rynku. Ponadto organy nadzoru rynku powinny mieć możliwość zwrócenia się o pomoc do Urzędu ds. AI, jeżeli organ nadzoru rynku nie jest w stanie zakończyć postępowania w sprawie systemu AI wysokiego ryzyka ze względu na niemożność dostępu do niektórych informacji związanych z modelem AI ogólnego przeznaczenia, na którym opiera się ten system AI wysokiego ryzyka. W takich przypadkach powinna mieć zastosowanie odpowiednio procedura dotycząca wzajemnej pomocy transgranicznej określona w rozdziale VI rozporządzenia (UE) 2019/1020.

(162) Aby jak najlepiej wykorzystać scentralizowaną unijną wiedzę fachową i synergie na poziomie Unii, uprawnienia w zakresie nadzoru i egzekwowania obowiązków spoczywających na dostawcach modeli AI ogólnego przeznaczenia powinny należeć do kompetencji Komisji. Komisja powinna powierzyć realizację tych zadań Urzędowi ds. AI, bez uszczerbku dla uprawnień organizacyjnych Komisji i podziału kompetencji między państwami członkowskimi a Unią na podstawie Traktatów. Urząd ds. AI powinien mieć możliwość prowadzenia wszelkich niezbędnych działań w celu monitorowania skutecznego wdrażania niniejszego rozporządzenia w odniesieniu do modeli AI ogólnego przeznaczenia. Powinien mieć możliwość prowadzenia postępowań w sprawie ewentualnych naruszeń przepisów dotyczących dostawców modeli AI ogólnego przeznaczenia zarówno z własnej inicjatywy, na podstawie wyników swoich działań monitorujących, jak i na wniosek organów nadzoru rynku zgodnie z warunkami określonymi w niniejszym rozporządzeniu. W ramach wsparcia skutecznego monitorowania Urząd ds. AI powinien przewidywać możliwość składania przez dostawców niższego szczebla na dostawców systemów AI ogólnego przeznaczenia skarg dotyczących ewentualnych naruszeń przepisów.

(163) W celu uzupełnienia systemów zarządzania modelami AI ogólnego przeznaczenia panel naukowy powinien wspierać działania monitorujące Urzędu ds. AI i może, w niektórych przypadkach, przekazywać Urzędowi ds. AI ostrzeżenia kwalifikowane, które uruchamiają działania następcze, takie jak postępowania. Powinno to mieć miejsce w przypadku, gdy panel naukowy ma powody, by podejrzewać, że model AI ogólnego przeznaczenia stwarza konkretne i możliwe do zidentyfikowania ryzyko na poziomie Unii. Ponadto powinno to mieć miejsce w przypadku, gdy panel naukowy ma powody, by podejrzewać, że model AI ogólnego przeznaczenia spełnia kryteria, które prowadziłyby do zaklasyfikowania go jako modelu AI ogólnego przeznaczenia z ryzykiem systemowym. Aby panel naukowy mógł dysponować informacjami niezbędnymi do wykonywania tych zadań, powinien istnieć mechanizm, w ramach którego panel naukowy może zwrócić się do Komisji o zażądanie od dostawcy dokumentacji lub informacji.

(164) Urząd ds. AI powinien mieć możliwość podejmowania niezbędnych działań w celu monitorowania skutecznego wdrażania i przestrzegania obowiązków przez dostawców modeli AI ogólnego przeznaczenia określonych w niniejszym rozporządzeniu. Urząd ds. AI powinien mieć możliwość prowadzenia postępowań w sprawie ewentualnych naruszeń zgodnie z uprawnieniami przewidzianymi w niniejszym rozporządzeniu, w tym poprzez zwracanie się o dokumentację i informacje, przeprowadzanie ocen, a także zwracanie się do dostawców modeli AI ogólnego przeznaczenia o zastosowanie określonych środków. Aby wykorzystać niezależną wiedzę fachową w ramach prowadzenia ocen, Urząd ds. AI powinien mieć możliwość angażowania niezależnych ekspertów do prowadzenia ocen w jego imieniu. Przestrzeganie obowiązków powinno być możliwe do wyegzekwowania m.in. poprzez wezwanie do podjęcia odpowiednich środków, w tym środków ograniczających ryzyko w przypadku zidentyfikowanego ryzyka systemowego, a także poprzez ograniczenie udostępniania modelu na rynku, wycofanie modelu z rynku lub od użytkowników. Jako zabezpieczenie, jeśli zaistnieją potrzeby wykraczające poza prawa proceduralne przewidziane w niniejszym rozporządzeniu, dostawcy modeli AI ogólnego przeznaczenia powinni dysponować prawami proceduralnymi przewidzianymi w art. 18 rozporządzenia (UE) 2019/1020, które powinny mieć zastosowanie odpowiednio, bez uszczerbku dla bardziej szczegółowych praw proceduralnych przewidzianych w niniejszym rozporządzeniu.

(165) Opracowywanie systemów AI innych niż systemy AI wysokiego ryzyka z uwzględnieniem wymogów niniejszego rozporządzenia może doprowadzić do szerszego upowszechnienia ***etycznej i*** godnej zaufania AI w Unii. Dostawców systemów AI niebędących systemami wysokiego ryzyka należy zachęcać do opracowywania kodeksów postępowania***, w tym powiązanych mechanizmów zarządzania,*** wspierających dobrowolne stosowanie ***niektórych lub wszystkich*** obowiązkowych wymogów mających zastosowanie do systemów AI wysokiego ryzyka***, dostosowanych do przeznaczenia tych systemów i związanego z nimi niższego ryzyka oraz z uwzględnieniem dostępnych rozwiązań technicznych i najlepszych praktyk branżowych, takich jak karty modeli i karty charakterystyki***. Dostawców ***wszystkich systemów AI, wysokiego ryzyka lub nie, oraz modeli AI, a w stosownych przypadkach, podmioty stosujące te systemy i modele*** należy również zachęcać do dobrowolnego stosowania dodatkowych wymogów dotyczących na przykład ***elementów unijnych Wytycznych w zakresie etyki dotyczących godnej zaufania sztucznej inteligencji***, zrównoważenia środowiskowego, ***środków wspierających kompetencje w zakresie AI, projektowania i opracowywania systemów AI z uwzględnieniem różnorodności i inkluzywności, w tym szczególnej uwagi poświęconej osobom szczególnie wrażliwym i*** dostępności dla osób z niepełnosprawnościami, udziału zainteresowanych stron ***w tym, w stosownych przypadkach, organizacji przedsiębiorców i społeczeństwa obywatelskiego, środowisk akademickich, organizacji badawczych, związków zawodowych i organizacji ochrony konsumentów*** w projektowaniu i opracowywaniu systemów AI oraz dotyczących różnorodności zespołów programistycznych***, w tym pod względem równowagi płci. By być skuteczne, dobrowolne kodeksy postępowania powinny opierać się na jasnych celach i kluczowych wskaźnikach skuteczności działania służących do pomiaru stopnia osiągnięcia tych celów. Należy je również rozwijać w sposób inkluzywny, w stosownych przypadkach, z udziałem odpowiednich zainteresowanych stron, takich jak organizacje przedsiębiorców i społeczeństwa obywatelskiego, środowiska akademickie, organizacje badawcze, związki zawodowe i organizacje ochrony konsumentów***. Komisja może opracowywać inicjatywy, również o charakterze sektorowym, aby ułatwiać zmniejszanie barier technicznych utrudniających transgraniczną wymianę danych na potrzeby rozwoju AI, w tym w zakresie infrastruktury dostępu do danych oraz interoperacyjności semantycznej i technicznej różnych rodzajów danych.

(166) Istotne jest, aby systemy AI związane z produktami, które nie są systemami wysokiego ryzyka w rozumieniu niniejszego rozporządzenia, a zatem nie muszą spełniać wymogów dla ***systemów AI wysokiego ryzyka***, były mimo to bezpieczne w chwili wprowadzenia ich do obrotu lub oddawania ich do użytku. Aby przyczynić się do osiągnięcia tego celu, ***rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988***[56] miałoby zastosowanie jako „bezpiecznik".

(167) 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***, zgodnie z prawem unijnym lub krajowym***. ***Powinny one wykonywać swoje zadania i prowadzić działania w taki sposób, aby chronić w szczególności prawa własności intelektualnej, poufne informacje handlowe i tajemnice przedsiębiorstwa, skuteczne wdrażanie niniejszego rozporządzenia, interesy bezpieczeństwa publicznego i narodowego, integralność postępowań karnych i administracyjnych oraz integralność informacji niejawnych.***

---

[56] ***Rozporządzenie*** Parlamentu Europejskiego i Rady ***(UE) 2023/988*** z dnia ***10 maja 2023 r.*** w sprawie ogólnego bezpieczeństwa produktów***, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz.U. L 135 z 23.5.2023, s. 1).***

(168) ***Zgodność z niniejszym rozporządzeniem powinna być możliwa do wyegzekwowania poprzez nakładanie kar i innych środków egzekwowania prawa.*** 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 tym w poszanowaniu zasady ne bis in idem. Aby wzmocnić i zharmonizować kary administracyjne za naruszenie niniejszego rozporządzenia należy ustanowić górne limity dla ustalania administracyjnych kar pieniężnych*** za niektóre konkretne naruszenia. ***Przy ocenie wysokości kar pieniężnych,*** państwa członkowskie powinny w ***każdym indywidualnym przypadku*** brać pod uwagę ***wszystkie istotne okoliczności danej sytuacji, z należytym uwzględnieniem w szczególności charakteru, wagi i czasu trwania naruszenia oraz jego skutków, a także wielkości dostawcy, w szczególności faktu, czy dostawca jest MŚP, w tym przedsiębiorstwem typu start-up***. Europejski Inspektor Ochrony Danych powinien mieć uprawnienia do nakładania kar pieniężnych na instytucje, organy i jednostki organizacyjne Unii objęte zakresem stosowania niniejszego rozporządzenia.

(169) Zgodność z obowiązkami spoczywającymi na dostawcach modeli AI ogólnego przeznaczenia nałożonymi na mocy niniejszego rozporządzenia powinna być możliwa do wyegzekwowania m.in. za pomocą kar pieniężnych. W tym celu należy również ustanowić odpowiednią wysokość kar pieniężnych za naruszenie tych obowiązków, w tym za niezastosowanie środków wymaganych przez Komisję zgodnie z niniejszym rozporządzeniem, z zastrzeżeniem odpowiednich terminów przedawnienia zgodnie z zasadą proporcjonalności. Wszystkie decyzje przyjmowane przez Komisję na podstawie niniejszego rozporządzenia podlegają kontroli Trybunału Sprawiedliwości Unii Europejskiej zgodnie z TFUE.

(170) W przepisach unijnych i krajowych przewidziano już skuteczne środki odwoławcze dla osób fizycznych i prawnych, na których prawa i wolności negatywnie wpływa wykorzystanie systemów AI. Bez uszczerbku dla tych środków odwoławczych każda osoba fizyczna lub prawna, która ma podstawy, by uznać, że doszło do naruszenia niniejszego rozporządzenia, powinna być uprawniona do wniesienia skargi do właściwego organu nadzoru rynku.

(171) Osoby, których to dotyczy, powinny mieć prawo do uzyskania wyjaśnienia, jeżeli decyzja podmiotu stosującego AI opiera się głównie na wynikach określonych systemów wysokiego ryzyka objętych zakresem stosowania niniejszego rozporządzenia i jeżeli decyzja ta wywołuje skutki prawne lub podobnie znacząco oddziałuje na te osoby w sposób, który ich zdaniem ma niepożądany wpływ na ich zdrowie, bezpieczeństwo lub prawa podstawowe. Wyjaśnienie to powinno być jasne i merytoryczne oraz powinno dawać osobom, których to dotyczy, podstawę do korzystania z ich praw. Prawo do uzyskania wyjaśnienia nie powinno mieć zastosowania do wykorzystania systemów AI, co do których na mocy unijnych lub krajowych przepisów obowiązują wyjątki lub ograniczenia, i powinno mieć zastosowanie wyłącznie w zakresie, w jakim prawo to nie jest jeszcze przewidziane w przepisach Unii.

(172) Osoby działające w charakterze sygnalistów w związku z naruszeniami niniejszego rozporządzenia powinny być chronione na mocy prawa Unii. Do zgłaszania naruszeń przepisów niniejszego rozporządzenia oraz ochrony osób zgłaszających przypadki naruszeń powinno zatem stosować się dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937[57].

---

57 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.U. L 305 z 26.11.2019, s. 17).

(173) Aby zapewnić możliwość dostosowania w razie potrzeby ram regulacyjnych, Komisji należy na podstawie art. 290 TFUE przekazać uprawnienia do przyjmowania aktów w celu zmiany warunków, na podstawie których system AI nie jest uznawany za system AI wysokiego ryzyka, zmiany wykazu systemów AI wysokiego ryzyka, przepisów dotyczących dokumentacji technicznej, treści deklaracji zgodności UE, przepisów dotyczących procedur oceny zgodności**,** przepisów określających systemy AI wysokiego ryzyka, do których powinna mieć zastosowanie procedura oceny zgodności oparta na ocenie systemu zarządzania jakością oraz ocenie dokumentacji technicznej***, progu, poziomów odniesienia i wskaźników, które zostały określone w przepisach dotyczących klasyfikacji modeli AI ogólnego przeznaczenia z ryzykiem systemowym, w tym poprzez uzupełnienie tych poziomów odniesienia i wskaźników, kryteriów uznawania modeli za modele AI ogólnego przeznaczenia z ryzykiem systemowym, dokumentacji technicznej dostawców modeli AI ogólnego przeznaczenia oraz informacji dotyczących przejrzystości od dostawców modeli AI ogólnego przeznaczenia***. 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.

---

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

(174) Z uwagi na szybki rozwój technologiczny i konieczność dysponowania wiedzą techniczną dla skutecznego stosowania niniejszego rozporządzenia, Komisja powinna dokonać oceny i przeglądu niniejszego rozporządzenia do dnia ... [pięć lat od daty wejścia w życie niniejszego rozporządzenia], a następnie co cztery lata oraz składać sprawozdania Parlamentowi Europejskiemu i Radzie. Ponadto ze względu na skutki dla zakresu stosowania niniejszego rozporządzenia Komisja powinna raz w roku ocenić, czy konieczne jest wprowadzenie zmian w wykazie systemów AI wysokiego ryzyka i w wykazie zakazanych praktyk. Dodatkowo w terminie dwóch lat od daty rozpoczęcia stosowania niniejszego rozporządzenia, a następnie co cztery lata, Komisja powinna ocenić, czy należy wprowadzić zmiany w wykazie obszarów wysokiego ryzyka zawartym w załączniku do niniejszego rozporządzenia, zmiany w wykazie systemów AI objętych obowiązkami w zakresie przejrzystości, zmiany służące skuteczności systemu nadzoru i zarządzania oraz ocenić postępy w opracowywaniu dokumentów normalizacyjnych dotyczących efektywnego energetycznie rozwoju modeli AI ogólnego przeznaczenia, w tym potrzebę wprowadzenia dalszych środków lub działań, a następnie przekazać sprawozdania z tych ocen Parlamentowi Europejskiemu i Radzie. Ponadto do dnia ... [cztery lata od wejścia w życie niniejszego rozporządzenia], a następnie co trzy lata, Komisja powinna oceniać wpływ i skuteczność dobrowolnych kodeksów postępowania pod kątem wspierania stosowania wymogów przewidzianych wobec systemów AI wysokiego ryzyka w przypadku systemów AI innych niż systemy AI wysokiego ryzyka oraz ewentualnie innych dodatkowych wymogów dotyczących takich systemów.

(175) 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].

(176) Ponieważ cel niniejszego rozporządzenia, a mianowicie poprawa funkcjonowania rynku wewnętrznego i promowanie upowszechniania ukierunkowanej na człowieka i godnej zaufania AI, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych zapisanych w Karcie, w tym demokracji, praworządności i ochrony środowiska przed szkodliwymi skutkami systemów AI w Unii, oraz wspieranie innowacji, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary lub skutki działania 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 tych celów.

---

[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).

(177) Aby zapewnić pewność prawa, zapewnić operatorom odpowiedni okres na dostosowanie się i uniknąć zakłóceń na rynku, w tym dzięki zapewnieniu ciągłości korzystania z systemów AI, niniejsze rozporządzenie powinno mieć zastosowanie do systemów AI wysokiego ryzyka, które zostały wprowadzone do obrotu lub oddane do użytku przed ogólną datą rozpoczęcia jego stosowania, tylko wtedy, gdy po tej dacie w systemach tych wprowadzane będą istotne zmiany w ich projekcie lub przeznaczeniu. Należy wyjaśnić, że w tym względzie pojęcie istotnej zmiany należy rozumieć jako równoważne znaczeniowo z pojęciem istotnej zmiany, które stosuje się wyłącznie w odniesieniu do systemów AI wysokiego ryzyka na mocy niniejszego rozporządzenia. W drodze wyjątku i z uwagi na odpowiedzialność publiczną, operatorzy systemów AI, które są elementami wielkoskalowych systemów informatycznych ustanowionych na mocy aktów prawnych wymienionych w załączniku do niniejszego rozporządzenia, oraz operatorzy systemów AI wysokiego ryzyka, które mają być wykorzystywane przez organy publiczne, powinni odpowiednio podjąć niezbędne kroki w celu spełnienia wymogów niniejszego rozporządzenia do końca 2030 r. i w terminie sześciu lat po jego wejściu w życie.

(178) Dostawców systemów AI wysokiego ryzyka zachęca się, by dobrowolnie zaczęli wypełniać odpowiednie obowiązki wynikające z niniejszego rozporządzenia już w okresie przejściowym.

(179) Niniejsze rozporządzenie powinno stosować się od ... [dwa lata od daty wejścia w życie niniejszego rozporządzenia] r. ***Biorąc*** jednak ***pod uwagę niedopuszczalne ryzyko związane z niektórymi sposobami stosowania AI, przedmiotowe zakazy powinny obowiązywać już od dnia... [sześć miesięcy od daty wejścia w życie niniejszego rozporządzenia]. Chociaż pełne skutki tych zakazów zrealizowane zostaną w momencie ustanowienia zarządzania i egzekwowania niniejszego rozporządzenia, wcześniejsze ich stosowanie jest ważne, by uwzględnić niedopuszczalne ryzyko i wywrzeć wpływ na inne procedury, np. w prawie cywilnym. Ponadto*** infrastruktura związana z zarządzaniem i systemem oceny zgodności powinna być gotowa do działania przed tą datą, w związku z czym przepisy dotyczące jednostek notyfikowanych oraz struktury zarządzania powinny mieć zastosowanie od dnia … [***12*** miesięcy ***od daty*** wejścia w życie niniejszego rozporządzenia]. ***Biorąc pod uwagę szybkie tempo postępu technologicznego i przyjęcie modeli AI ogólnego przeznaczenia, obowiązki dostawców modeli AI ogólnego przeznaczenia powinny mieć zastosowanie od dnia ... [12 miesięcy od daty wejścia w życie niniejszego rozporządzenia]. Kodeksy praktyk powinny być gotowe do dnia ... [9 miesięcy od daty wejścia w życie*** niniejszego rozporządzenia]***, tak aby umożliwić dostawcom terminowe wykazanie zgodności. Urząd ds. AI powinien zapewniać aktualność zasad i procedur klasyfikacji w świetle rozwoju technologicznego.*** 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 … [12 miesięcy od daty wejścia w życie niniejszego rozporządzenia].

(180) Zgodnie z art. 42 ust. 1 i 2 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, którzy wydali wspólną opinię dnia ▌ ***18 czerwca 2021 r.***,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

1. ***Celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego i promowanie upowszechniania ukierunkowanej na człowieka i godnej zaufania sztucznej inteligencji (AI), przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie praw podstawowych, w tym demokracji, praworządności oraz ochrony środowiska, przed szkodliwymi skutkami systemów sztucznej inteligencji*** (systemów AI) w ***Unii, a także wspieranie innowacji.***

2. W niniejszym rozporządzeniu ustanawia się:

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

   b) zakazy dotyczące niektórych praktyk w zakresie AI;

   c) szczególne wymogi dotyczące systemów AI wysokiego ryzyka oraz obowiązki spoczywające na operatorach takich systemów;

d) zharmonizowane przepisy dotyczące przejrzystości w przypadku ***niektórych*** systemów AI;

e) zharmonizowane przepisy dotyczące wprowadzania do obrotu modeli AI ogólnego przeznaczenia;

f) przepisy dotyczące monitorowania wprowadzania do obrotu***, zarządzania nadzorem rynku i egzekwowania tego nadzoru;***

g) środki wspierające innowacje, ze szczególnym uwzględnieniem MŚP, w tym przedsiębiorstw typu start-up.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do:

a) dostawców wprowadzających do obrotu lub oddających do użytku systemy AI ***lub wprowadzających do obrotu modele AI ogólnego przeznaczenia*** w Unii, niezależnie od tego, czy dostawcy ci mają siedzibę ***lub znajdują się*** w Unii czy w państwie trzecim;

b) ***podmiotów stosujących systemy*** AI, ***które to podmioty mają siedzibę lub*** znajdują się w Unii;

c) dostawców systemów AI i ***podmiotów stosujących systemy AI***, którzy ***mają siedzibę lub*** znajdują się w państwie trzecim, w przypadku gdy wyniki działania systemu AI są wykorzystywane w Unii;

d) importerów i dystrybutorów systemów AI;

e) producentów, którzy wraz ze swoim produktem wprowadzają do obrotu lub oddają do użytku system AI opatrzony ich nazwą handlową lub znakiem towarowym;

f) upoważnionych przedstawicieli dostawców niemających siedziby w Unii;

g) osób, na które AI ma wpływ i które znajdują się w Unii.

2. W przypadku systemów AI ▌ ***zaklasyfikowanych jako systemy AI wysokiego ryzyka zgodnie z art. 6 ust. 1 i 2 związanych z*** produktami ***objętymi unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I sekcja B,*** zastosowanie ma wyłącznie art. 112***. Art. 57 stosuje się wyłącznie w zakresie, w jakim wymogi dotyczące systemów AI wysokiego ryzyka określone w niniejszym rozporządzeniu zostały włączone do tego unijnego prawodawstwa harmonizacyjnego.***

▌

3. ***Niniejsze rozporządzenie nie ma zastosowania do obszarów wykraczających poza zakres prawa Unii i w żadnym wypadku nie wpływa na kompetencje państw członkowskich w zakresie bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu, któremu państwa członkowskie powierzyły wykonywanie zadań związanych z tymi kompetencjami.***

Niniejsze rozporządzenie nie ma zastosowania do systemów AI***, jeżeli – i w zakresie, w jakim – wprowadzono je do obrotu, oddano do użytku lub korzysta się z nich ze zmianami lub bez zmian wyłącznie do celów wojskowych, obronnych lub do celów bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu prowadzącego te działania.***

Niniejsze rozporządzenie nie ma zastosowania do systemów AI, które nie są wprowadzone do obrotu ani oddane do użytku w Unii, a których wyniki są wykorzystywane w Unii wyłącznie do celów wojskowych***, obronnych lub de celów bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu prowadzącego te działania***.

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 AI w ramach ***współpracy międzynarodowej lub*** umów międzynarodowych w sprawie ścigania przestępstw i współpracy sądowej zawartych z Unią lub z jednym państwem członkowskim bądź ich większą liczbą***, pod warunkiem zapewnienia przez to państwo trzecie lub organizację międzynarodową odpowiednich zabezpieczeń w odniesieniu do ochrony podstawowych praw i wolności jednostek.***

5. Niniejsze rozporządzenie nie ma wpływu na stosowanie przepisów dotyczących odpowiedzialności dostawców usług pośrednich określonych w rozdziale II rozporządzenia (UE) 2022/2065.

6. Niniejsze rozporządzenie nie ma zastosowania do systemów AI lub modeli AI, w tym ich wyników, opracowanych i oddanych do użytku wyłącznie do celów badań naukowych i działalności rozwojowej.

7. Prawo Unii w zakresie ochrony danych osobowych, prywatności i poufności komunikacji ma zastosowanie do danych osobowych przetwarzanych w związku z prawami i obowiązkami określonymi w niniejszym rozporządzeniu. Niniejsze rozporządzenie nie ma wpływu na rozporządzenia (UE) 2016/679 i (UE) 2018/1725, ani na dyrektywy 2002/58/WE i (UE) 2016/680, z zastrzeżeniem ustaleń przewidzianych w art. 10 ust. 5 i art. 59 niniejszego rozporządzenia.

8. Niniejsze rozporządzenie nie ma zastosowania do żadnej działalności badawczej, testowej ani rozwojowej dotyczącej systemów lub modeli AI przed wprowadzeniem ich do obrotu lub oddaniem do użytku. Działania te prowadzone są zgodnie z mającym zastosowanie prawem Unii. Niniejsze wyłączenie nie obejmuje testów w warunkach rzeczywistych.

9. Niniejsze rozporządzenie nie narusza przepisów określonych w innych aktach prawnych Unii dotyczących ochrony konsumentów i bezpieczeństwa produktów.

10. Niniejsze rozporządzenie nie ma zastosowania do obowiązków podmiotów stosujących AI będących osobami fizycznymi, które korzystają z systemów AI w ramach czysto osobistej działalności pozazawodowej.

11. Niniejsze rozporządzenie nie uniemożliwia Unii ani państwom członkowskim utrzymywania lub wprowadzania przepisów ustawowych, wykonawczych lub administracyjnych, które są korzystniejsze dla pracowników pod względem ochrony ich praw w odniesieniu do korzystania z systemów AI przez pracodawców, ani zachęcania do stosowania korzystniejszych dla pracowników układów zbiorowych lub zezwalania na ich stosowanie.

12. Niniejsze rozporządzenie ma zastosowanie do systemów AI udostępnianych na podstawie bezpłatnych i otwartych licencji, chyba że systemy te są wprowadzane do obrotu lub oddawane do użytku jako systemy AI wysokiego ryzyka lub system AI objęty art. 5 lub art. 50.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „system ***AI***” ***oznacza system maszynowy, zaprojektowany do działania z różnym poziomem autonomii, który może po wdrożeniu wykazywać zdolność adaptacji i który – do wyraźnych lub dorozumianych celów – wnioskuje, jak*** generować ***na podstawie danych wejściowych*** wyniki, takie jak ***predykcje, treści***, zalecenia lub decyzje***, które mogą wpływać na*** środowisko ***fizyczne lub wirtualne***;

2) „ryzyko” oznacza połączenie prawdopodobieństwa wystąpienia szkody oraz stopnia jej powagi;

3) „dostawca” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które opracowują system AI lub ***model AI ogólnego przeznaczenia lub zlecają ich opracowanie i które wprowadzają go do obrotu lub oddają system AI*** do użytku pod własną nazwą handlową lub własnym znakiem towarowym – odpłatnie lub nieodpłatnie;

4) ***„podmiot stosujący AI”*** oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które korzystają z systemu AI i sprawują nad nim kontrolę, z wyjątkiem sytuacji, gdy system AI jest wykorzystywany w ramach osobistej działalności pozazawodowej;

5) „upoważniony przedstawiciel” oznacza osobę fizyczną lub prawną ***znajdującą się lub*** mającą siedzibę w Unii, która otrzymała ***i zaakceptowała*** pisemne pełnomocnictwo od dostawcy systemu AI ***lub modelu AI ogólnego przeznaczenia*** do, odpowiednio, realizacji w jego imieniu obowiązków i przeprowadzania procedur ustanowionych w niniejszym rozporządzeniu;

6) „importer” oznacza osobę fizyczną lub prawną ***znajdującą się lub*** mającą siedzibę w Unii, która wprowadza do obrotu ▌ system AI opatrzony nazwą handlową lub znakiem towarowym osoby fizycznej lub prawnej mającej siedzibę w państwie trzecim;

7) „dystrybutor” oznacza osobę fizyczną lub prawną w łańcuchu dostaw, inną niż dostawca lub importer, która udostępnia system AI na rynku unijnym ▌ ;

8) „operator” oznacza dostawcę, ***producenta produktu, podmiot stosujący AI,*** upoważnionego przedstawiciela, importera ***lub*** dystrybutora;

9) „wprowadzenie do obrotu” oznacza udostępnienie systemu AI ***lub modelu AI ogólnego przeznaczenia*** na rynku unijnym po raz pierwszy;

10) „udostępnianie na rynku” oznacza dostarczanie systemu AI ***lub modelu AI ogólnego przeznaczenia*** w celu jego dystrybucji lub wykorzystania na rynku unijnym w ramach działalności handlowej, odpłatnie lub nieodpłatnie;

11) „oddanie do użytku” oznacza dostarczenie przez dostawcę systemu AI do pierwszego użycia bezpośrednio ***podmiotowi stosującemu AI*** lub do użytku własnego – w Unii, zgodnie z jego przeznaczeniem;

12) „przeznaczenie” oznacza zastosowanie, do jakiego system AI został przeznaczony przez jego dostawcę, w tym konkretny 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 AI w sposób niezgodny z jego przeznaczeniem, które może wynikać z dającego się racjonalnie przewidzieć zachowania człowieka lub interakcji z innymi systemami***, w tym z innymi systemami AI***;

14) „element związany z bezpieczeństwem” 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 podmiotu stosującego AI w szczególności o przeznaczeniu i właściwym użytkowaniu systemu AI ▌ ;

16) „wycofanie systemu AI z użytku” oznacza dowolny środek mający na celu doprowadzenie do zwrotu do dostawcy systemu AI udostępnionego ***podmiotom stosującym AI lub do wyłączenia takiego systemu z eksploatacji lub uniemożliwienia korzystania z niego***;

17) „wycofanie systemu AI z rynku” oznacza dowolny środek mający na celu uniemożliwienie ***udostępnienia na rynku systemu AI w ramach łańcucha dostaw***;

18) „skuteczność działania systemu AI” oznacza zdolność systemu AI 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 ***wykazania,*** czy spełniono wymogi określone w rozdziale II sekcja 2 w odniesieniu do systemu AI ***wysokiego ryzyka***;

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

22) „jednostka notyfikowana” oznacza jednostkę oceniającą zgodność, którą ***notyfikuje się*** zgodnie z niniejszym rozporządzeniem i innym stosownym unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I sekcja B;

23) „istotna zmiana” oznacza modyfikację w systemie AI ***po*** jego wprowadzeniu do obrotu lub oddaniu do użytku, która ***nie została przewidziana lub zaplanowana przy początkowej ocenie zgodności przeprowadzonej przez dostawcę i w wyniku której naruszona zostaje*** zgodność systemu AI z wymogami określonymi w rozdziale II sekcja 2, lub która powoduje zmianę przeznaczenia, w odniesieniu do którego oceniono system AI;

24) „oznakowanie CE” oznacza oznakowanie, za pomocą którego dostawca wskazuje, że system AI spełnia wymogi określone w rozdziale II sekcja 2 i innych mających zastosowanie unijnych przepisach harmonizacyjnych wymienionych w załączniku I, przewidujących umieszczanie takiego oznakowania;

25) „***system*** monitorowania po wprowadzeniu do obrotu” oznacza wszelkie działania prowadzone przez dostawców systemów AI służące ▌ gromadzeniu i przeglądowi doświadczeń zdobytych w wyniku użytkowania systemów AI, 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 zharmonizowaną określoną w art. 2 pkt 1 lit. c) rozporządzenia (UE) nr 1025/2012;

28) „wspólna ***specyfikacja***” oznacza ***zestaw specyfikacji technicznych zdefiniowanych w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012 zapewniających*** środki umożliwiające spełnienie niektórych wymogów ▌ ustanowionych w niniejszym rozporządzeniu;

29) „dane treningowe” oznaczają dane wykorzystywane do trenowania systemu AI poprzez dopasowanie jego parametrów podlegających uczeniu ▌ ;

30) „dane walidacyjne” oznaczają dane służące do oceny trenowanego systemu AI oraz do dostosowywania jego parametrów niepodlegających uczeniu oraz procesu uczenia, między innymi w celu zapobiegania ***niedostatecznemu wytrenowaniu lub*** przetrenowaniu;

31) „zbiór danych walidacyjnych” oznacza oddzielny zbiór danych lub część zbioru danych treningowych, w którym to przypadku udział tego podzbioru w zbiorze danych treningowych może być stały lub zmienny;

32) „dane testowe” oznaczają dane wykorzystywane do przeprowadzenia niezależnej oceny systemu ▌ AI w celu potwierdzenia oczekiwanej skuteczności działania tego systemu przed wprowadzeniem go do obrotu lub oddaniem go do użytku;

33) „dane wejściowe” oznaczają dane dostarczone do systemu AI lub bezpośrednio przez niego pozyskiwane, na podstawie których system ten generuje wynik działania;

34) „dane biometryczne” oznaczają dane osobowe będące wynikiem specjalnego przetwarzania technicznego, które dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, takich jak wizerunek twarzy lub dane daktyloskopijne;

35) „identyfikacja biometryczna” oznacza automatyczne rozpoznawanie fizycznych, fizjologicznych, behawioralnych lub psychologicznych cech ludzkich w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z danymi biometrycznymi osób przechowywanymi w bazie danych;

36) „weryfikacja biometryczna” oznacza zautomatyzowaną weryfikację typu jeden-do-jednego tożsamości osób fizycznych przez porównanie ich danych biometrycznych z wcześniej przekazanymi danymi biometrycznymi, w tym uwierzytelnianie;

37) „szczególne kategorie danych osobowych” oznaczają 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;

38) „wrażliwe dane operacyjne” oznaczają dane operacyjne związane z działaniami w zakresie zapobiegania przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania, których ujawnienie mogłoby zagrozić integralności postępowania karnego;

39) „system rozpoznawania emocji” oznacza system AI służący do rozpoznawania emocji lub zamiarów osób fizycznych na podstawie danych biometrycznych tych osób, lub wyciągania wniosków odnośnie do tych emocji lub zamiarów;

40) „system kategoryzacji biometrycznej” oznacza system AI służący do przypisywania osób fizycznych do określonych kategorii ***na podstawie danych biometrycznych tych osób, oprócz przypadków, gdy taki system pełni funkcję pomocniczą w stosunku do innej usługi komercyjnej i jest bezwzględnie konieczny z obiektywnych względów technicznych***;

41) „system zdalnej identyfikacji biometrycznej” oznacza system AI służący do identyfikacji osób fizycznych ***bez ich aktywnego udziału, co do zasady*** na odległość, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych ▌ ;

42) „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, i obejmuje nie tylko natychmiastową identyfikację, ale też – aby uniknąć obchodzenia przepisów – identyfikację dokonywaną z niewielkim opóźnieniem;

43) „system zdalnej identyfikacji biometrycznej *post factum*” oznacza system zdalnej identyfikacji biometrycznej inny niż system zdalnej identyfikacji biometrycznej w czasie rzeczywistym;

44) „przestrzeń publiczna” oznacza każde miejsce fizyczne, ***będące własnością prywatną czy publiczną***, dostępne dla ***nieokreślonej liczby osób fizycznych*** niezależnie od tego, czy mogą mieć zastosowanie określone warunki dostępu***, oraz niezależnie od potencjalnych ograniczeń pojemności***;

45) „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;

46) „ściganie przestępstw” oznacza działania prowadzone przez organy ścigania ***lub w ich imieniu*** 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;

47) ***„Urząd ds. AI” oznacza należące do Komisji zadanie polegające na przyczynianiu się do wdrażania, monitorowania i nadzorowania systemów AI i zarządzania AI, które wykonuje Europejski Urząd ds. Sztucznej Inteligencji ustanowiony decyzją Komisji z dnia 24 stycznia 2024 r.; zawarte w niniejszym rozporządzeniu odniesienia do Urzędu ds. AI rozumie się jako odniesienia do Komisji;***

48) „właściwy organ krajowy” oznacza organ notyfikujący i organ nadzoru rynku***;***

49) „poważny incydent” oznacza incydent ***lub nieprawidłowe działanie systemu AI, które bezpośrednio lub pośrednio prowadzą*** do któregokolwiek z poniższych zdarzeń:

a) śmierci osoby lub poważnego uszczerbku na zdrowiu osoby***;***

b) poważnego i nieodwracalnego zakłócenia w zarządzaniu infrastrukturą krytyczną lub jej obsłudze;

c) naruszenia ***obowiązków przewidzianych w prawie Unii, których celem jest ochrona praw podstawowych;***

d) poważnego uszkodzenia mienia lub szkody dla środowiska;

50) „dane osobowe” oznaczają dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

51) „dane nieosobowe” oznaczają dane inne niż dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

52) „profilowanie” oznacza profilowanie zdefiniowane w art. 4 pkt 4 rozporządzenia (UE) 2016/679 lub – w przypadku organów ścigania – zdefiniowane w art. 3 pkt 4 dyrektywy (UE) 2016/680 lub – w przypadku instytucji, organów lub jednostek organizacyjnych Unii – w art. 3 pkt 5 rozporządzenia (UE) 2018/1725;

53) „plan testów w warunkach rzeczywistych” oznacza dokument opisujący cele, metodykę, zasięg geograficzny, populacyjny i czasowy, monitorowanie, organizację i przeprowadzanie testów w warunkach rzeczywistych;

54) „plan działania piaskownicy” oznacza dokument uzgodniony między uczestniczącym dostawcą a właściwym organem opisujący cele, warunki, ramy czasowe, metodykę i wymogi dotyczące działań prowadzonych w ramach piaskownicy;

55) „piaskownica regulacyjna w zakresie AI” oznacza kontrolowane ramy ustanowione przez właściwy organ, umożliwiające dostawcom lub potencjalnym dostawcom systemów AI możliwość opracowywania, trenowania, walidacji i testowania – w stosownych przypadkach w warunkach rzeczywistych – innowacyjnych systemów AI, w oparciu o plan działania piaskownicy, w ograniczonym czasie i pod nadzorem regulacyjnym;

56) „kompetencje w zakresie AI" oznaczają umiejętności, wiedzę oraz zrozumienie, które pozwalają dostawcom, podmiotom stosującym AI i osobom, na które AI ma wpływ – z uwzględnieniem ich odnośnych praw i obowiązków w kontekście niniejszego rozporządzenia – w przemyślany sposób stosować systemy sztucznej inteligencji oraz mieć świadomość, jakie możliwości i zagrożenia wiążą się z AI oraz jakie potencjalne szkody może ona wyrządzić;

57) „testy w warunkach rzeczywistych" oznaczają ograniczone w czasie testy systemu AI dotyczące jego przeznaczenia prowadzone w warunkach rzeczywistych – poza środowiskiem laboratoryjnym lub środowiskiem symulowanym innego typu – w celu zgromadzenia wiarygodnych i solidnych danych oraz w celu oceny i weryfikacji zgodności systemu AI z wymogami niniejszego rozporządzenia i nie są uznawane za wprowadzanie systemu AI do obrotu lub oddawanie go do użytku w rozumieniu niniejszego rozporządzenia, o ile spełnione są wszystkie warunki określone w art. 57 lub 60;

58) „uczestnik" do celów testów w warunkach rzeczywistych oznacza osobę fizyczną, która uczestniczy w testach tego typu;

59) „świadoma zgoda" oznacza swobodne, konkretne, jednoznaczne i dobrowolne wyrażenie przez uczestnika zgody na uczestnictwo w określonych testach w warunkach rzeczywistych, po uzyskaniu informacji o wszystkich aspektach testów, które są istotne dla decyzji o uczestnictwie podejmowanej przez uczestnika;

60) „deepfake" oznacza wygenerowane lub zmanipulowane obraz, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca lub inne podmioty lub zdarzenia i które odbiorca mogłyby niesłusznie uznać za autentyczne lub prawdziwe;

61) „powszechne naruszenie" oznacza każdy czyn lub każde zaniechanie sprzeczne z prawem Unii chroniącym interesy jednostek, które:

a) szkodzi lub może zaszkodzić zbiorowym interesom jednostek zamieszkałych w co najmniej dwóch państwach członkowskich innych niż państwo członkowskie, w którym:

(i) czyn lub zaniechanie miały swoje źródło lub miejsce;

(ii) znajduje się lub siedzibę ma dany dostawca lub, w stosownych przypadkach, jego upoważniony przedstawiciel; lub

(iii) siedzibę ma podmiot stosujący AI, jeżeli naruszenie zostało popełnione przez ten podmiot;

b) zaszkodziło, szkodzi lub może zaszkodzić zbiorowym interesom jednostek i ma cechy wspólne, w tym dotyczy tej samej bezprawnej praktyki lub naruszenia tego samego interesu, oraz zachodzi jednocześnie, dopuszcza się ich ten sam operator, w co najmniej trzech państwach członkowskich;

62) „infrastruktura krytyczna” oznacza infrastrukturę krytyczną zdefiniowaną w art. 2 pkt 4 dyrektywy (UE) 2022/2557;

63) „model AI ogólnego przeznaczenia” oznacza model AI, w tym model AI trenowany dużą ilością danych z wykorzystaniem nadzoru własnego na dużą skalę, który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model jest wprowadzany do obrotu, i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla – z wyłączeniem modeli AI, które są wykorzystywane na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu;

64) „zdolności dużego oddziaływania” oznaczają zdolności, które dorównują zdolnościom zapisanym w najbardziej zaawansowanych modelach AI ogólnego przeznaczenia lub je przewyższają;

65) „ryzyko systemowe” oznacza ryzyko, które jest charakterystyczne dla modeli AI ogólnego przeznaczenia posiadających zdolności dużego oddziaływania i ma znaczący wpływ na rynek Unii ze względu na zasięg tych modeli lub rzeczywiste lub racjonalnie przewidywalne negatywne skutki dla zdrowia publicznego, porządku publicznego, bezpieczeństwa publicznego, praw podstawowych lub całego społeczeństwa, mogące rozprzestrzenić się na dużą skalę w całym łańcuchu wartości;

66) „system AI ogólnego przeznaczenia" oznacza system AI oparty na modelu AI ogólnego przeznaczenia, który może służyć różnym celom, nadający się zarówno do bezpośredniego wykorzystania, jak i do integracji z innymi systemami AI;

67) „operacja zmiennoprzecinkowa" („FLOP") oznacza każdą operację matematyczną lub zadanie z wykorzystaniem liczb zmiennoprzecinkowych, które stanowią podzbiór liczb rzeczywistych zwykle przedstawianych na komputerach przez liczbę całkowitą o stałej dokładności przeskalowaną przez całkowity wykładnik stałej podstawy systemu liczbowego;

68) „dostawca niższego szczebla" oznacza dostawcę systemu AI, w tym systemu AI ogólnego przeznaczenia, opracowanego w drodze integracji modelu AI, niezależnie od tego, czy model ten jest dostarczany przez tego samego dostawcę i zintegrowany pionowo czy dostarczany przez inny podmiot na podstawie stosunków umownych.

Artykuł 4
Kompetencje w zakresie AI

Dostawcy i podmioty stosujące AI podejmują środki w celu zapewnienia, w możliwie największym stopniu, odpowiedniego poziomu kompetencji w zakresie AI wśród swojego personelu i innych osób zajmujących się obsługą i użytkowaniem systemów AI w ich imieniu, z uwzględnieniem ich wiedzy technicznej, doświadczenia, wykształcenia i wyszkolenia oraz kontekstu, w którym systemy AI mają być użytkowane, a także biorąc pod uwagę osoby lub grupy osób, wobec których systemy AI mają być wykorzystywane.

ROZDZIAŁ II
ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

Artykuł 5

Zakazane praktyki w zakresie AI

1. Zakazuje się następujących praktyk w zakresie AI:

   a) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu AI, który stosuje techniki podprogowe będące poza świadomością danej osoby ***lub celowe techniki manipulacyjne lub wprowadzające w błąd, czego celem lub skutkiem jest*** istotne ***zniekształcenie*** zachowania danej osoby ***lub grupy osób poprzez znaczące ograniczenie ich zdolności do podejmowania świadomych decyzji, powodując tym samym podjęcie przez daną osobę decyzji, której inaczej by nie podjęła,*** w sposób, który powoduje lub może powodować u niej, u innej osoby ***lub u grupy osób poważną*** szkodę;

b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu AI, który wykorzystuje dowolne słabości danej ***osoby lub*** określonej grupy osób ze względu na ich wiek, ***niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną, czego celem lub skutkiem jest*** istotne ***zniekształcenie*** zachowania ***danej osoby lub*** osoby należącej do tej grupy w sposób, który powoduje lub może z ***uzasadnionym*** prawdopodobieństwem spowodować u tej osoby lub u innej osoby ***poważną szkodę***;

c) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów AI ▌ na potrzeby oceny lub klasyfikacji ***osób fizycznych lub grup osób*** prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych***,*** ***wnioskowanych*** bądź przewidywanych cech osobistych lub cech osobowości, kiedy to scoring obywateli 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 ▌ grup osób, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;

d) ***wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemu AI do przeprowadzania ocen ryzyka w odniesieniu do osób fizycznych, by ocenić lub przewidzieć prawdopodobieństwo popełnienia przestępstwa przez osobę fizyczną, wyłącznie na podstawie profilowania osoby fizycznej lub oceny jej cech osobowości i cech charakterystycznych; zakaz ten nie ma zastosowania do systemów AI wykorzystywanych do wspierania dokonywanej przez człowieka oceny zaangażowania danej osoby w działalność przestępczą, która to ocena opiera się już na obiektywnych i weryfikowalnych faktach bezpośrednio związanych z działalnością przestępczą;***

e) ***wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemów AI, które tworzą lub rozbudowują bazy danych służące rozpoznawaniu twarzy poprzez niecelowane pozyskiwanie (ang. scraping) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej;***

f) ***wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemów AI do wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych, z wyjątkiem przypadków, w których system AI ma zostać wdrożony lub wprowadzony do obrotu ze względów medycznych lub bezpieczeństwa;***

g) ***wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemów kategoryzacji biometrycznej, które indywidualnie kategoryzują osoby fizyczne w oparciu o ich dane biometryczne, by wydedukować lub wywnioskować informacje na temat ich rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub filozoficznych, życia seksualnego lub orientacji seksualnej; zakaz ten nie obejmuje żadnych przypadków etykietowania ani filtrowania legalnie pozyskanych zbiorów danych biometrycznych, takich jak obrazy, w oparciu o dane biometryczne, ani kategoryzacji danych biometrycznych – w obszarze ścigania przestępstw;***

h) wykorzystywania systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw, ▌ chyba że – i w zakresie, w jakim – takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:

(i) ukierunkowanego poszukiwania konkretnych ▌ ofiar ***uprowadzeń, handlu ludźmi lub wykorzystywania seksualnego ludzi, a także poszukiwania osób*** zaginionych;

(ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych bądź ***rzeczywistemu i aktualnemu lub rzeczywistemu i przewidywalnemu zagrożeniu*** atakiem terrorystycznym;

(iii) ▌ lokalizowania ***lub*** identyfikowania ***osoby podejrzanej o popełnienie przestępstwa w celu prowadzenia postępowania*** przygotowawczego***, ścigania lub wykonania kar w odniesieniu do przestępstw, o których mowa w załączniku II,*** podlegających w danym państwie członkowskim karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej ***cztery*** lata;

▌

Akapit pierwszy lit. h) pozostaje bez uszczerbku dla art. 9 rozporządzenia (UE) 2016/679 w odniesieniu do przetwarzania danych biometrycznych do celów innych niż ściganie przestępstw.

2. Systemy zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw w odniesieniu do któregokolwiek z celów, o których mowa w ust. 1 lit. h), ***wykorzystuje się jedynie w celach określonych w ust. 1 lit. h), aby potwierdzić tożsamość konkretnej poszukiwanej osoby, i*** uwzględnia się przy tym następujące elementy:

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

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

Ponadto wykorzystywanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw w odniesieniu do któregokolwiek z celów, o których mowa w ust. 1 lit. h) niniejszego artykułu, musi przebiegać z zachowaniem niezbędnych i proporcjonalnych zabezpieczeń i warunków w odniesieniu do takiego wykorzystywania ***zgodnie z zezwalającym na takie wykorzystanie prawem krajowym***, w szczególności w odniesieniu do ograniczeń czasowych, geograficznych i osobowych. ***Wykorzystanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej jest dozwolone tylko wtedy, gdy organ ścigania przeprowadził ocenę skutków w zakresie praw podstawowych, jak przewidziano w art. 27, oraz zarejestrował system w unijnej bazie danych zgodnie z przepisami art. 49. W należycie uzasadnionych nadzwyczajnych przypadkach można jednak rozpocząć korzystanie z takich systemów bez rejestracji w unijnej bazie danych, pod warunkiem że taka rejestracja zostanie dokonana bez zbędnej zwłoki.***

3. Na potrzeby ust. 1 lit. h) i ust. 2, każde ▌ wykorzystanie systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw wymaga uzyskania uprzedniego zezwolenia udzielonego przez organ sądowy lub ▌ ***wydający wiążące decyzje*** niezależny organ administracyjny państwa członkowskiego, w którym ma nastąpić wykorzystanie; zezwolenie to wydawane jest na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego, o których mowa w ust. 5. W należycie uzasadnionych nadzwyczajnych przypadkach korzystanie z takiego systemu można jednak rozpocząć bez zezwolenia***, pod warunkiem że*** wniosek o takie zezwolenie ***zostanie*** złożony ***bez zbędnej zwłoki, najpóźniej w ciągu 24 godzin. W przypadku odmowy udzielenia takiego zezwolenia wykorzystywanie systemu zostaje wstrzymane ze skutkiem natychmiastowym, a wszystkie dane, a także rezultaty i wyniki uzyskane podczas tego wykorzystania zostają natychmiast odrzucone i usunięte***.

Właściwy ***organ*** sądowy ***lub wydający wiążące decyzje niezależny*** organ 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. h), wskazanego we wniosku***, a w szczególności ogranicza się do tego, co jest bezwzględnie konieczne w odniesieniu do przedziału czasowego, a także zakresu geograficznego i podmiotowego.*** Podejmując decyzję w sprawie wniosku ***organ ten*** bierze pod uwagę elementy, o których mowa w ust. 2***. Nie jest możliwe podjęcie decyzji wywołującej niepożądane skutki prawne dla danej osoby wyłącznie na podstawie wyników uzyskanych z systemu zdalnej identyfikacji biometrycznej*** w czasie rzeczywistym***.***

4. Bez uszczerbku dla ust. 3, o każdym wykorzystaniu systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw powiadamia się właściwy organ nadzoru rynku i krajowy organ ochrony danych zgodnie z przepisami krajowymi, o których mowa w ust. 5. Powiadomienie zawiera co najmniej informacje określone w ust. 6 i nie obejmuje wrażliwych danych operacyjnych.

5. Państwo członkowskie może podjąć decyzję o wprowadzeniu możliwości pełnego lub częściowego zezwolenia na wykorzystywanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw w granicach i na warunkach wymienionych w ust. 1 lit. h) i w ust. 2 i 3. ▌ ***Zainteresowane państwa*** członkowskie ustanawiają 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 ***i przygotowywanie sprawozdań w ich sprawie***. W przepisach tych określa się również, w odniesieniu do których celów wymienionych w ust. 1 lit. h) – w tym w odniesieniu do których przestępstw wymienionych w ust. 1 lit. h) ppkt (iii) – właściwe organy mogą uzyskać zezwolenie na wykorzystanie powyższych systemów do celów celu ścigania przestępstw. ***Państwa członkowskie powiadamiają Komisję o tych przepisach najpóźniej 30 dni po ich przyjęciu. Państwa członkowskie mogą wprowadzić, zgodnie z prawem Unii, bardziej restrykcyjne przepisy dotyczące korzystania z systemów zdalnej identyfikacji biometrycznej.***

6. Krajowe organy nadzoru rynku i krajowe organy ochrony danych państw członkowskich, które zostały powiadomione o wykorzystaniu systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw zgodnie z ust. 4, przedkładają Komisji roczne sprawozdania z takiego wykorzystania. W tym celu Komisja przekazuje państwom członkowskim i krajowym organom nadzoru rynku i organom ochrony danych wzór formularza zawierającego informacje na temat liczby decyzji podjętych przez właściwe organy sądowe lub wydający wiążące decyzje niezależny organ administracyjny w odniesieniu do wniosków o udzielenie zezwolenia zgodnie z ust. 3 oraz wyników ich rozpatrzenia.

7. Komisja publikuje roczne sprawozdania na temat wykorzystania systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw, oparte na zagregowanych danych w państwach członkowskich przekazanych w sprawozdaniach rocznych, o których mowa w ust. 6. Te sprawozdania roczne nie zawierają wrażliwych danych operacyjnych dotyczących powiązanych działań w zakresie ścigania przestępstw.

8. Niniejszy artykuł nie ma wpływu na zakazy mające zastosowanie w przypadku, gdy praktyka związana z AI narusza inne przepisy prawa Unii.

ROZDZIAŁ III
SYSTEMY AI WYSOKIEGO RYZYKA

Sekcja 1
Klasyfikacja systemów AI jako systemów AI wysokiego ryzyka

Artykuł 6

Zasady klasyfikacji systemów AI wysokiego ryzyka

1. Bez względu na to, czy system AI wprowadza się do obrotu lub oddaje do użytku niezależnie od produktów, o których mowa w lit. a) i b), taki system AI uznaje się za system wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

   a) system AI jest przeznaczony do stosowania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I lub ***system AI*** sam w sobie jest takim produktem;

   b) produkt, w którym ***zgodnie z lit. a)*** związanym z bezpieczeństwem elementem jest system AI, lub system AI sam w sobie jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I – ocenie zgodności przez stronę trzecią w związku z wprowadzeniem tego produktu do obrotu lub oddania go do użytku.

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

3. Na zasadzie odstępstwa od ust. 2 systemu AI nie uznaje się za system wysokiego ryzyka, jeżeli nie stwarza on znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych, w tym poprzez brak znaczącego wpływu na wynik procesu decyzyjnego. Ma to miejsce w przypadku, gdy spełniony jest co najmniej jeden z następujących warunków:

a) system AI jest przeznaczony do wykonywania wąskiego zadania proceduralnego;

b) system AI jest przeznaczony do poprawienia wyniku zakończonej uprzednio czynności wykonywanej przez człowieka;

c) system AI jest przeznaczony do wykrywania wzorców podejmowania decyzji lub odstępstw od wzorców podjętych uprzednio decyzji i nie ma na celu zastąpienia ani wywarcia wpływu na ukończoną uprzednio ocenę dokonaną przez człowieka – bez odpowiedniej weryfikacji przez człowieka; lub

d) system AI jest przeznaczony do wykonywania zadań przygotowawczych w kontekście oceny istotnej z punktu widzenia przypadków użycia wymienionych w załączniku III.

Niezależnie od akapitu pierwszego system AI, o którym mowa w załączniku III, zawsze uznaje się za system wysokiego ryzyka, w przypadku gdy system ten dokonuje profilowania osób fizycznych.

4. Dostawca, który uważa, że system AI, o którym mowa w załączniku III, nie jest system wysokiego ryzyka, przed wprowadzeniem tego systemu do obrotu lub oddaniem go do użytku dokumentuje swoją ocenę. Taki dostawca podlega obowiązkowi rejestracji określonemu w art. 49 ust. 2. Na żądanie właściwych organów krajowych dostawca przedstawia dokumentację tej oceny.

5. Po konsultacji z Europejską Radą ds. Sztucznej Inteligencji (zwaną dalej „Radą ds. AI"), nie później jednak niż... [18 miesięcy od daty wejścia w życie niniejszego rozporządzenia] Komisja przedstawi wytyczne określające praktyczne wdrożenie niniejszego artykułu zgodnie z art. 96 wraz z kompleksowym wykazem praktycznych przykładów przypadków użycia systemów AI, które są systemami wysokiego ryzyka i które nie są systemami wysokiego ryzyka.

6. Komisja przyjmuje zgodnie z art. 97 akty delegowane dotyczące zmiany warunków ustanowionych w ust. 3 akapit pierwszy niniejszego artykułu.

Komisja może przyjmować akty delegowane zgodnie z art. 97 w celu dodania nowych warunków do warunków ustanowionych w ust. 3 akapit pierwszy lub w celu ich zmiany wyłącznie w przypadku, gdy istnieją konkretne i wiarygodne dowody na istnienie systemów AI, które wchodzą w zakres stosowania załącznika III, ale nie stwarzają znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych.

Komisja przyjmuje zgodnie z art 97 akty delegowane dotyczące usunięcia któregokolwiek z warunków ustanowionych w ust. 3 akapit pierwszy, w przypadku gdy istnieją konkretne i wiarygodne dowody na to, że jest to konieczne z punktu widzenia utrzymania poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych w Unii.

Żadna zmiana warunków ustanowionych w ust. 3 akapit pierwszy nie obniża ogólnego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych w Unii.

Przyjmując akty delegowane, Komisja zapewnia spójność z aktami delegowanymi przyjętymi zgodnie z art. 7 ust. 1 oraz uwzględnia rozwój rynku i technologii.

Artykuł 7

Zmiany w załączniku III

1. Komisja przyjmuje akty delegowane zgodnie z art. 97 w celu ***zmiany*** załącznika III poprzez dodanie systemów AI wysokiego ryzyka ***lub zmianę przypadków ich użycia***, w przypadku gdy spełnione są oba poniższe warunki:

   a) systemy AI są przeznaczone do stosowania w którymkolwiek z obszarów wymienionych w załączniku III;

b) systemy AI stwarzają ryzyko szkody dla ▌ zdrowia i bezpieczeństwa lub ryzyko niepożądanego wpływu na prawa podstawowe ***i ryzyko to jest*** równoważne ryzyku szkody lub niepożądanego wpływu, jakie stwarzają systemy AI wysokiego ryzyka wymienione już w załączniku III, lub jest od niego większe.

2. Przy ocenie warunku określonego w ust. 1 lit. b) Komisja uwzględnia następujące kryteria:

a) przeznaczenie systemu AI;

b) zakres, w jakim system AI jest wykorzystywany lub prawdopodobnie będzie wykorzystywany;

c) charakter i ilość danych przetwarzanych i wykorzystywanych przez system AI, w szczególności, czy przetwarzane są szczególne kategorie danych osobowych;

d) zakres, w jakim system AI działa autonomicznie oraz możliwość unieważnienia przez człowieka decyzji lub zaleceń, które mogą prowadzić do potencjalnej szkody;

e) zakres, w jakim wykorzystywanie systemu AI spowodowało już szkodę dla ▌ zdrowia i bezpieczeństwa lub ***miało*** niepożądany wpływ na ▌ prawa podstawowe lub wzbudziło istotne obawy co do ***prawdopodobieństwa*** takiej szkody lub niepożądanego wpływu, czego potwierdzeniem są ***np.*** zgłoszenia lub udokumentowane zarzuty przedłożone właściwym organom krajowym, ***lub, w stosownych przypadkach, inne zgłoszenia***;

f) potencjalny zakres takiej szkody lub takiego niepożądanego wpływu, w szczególności pod względem ich nasilenia i możliwości oddziaływania na wiele osób ***lub nieproporcjonalnego oddziaływania na określoną grupę osób;***

g) zakres, w jakim osoby potencjalnie poszkodowane lub doświadczające niepożądanego wpływu są zależne od wyniku działania systemu AI, w szczególności ze względu na fakt, że z przyczyn praktycznych lub prawnych nie jest racjonalnie możliwa rezygnacja z objęcia tym wynikiem;

h) zakres, w jakim ***występuje nierówny układ sił lub osoby*** potencjalnie poszkodowane lub doświadczające niepożądanego wpływu znajdują się w słabszym położeniu względem podmiotu stosującego system AI, w szczególności z powodu ***statusu, władzy***, wiedzy, sytuacji gospodarczej lub społecznej lub wieku;

i) zakres, w jakim wynik uzyskany ***przy wykorzystaniu*** systemu AI jest łatwy ***do skorygowania lub*** odwracalny, ***przy uwzględnieniu dostępnych rozwiązań technicznych umożliwiających jego skorygowanie lub odwrócenie***, przy czym za łatwe ***do skorygowania lub*** odwracalne nie uznaje się wyników działania systemu mających ***niepożądany*** wpływ na ▌ zdrowie, bezpieczeństwo ***lub prawa podstawowe***;

j) zakres i prawdopodobieństwo korzyści płynących z wdrażania systemu AI dla osób fizycznych, grup lub ogółu społeczeństwa, w tym możliwość poprawy bezpieczeństwa produktów;

k) zakres, w jakim obowiązujące prawo Unii przewiduje:

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

(ii) skuteczne środki zapobiegania tym zagrożeniom lub ich znacznego minimalizowania.

3. Komisja przyjmuje zgodnie z art. 97 akty delegowane w celu zmiany wykazu zawartego w załączniku III poprzez usunięcie systemów AI wysokiego ryzyka, jeżeli spełnione są oba poniższe warunki:

a) dany system AI wysokiego ryzyka nie stwarza już jakichkolwiek istotnych zagrożeń dla praw podstawowych, zdrowia lub bezpieczeństwa, biorąc pod uwagę kryteria wymienione w ust. 2;

b) usunięcie systemu z wykazu nie obniża ogólnego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych przewidzianego w prawie Unii.

Sekcja 2

Wymogi dotyczące systemów AI wysokiego ryzyka

Artykuł 8

Zgodność z wymogami

1. Systemy AI wysokiego ryzyka muszą spełniać wymogi ustanowione w niniejszej sekcji, ***przy uwzględnieniu ich przeznaczenia oraz powszechnie uznanego stanu wiedzy technicznej w dziedzinie sztucznej inteligencji oraz powiązanych technologii. Przy zapewnianiu zgodności z tymi wymogami uwzględnia się system zarządzania ryzykiem, o którym mowa w art. 9.***

2. ***W przypadku gdy produkt zawiera system AI, do którego mają zastosowanie wymogi niniejszego rozporządzenia oraz wymogi unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A, dostawcy są odpowiedzialni za zapewnienie pełnej zgodności ich produktu ze wszystkimi mającymi zastosowanie wymogami obowiązującymi na podstawie mającego zastosowanie unijnego prawodawstwa harmonizacyjnego. Przy zapewnianiu zgodności systemów AI wysokiego ryzyka, o których mowa w ust. 1, z wymogami określonymi w niniejszej sekcji oraz w celu zapewnienia spójności, unikania powielania i zminimalizowania dodatkowych obciążeń, dostawcy mogą wybrać, w stosownych przypadkach, integrację niezbędnych procesów testowania i sprawozdawczości, informacji i dokumentacji, które dostarczają w odniesieniu do swojego produktu, z istniejącą już dokumentacją i procedurami wymaganymi na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A.***

Artykuł 9

System zarządzania ryzykiem

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

2. System zarządzania ryzykiem ***należy rozumieć*** jako ciągły, iteracyjny proces, ***planowany i*** realizowany przez cały cykl życia systemu AI wysokiego ryzyka, wymagający regularnego systematycznego ***przeglądu i*** aktualizacji. Obejmuje on następujące etapy:

   a) identyfikację i analizę znanego i dającego się ***racjonalnie*** przewidzieć ryzyka, ***jakie dany system AI wysokiego ryzyka może stwarzać dla zdrowia, bezpieczeństwa lub praw podstawowych, kiedy*** system ten ***będzie stosowany zgodnie ze swoim przeznaczeniem;***

   b) oszacowanie i ocenę ryzyka, jakie może wystąpić podczas wykorzystywania systemu AI 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. 72;

   d) przyjęcie ***odpowiednich i ukierunkowanych*** środków zarządzania ryzykiem ***zaprojektowanych w celu przeciwdziałania ryzyku zidentyfikowanemu zgodnie z lit. a).***

3. ***Rodzaje ryzyka, o których mowa w niniejszym*** artykule, ***oznaczają tylko takie jego rodzaje, które można w rozsądny sposób ograniczyć lub wyeliminować poprzez opracowanie lub zaprojektowanie systemu AI wysokiego ryzyka lub poprzez zapewnienie odpowiednich informacji technicznych.***

4. 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 niniejszej sekcji, ***z myślą o skuteczniejszym minimalizowaniu ryzyka przy jednoczesnym osiągnięciu odpowiedniej równowagi we wdrażaniu środków służących spełnieniu przedmiotowych wymogów.***

5. Środki zarządzania ryzykiem, o których mowa w ust. 2 lit. d), muszą być takie, aby ***odnośne*** ryzyko szczątkowe związane z każdym zagrożeniem, jak również ogólne ryzyko szczątkowe systemów AI wysokiego ryzyka, oceniano ***jako dopuszczalne.***

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

   a) eliminację lub ograniczenie – w zakresie, w jakim jest to ***technicznie wykonalne*** – ryzyka ***zidentyfikowanego i ocenionego zgodnie z ust. 2*** poprzez odpowiedni projekt ***systemu AI wysokiego ryzyka*** i proces jego opracowywania;

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

   c) dostarczenie informacji ***wymaganych*** zgodnie z art. 13 oraz, w stosownych przypadkach, przeszkolenie ***podmiotów stosujących AI.*** ▌

W celu eliminowania lub ograniczania ryzyka związanego z wykorzystaniem systemu AI wysokiego ryzyka należytą uwagę zwraca się na wiedzę techniczną, doświadczenie, wykształcenie i szkolenia, jakich oczekuje się od ***podmiotu stosującego AI***, oraz ***zakładany kontekst***, w którym ma być stosowany system.

6. Systemy AI wysokiego ryzyka testuje się w celu określenia najodpowiedniejszych i ***ukierunkowanych*** środków zarządzania ryzykiem. Testy zapewniają, by systemy AI wysokiego ryzyka działały zgodnie z ich przeznaczeniem oraz były zgodne z wymogami określonymi w niniejszej sekcji.

7. Procedury testowe ***mogą obejmować testy w warunkach rzeczywistych zgodnie z art. 60.***

8. Testy systemów AI wysokiego ryzyka przeprowadza się, w stosownych przypadkach, w dowolnym momencie procesu opracowywania systemu, a w każdym przypadku przed wprowadzeniem go do obrotu lub oddaniem do użytku. Testy przeprowadza się w odniesieniu do ***uprzednio*** określonych wskaźników i progów probabilistycznych, stosownych do przeznaczenia systemu AI wysokiego ryzyka.

9. Przy wdrażaniu systemu zarządzania ryzykiem przewidzianego w ust. 1–7 ***dostawcy zwracają*** uwagę, ***na ile prawdopodobne jest, że w świetle swojego przeznaczenia*** dany system AI wysokiego ryzyka będzie ***niekorzystnie wpływał na osoby poniżej 18 roku życia oraz, w stosownych przypadkach, inne grupy osób szczególnie wrażliwych.***

10. W odniesieniu do ***dostawców systemów AI wysokiego ryzyka, którzy podlegają wymogom dotyczącym wewnętrznych procesów zarządzania ryzykiem na podstawie innego odpowiedniego prawa Unii***, aspekty przewidziane w ust. 1–9 ***mogą*** być częścią procedur zarządzania ryzykiem ustanowionych ▌ zgodnie ***z tym prawem lub łączyć się z*** tymi procedurami.

Artykuł 10

Dane i zarządzanie danymi

1. Systemy AI 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, ***gdy tylko takie zbiory danych są wykorzystywane.***

2. Zbiory danych treningowych, walidacyjnych i testowych podlegają praktykom w zakresie zarządzania danymi ***stosownym do przeznaczenia danego systemu AI wysokiego ryzyka***. Praktyki te dotyczą w szczególności:

   a) odpowiednich decyzji projektowych;

   b) procesów gromadzenia danych i pochodzenia danych oraz, w przypadku danych osobowych, pierwotnego celu gromadzenia danych;

   ▌

c) odpowiednich operacji przetwarzania na potrzeby przygotowania danych, takich jak dodawanie komentarzy, etykietowanie, czyszczenie, ***aktualizacja***, wzbogacanie i agregacja;

d) sformułowania ▌ założeń, w szczególności w odniesieniu do informacji, do których pomiaru i reprezentowania mają służyć dane;

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

f) badania pod kątem ewentualnej stronniczości, ***która może mieć wpływ na zdrowie i bezpieczeństwo osób, negatywnie wpływać na prawa podstawowe lub prowadzić do dyskryminacji zakazanej na mocy prawa Unii, zwłaszcza w przypadku gdy dane wyjściowe wpływają na dane wejściowe wykorzystywane na potrzeby przyszłych operacji;***

g) odpowiednich środków służących wykrywaniu ewentualnej stronniczości określonej zgodnie z lit. f) oraz zapobieganiu jej i jej ograniczaniu ;

h) określenia ***istotnych*** luk w danych lub braków w danych, ***które uniemożliwiają stosowanie się do niniejszego rozporządzenia***, oraz tego, w jaki sposób można zaradzić tym lukom i brakom.

3. ***Zbiory danych*** treningowych, walidacyjnych i testowych muszą być adekwatne, ***wystarczająco*** reprezentatywne ***oraz w jak największym stopniu*** wolne od błędów i kompletne z ***punktu widzenia przeznaczenia***. Muszą się one charakteryzować odpowiednimi właściwościami statystycznymi, w tym, w stosownych przypadkach, w odniesieniu do osób lub grup osób, ***wobec których*** ma być stosowany system AI wysokiego ryzyka. Te kryteria zbiorów danych mogą zostać spełnione na poziomie pojedynczych zbiorów danych lub na poziomie ich kombinacji.

4. ***Zbiory danych*** muszą uwzględniać, w zakresie wymaganym z uwagi na ich przeznaczenie, cechy lub elementy, które są specyficzne dla określonego otoczenia geograficznego, ***kontekstualnego***, behawioralnego lub funkcjonalnego, w którym ma być stosowany system AI wysokiego ryzyka.

5. W zakresie, w jakim jest to ściśle niezbędne do celów zapewnienia ***zgodnie z ust. 2 lit. f) i g) niniejszego artykułu*** ▌ wykrywania i korygowania stronniczości systemów AI wysokiego ryzyka, dostawcy takich systemów mogą ***wyjątkowo*** przetwarzać szczególne kategorie danych osobowych, pod warunkiem stosowania odpowiednich zabezpieczeń gwarantujących ochronę podstawowych praw i wolności osób fizycznych. ***Oprócz przepisów określonych w rozporządzeniu (UE) 2016/679, dyrektywie (UE) 2016/680 i rozporządzeniu (UE) 2018/1725, aby takie przetwarzanie mogło się odbyć, obowiązują wszystkie następujące warunki:***

   a) nie jest możliwe skuteczne wykrywanie i korygowanie stronniczości poprzez przetwarzanie innych danych, w tym danych syntetycznych lub zanonimizowanych;

b) szczególne kategorie danych osobowych podlegają ograniczeniom technicznym dotyczącym ponownego wykorzystywania danych osobowych oraz najnowocześniejszym środkom bezpieczeństwa i ochrony prywatności, w tym pseudonimizacji;

c) szczególne kategorie danych osobowych podlegają środkom zapewniającym, by przetwarzane dane osobowe były zabezpieczone, chronione, podlegały odpowiednim środkom ochronnym, w tym ścisłym kontrolom i dokumentowaniu dostępu, aby uniknąć nadużyć i zapewnić, by dostęp do tych danych miały wyłącznie osoby upoważnione objęte odpowiednimi obowiązkami w zakresie poufności;

d) dane osobowe należące do tych szczególnych kategorii danych osobowych nie są przesyłane, przekazywane ani w inny sposób udostępniane innym podmiotom;

e) dane osobowe należące do tych szczególnych kategorii danych osobowych usuwa się po skorygowaniu stronniczości lub po upływie okresu przechowywania danych osobowych, w zależności od tego, który z tych terminów przypadnie wcześniej;

f) rejestry czynności przetwarzania na podstawie rozporządzeń (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywy (UE) 2016/680 zawierają uzasadnienie, dlaczego przetwarzanie szczególnych kategorii danych osobowych było absolutnie niezbędne do wykrycia i skorygowania stronniczości oraz dlaczego cel ten nie mógł zostać osiągnięty w wyniku przetwarzania innych danych.

6. ▌ W przypadkach opracowywania systemów AI wysokiego ryzyka ***niewykorzystujących*** technik obejmujących trenowanie modeli AI ***ust. 2–5 stosuje się jedynie do zbiorów danych testowych***.

Artykuł 11

Dokumentacja techniczna

1. Dokumentację techniczną dla systemu AI 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 AI wysokiego ryzyka spełnia wymogi określone w niniejszej sekcji, oraz aby dostarczyć właściwym organom krajowym i jednostkom notyfikowanym informacji – ***w jasnej i kompleksowej formie*** – niezbędnych do oceny zgodności systemu AI z tymi wymogami. Zawiera ona co najmniej elementy określone w załączniku IV. ***MŚP, w tym przedsiębiorstwa typu start-up, mogą podawać elementy dokumentacji technicznej określone w załączniku IV w formie uproszczonej. W tym celu Komisja ustanawia uproszczony formularz dokumentacji technicznej ukierunkowany na potrzeby małych przedsiębiorstw i mikroprzedsiębiorstw. W przypadku gdy MŚP, w tym przedsiębiorstwa typu start-up, zdecydują się na podawanie informacji wymaganych w załączniku IV w sposób uproszczony, korzystają z formularza, o którym mowa w niniejszym ustępie. Jednostki notyfikowane akceptują ten formularz do celów oceny zgodności.***

2. W przypadku gdy wprowadzany do obrotu lub oddawany do użytku jest system AI wysokiego ryzyka związany z produktem objętym zakresem stosowania unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A, sporządza się jedną dokumentację techniczną zawierającą wszystkie informacje określone w ***ust. 1***, jak również informacje wymagane na podstawie tych aktów prawnych.

3. Komisja przyjmuje akty delegowane zgodnie z art. 97 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 niniejszej sekcji.

Artykuł 12

Rejestrowanie zdarzeń

1. Systemy AI wysokiego ryzyka ***muszą dysponować technicznymi możliwościami*** automatycznego rejestrowania zdarzeń („rejestry zdarzeń”) w ***trakcie całego cyklu ich życia***.

2. ***W celu zapewnienia***, by poziom identyfikowalności funkcjonowania systemu AI wysokiego ryzyka ▌był odpowiedni do przeznaczenia tego systemu, ***funkcja rejestracji zdarzeń zapewnia rejestrowanie zdarzeń istotnych dla:***

   a) identyfikacji sytuacji, które mogą skutkować tym, że system AI wysokiego ryzyka będzie stwarzał ryzyko w rozumieniu art. 79 ust. 1, lub które mogą prowadzić do wystąpienia istotnej zmiany;

   b) ułatwiania monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 72; oraz

   c) monitorowania działania systemów AI wysokiego ryzyka, o których mowa w art. 26 ust. 6.

▌

3. W przypadku systemów AI wysokiego ryzyka, o których mowa w załączniku 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 ***podmiotom stosującym AI***

1. Systemy AI wysokiego ryzyka projektuje się i opracowuje w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą ***podmiotom stosującym AI*** interpretację wyników działania systemu i ich właściwe wykorzystanie. Zapewnia się odpowiedni rodzaj i stopień przejrzystości w celu osiągnięcia zgodności z odpowiednimi obowiązkami ***dostawcy i podmiotu stosującego AI***, określonymi w sekcji 3.

2. Do systemów AI 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 podmiotów stosujących AI.

3. ***Instrukcja obsługi zawiera co najmniej następujące informacje:***

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

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

(i) jego przeznaczenie;

(ii) poziom dokładności, ***wraz z odnośnymi wskaźnikami***, poziom solidności i cyberbezpieczeństwa, o których mowa w art. 15, względem których przetestowano system AI wysokiego ryzyka i dokonano jego walidacji oraz których to poziomów można oczekiwać, a także wszelkie znane i dające się przewidzieć okoliczności, które mogą mieć wpływ na te oczekiwane poziomy dokładności, solidności i cyberbezpieczeństwa;

(iii) wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu AI wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, mogące powodować ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych, ***o którym to ryzyku mowa w art. 9 ust. 2;***

(iv) w stosownych przypadkach, możliwości techniczne i właściwości systemu AI wysokiego ryzyka w ***zakresie podawania informacji istotnych dla wyjaśnienia jego wyników;***

(v) ***w stosownych przypadkach***, działanie systemu w ***odniesieniu do określonych*** osób lub grup osób, względem których ma on być stosowany;

(vi) w stosownych przypadkach, specyfikacje dotyczące danych wejściowych lub wszelkie inne istotne informacje dotyczące wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, uwzględniając przeznaczenie systemu AI wysokiego ryzyka;

(vii) w stosownych przypadkach, informacje umożliwiające podmiotom stosującym AI interpretację wyników systemu AI wysokiego ryzyka i odpowiednie wykorzystanie tych wyników;

c) ewentualne zmiany w systemie AI 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 ***podmiotom stosującym AI*** interpretacji wyników działania systemów AI wysokiego ryzyka;

e) ***potrzebne zasoby obliczeniowe i sprzętowe***, przewidywany cykl życia systemu AI wysokiego ryzyka oraz wszelkie niezbędne środki w zakresie konserwacji i utrzymania, ***w tym częstotliwość*** ich stosowania, mające na celu zapewnienie właściwego funkcjonowania tego systemu AI, w tym dotyczące aktualizacji oprogramowania;

f) w stosownych przypadkach – opis mechanizmów zawartych w systemie AI wysokiego ryzyka, ***które umożliwiają*** podmiotom stosującym AI ***prawidłowe gromadzenie, przechowywanie i interpretowanie rejestrów zdarzeń, zgodnie z art. 12.***

Artykuł 14

Nadzór ze strony człowieka

1. Systemy AI wysokiego ryzyka projektuje się i opracowuje się w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie wykorzystywania systemu AI 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 AI 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 niniejszej sekcji.

3. ***Środki w zakresie*** nadzoru ***są współmierne do ryzyka, poziomu autonomii i kontekstu stosowania danego systemu AI*** wysokiego ryzyka, a nadzór zapewnia się za pomocą co najmniej jednego z następujących ***rodzajów*** środków:

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

   b) ***środków*** określonych przez dostawcę przed wprowadzeniem systemu AI wysokiego ryzyka do obrotu lub oddaniem go do użytku i które to środki nadają się do wdrożenia przez podmiot stosujący AI.

4. ***Do celów wykonania ust. 1, 2 i 3 system AI wysokiego ryzyka udostępnia się użytkownikowi w taki sposób, aby umożliwić osobom fizycznym,*** którym powierzono sprawowanie nadzoru ze strony człowieka, odpowiednio i ***proporcjonalnie*** do następujących okoliczności:

a) ***należyte*** zrozumienie ***odpowiednich*** możliwości i ograniczeń systemu AI wysokiego ryzyka oraz należyte monitorowanie jego działania, również ***z myślą o wykrywaniu*** anomalii, nieprawidłowego funkcjonowania i nieoczekiwanych wyników działania ***oraz zaradzeniu*** im w przypadku ich wystąpienia ▌;

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

c) ▌ prawidłową interpretację wyniku działania systemu AI wysokiego ryzyka, biorąc pod uwagę ***na przykład*** dostępne narzędzia i metody interpretacji;

d) ▌ podjęcie decyzji, w każdej konkretnej sytuacji, o niekorzystaniu z systemu AI wysokiego ryzyka lub w inny sposób zignorowanie, unieważnienie lub odwrócenie wyniku działania systemu AI wysokiego ryzyka;

e) ▌ ingerowanie w działanie systemu AI wysokiego ryzyka lub przerwanie działania systemu za pomocą przycisku „***stop***" lub podobnej procedury, ***która pozwala na zatrzymanie systemu w stanie bezpiecznym.***

5. W przypadku systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 1 lit. a), środki, o których mowa w ust. 3 niniejszego artykułu, muszą ponadto zapewniać, aby ***podmiot stosujący AI*** nie podejmował żadnego działania ani decyzji na podstawie identyfikacji będącej wynikiem działania systemu, jeżeli identyfikacji tej nie zweryfikowały ani nie potwierdziły jej ***odrębnie*** co najmniej dwie osoby fizyczne ***mające wymagane kompetencje, przeszkolenie i uprawnienia***.

Wymóg odrębnej weryfikacji przez co najmniej dwie osoby fizyczne nie ma zastosowania do systemów AI wysokiego ryzyka wykorzystywanych do celów ścigania przestępstw, migracji, kontroli granicznej lub azylu, w przypadkach gdy prawo Unii lub prawo krajowe uznaje stosowanie tego wymogu za nieproporcjonalne.

Artykuł 15

Dokładność, solidność i cyberbezpieczeństwo

1. Systemy AI wysokiego ryzyka projektuje się i opracowuje się w taki sposób, aby osiągały ▌ odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz by działały konsekwentnie pod tymi względami w całym cyklu życia.

2. ***Aby odnieść się do technicznych aspektów pomiaru odpowiednich poziomów dokładności i solidności, o których mowa w ust. 1 oraz wszelkich innych istotnych pomiarów funkcjonowania, Komisja we współpracy z odpowiednimi zainteresowanymi stronami i organizacjami, takimi jak organy metrologiczne i organy ds. analizy porównawczej, zachęca w stosownych przypadkach do opracowywania wskaźników referencyjnych i metod pomiarowych.***

3. Poziomy dokładności i odpowiednie wskaźniki dokładności systemów AI wysokiego ryzyka deklaruje się w dołączonych do nich instrukcjach obsługi.

4. Systemy AI wysokiego ryzyka muszą być ***możliwie jak*** najodporniejsze 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. ***W tym celu podejmuje się środki techniczne i organizacyjne.***

   Solidność systemów AI 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 AI wysokiego ryzyka, które po wprowadzeniu na rynek lub oddaniu do użytku nadal się uczą, opracowuje się w taki sposób, aby w ***możliwie największym stopniu wyeliminować lub ograniczyć ryzyko potencjalnie stronniczych*** wyników działania wpływających na dane wejściowe w przyszłych operacjach („sprzężenie zwrotne") oraz aby zapewnić, by wszelkie tego typu sprzężenie zwrotne zostało odpowiednio uwzględnione dzięki użyciu odpowiednich środków zaradczych.

5. Systemy AI wysokiego ryzyka muszą być odporne na próby nieupoważnionych osób trzecich mające na celu zmianę ich zastosowania, ***wyników*** lub skuteczności działania poprzez wykorzystanie słabych punktów systemu.

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

Rozwiązania techniczne mające na celu eliminowanie słabych punktów charakterystycznych dla AI obejmują, w stosownych przypadkach, środki służące zapobieganiu atakom mającym na celu manipulowanie zbiorem danych treningowych („zatruwanie danych"), ***lub manipulowanie wstępnie wytrenowanymi modelami stosowanymi przy trenowaniu („zatruwanie modelu")***, wprowadzaniu danym wejściowym, które mają na celu spowodowanie błędu w modelu AI („ przykłady kontradyktoryjne" ***lub „omijanie modelu"***), ***atakom na poufność*** lub wadom modelu, a także środki w zakresie ***wykrywania tych zagrożeń, reagowania na nie, ich rozwiązywania*** i kontroli.

Sekcja 3

Obowiązki dostawców i podmiotów stosujących systemy AI wysokiego ryzyka oraz innych osób

Artykuł 16

Obowiązki dostawców systemów AI wysokiego ryzyka

Dostawcy systemów AI wysokiego ryzyka:

a) zapewniają zgodność swoich systemów AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2;

b) ***podają w systemie AI wysokiego ryzyka lub – przypadku gdy nie jest to możliwe – na jego opakowaniu lub w dokumentacji towarzyszącej, stosownie do przypadku, swoją nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy i adres, pod którym można się z nimi skontaktować;***

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

d) ***prowadzą*** dokumentację techniczną, o ***której mowa w art. 18***;

e) przechowują rejestry zdarzeń generowane automatycznie przez ich systemy AI wysokiego ryzyka, ***jak określono w art. 19***, gdy rejestry takie znajdują się pod ich kontrolą;

f) zapewniają, aby przed wprowadzeniem go do obrotu lub oddaniem do użytku system AI wysokiego ryzyka poddano odpowiedniej procedurze oceny zgodności, o ***której mowa w art. 43;***

g) sporządzają deklarację zgodności UE zgodnie z art. 47;

h) umieszczają, zgodnie z art. 48, oznakowanie CE w systemie AI wysokiego ryzyka lub – w przypadku gdy nie jest to możliwe – na jego opakowaniu lub w dokumentacji towarzyszącej, na potwierdzenie zgodności z niniejszym rozporządzeniem;

i) wypełniają obowiązki rejestracyjne, o których mowa w art. 49 ust. ***1***;

j) podejmują niezbędne działania naprawcze ***i przekazują informacje zgodnie z art. 20***;

k) wykazują, na ***uzasadnione*** żądanie właściwego organu krajowego, zgodność systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2;

l) zapewniają, by system AI wysokiego ryzyka spełniał wymogi dostępności zgodnie z dyrektywami (UE) 2016/2102 i (UE) 2019/882.

Artykuł 17

System zarządzania jakością

1. Dostawcy systemów AI 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 na rzecz zgodności regulacyjnej, w tym zgodności z procedurami oceny zgodności i procedurami zarządzania zmianami w systemie AI wysokiego ryzyka;

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

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

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

e) specyfikacje techniczne, w tym normy, które należy zastosować, oraz w przypadkach gdy normy zharmonizowane nie są stosowane w pełni ***lub nie obejmują wszystkich odpowiednich wymogów określonych w sekcji 2,*** środki, które należy zastosować do zapewnienia, by system AI wysokiego ryzyka był zgodny z ***tymi*** wymogami ▌;

f) systemy i procedury zarządzania danymi, w tym dotyczące ***nabywania danych***, 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 AI wysokiego ryzyka i do celu 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. 72;

i) procedury związane ze zgłaszaniem ***poważnego incydentu*** zgodnie z art. 73;

j) prowadzenie komunikacji z właściwymi organami krajowymi, ***innymi właściwymi*** organami, w ***tym*** organami 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. ***W każdym przypadku dostawcy zapewniają odpowiednią rygorystyczność i poziom ochrony wymagane do zapewnienia zgodności ich systemów AI wysokiego ryzyka z niniejszym rozporządzeniem.***

3. Dostawcy systemów AI wysokiego ryzyka, którzy podlegają obowiązkom dotyczącym systemów zarządzania jakością lub równoważnym obowiązkom na podstawie odpowiednich unijnych przepisów sektorowych, mogą uwzględnić aspekty opisane w ust. 1 jako część systemów zarządzania jakością zgodnie z tym prawem.

4. W odniesieniu do dostawców będących instytucjami ***finansowymi***, ***które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych***, obowiązek ***wprowadzenia*** systemu zarządzania jakością, ***z wyjątkiem ust. 1 lit. g), h) oraz i)*** niniejszego artykułu, uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi zarządzania wewnętrznego, uzgodnień ***lub procedur*** zgodnie z ***odpowiednimi unijnymi przepisami dotyczącymi usług finansowych***. W tym celu uwzględnia się wszelkie normy zharmonizowane, o których mowa w art. 40.

Artykuł 18

Prowadzenie dokumentacji

1. ***Przez okres 10 lat od dnia wprowadzenia systemu AI wysokiego ryzyka 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. 47.

2. ***Każde państwo członkowskie określa warunki, na jakich dokumentacja, o której mowa w ust. 1, pozostaje do dyspozycji właściwych organów krajowych przez okres wskazany w tym ustępie w przypadkach, gdy dostawca lub jego upoważniony przedstawiciel mający siedzibę na terytorium danego państwa członkowskiego ogłoszą upadłość lub zaprzestaną działalności przed upływem tego okresu.***

3. Dostawcy będący instytucjami ***finansowymi***, które ***podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych***, prowadzą rejestry zdarzeń jako część dokumentacji ***prowadzonej na podstawie odpowiednich unijnych przepisów dotyczących usług finansowych***.

I

Artykuł 19

Automatycznie generowane rejestry zdarzeń

1. Dostawcy systemów AI wysokiego ryzyka przechowują generowane automatycznie przez ich systemy AI wysokiego ryzyka rejestry zdarzeń, ***o których mowa w art. 12 ust. 1,*** w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą. ***Bez uszczerbku dla mającego zastosowanie prawa Unii lub prawa krajowego*** rejestry te są przechowywane przez okres ▌ zgodny z przeznaczeniem systemu AI wysokiego ryzyka, ***wynoszący co najmniej 6 miesięcy, o ile w mającym zastosowanie*** prawie Unii lub prawie krajowym, ***w szczególności prawie Unii dotyczącym ochrony danych osobowych, nie przewidziano inaczej.***

2. Dostawcy będący instytucjami ***finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych***, zachowują rejestry zdarzeń generowane automatycznie przez ich systemy AI wysokiego ryzyka jako część dokumentacji ***prowadzonej*** na podstawie ***odpowiednich przepisów dotyczących usług finansowych***.

Artykuł 20

Działania naprawcze ***i obowiązek informacyjny***

1. Dostawcy systemów AI wysokiego ryzyka, którzy uznają lub mają powody, by uznać, że system AI 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, ***wyłączenia go*** lub wycofania z użytku. Informują oni o tym dystrybutorów danego systemu AI wysokiego ryzyka oraz, w stosownych przypadkach, odpowiednio ***podmioty stosujące AI***, upoważnionego przedstawiciela i importerów.

2. ***W przypadku gdy system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1 i ryzyko to stanie się znane dostawcy danego systemu, dostawca ten niezwłocznie wyjaśnia przyczyny tego ryzyka, w stosownych przypadkach we współpracy z podmiotem stosującym AI, oraz informuje organy nadzoru rynku państwa członkowskiego lub państw członkowskich, w których udostępnił dany system AI wysokiego ryzyka na rynku, oraz, w stosownych przypadkach, jednostkę notyfikowaną, która zgodnie z art. 44 wydała certyfikat dla danego systemu AI wysokiego ryzyka, w szczególności o charakterze danej niezgodności oraz o wszelkich podjętych działaniach naprawczych.***

Artykuł 21

Współpraca z właściwymi organami

1. Dostawcy systemów AI wysokiego ryzyka, na ***uzasadnione*** żądanie właściwego organu ▌, przekazują temu organowi ▌ wszelkie informacje i dokumenty niezbędne do wykazania zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2, w języku ***łatwo zrozumiałym dla danego organu w jednym z oficjalnych języków instytucji Unii wskazanym przez dane państwo członkowskie.***

2. ***Na uzasadnione żądanie właściwego organu krajowego dostawcy zapewniają również temu właściwemu organowi krajowemu, w stosownych przypadkach, dostęp do generowanych automatycznie przez system AI wysokiego ryzyka rejestrów zdarzeń, o których mowa w art. 12 ust. 1, w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą.***

3. Wszelkie informacje uzyskane zgodnie z niniejszym artykułem przez właściwy organ krajowy traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 78.

Artykuł 22

Upoważnieni przedstawiciele dostawców systemów AI wysokiego ryzyka

1. Przed udostępnieniem swoich systemów AI wysokiego ryzyka na rynku Unii ▌ dostawcy mający siedzibę w państwach trzecich wyznaczają – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego siedzibę w Unii.

2. Dostawca umożliwia swojemu upoważnionemu przedstawicielowi wykonywanie zadań powierzonych mu na mocy pełnomocnictwa udzielonego przez dostawcę.

3. Upoważniony przedstawiciel wykonuje zadania powierzone mu na mocy pełnomocnictwa udzielonego przez dostawcę. ***Na żądanie przekazuje on organom nadzoru rynku kopię pełnomocnictwa w jednym z oficjalnych języków instytucji Unii wskazanym przez właściwy organ krajowy. Do celów niniejszego rozporządzenia*** pełnomocnictwo uprawnia upoważnionego przedstawiciela do wykonywania następujących zadań:

a) sprawdzenie, czy zostały sporządzone deklaracja zgodności UE i dokumentacja techniczna, o której mowa w art. 11, oraz czy została przeprowadzona przez dostawcę odpowiednia procedura oceny zgodności;

b) przechowywanie ***do dyspozycji właściwych organów krajowych i krajowych organów lub jednostek, o których mowa w art. 74 ust. 10, przez okres 10 lat od wprowadzenia systemu AI wysokiego ryzyka do obrotu lub oddania go do użytku, danych kontaktowych dostawcy, który wyznaczył upoważnionego przedstawiciela, kopii deklaracji zgodności UE, dokumentacji technicznej oraz, w stosownych przypadkach, certyfikatu wydanego przez jednostkę notyfikowaną;***

c) przekazywanie właściwemu organowi krajowemu na jego uzasadniony wniosek wszelkich informacji i dokumentów, ***w tym określonych w lit. b) niniejszego ustępu***, niezbędnych do wykazania zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2, w tym zapewnienie temu organowi dostępu do generowanych automatycznie przez system AI wysokiego ryzyka rejestrów zdarzeń, o ***których mowa w art. 12 ust. 1***, w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod kontrolą dostawcy ▌;

d) współpraca z właściwymi ▌ organami – na uzasadniony wniosek – w zakresie wszelkich działań, które organy te podejmują w odniesieniu do danego systemu AI wysokiego ryzyka, ***w szczególności, aby zmniejszyć i złagodzić ryzyko, jakie stwarza ten system AI wysokiego ryzyka;***

e) ***w stosownych przypadkach wypełnianie obowiązków rejestracyjnych, o których mowa w art. 49 ust. 1, lub, jeżeli rejestracji dokonuje sam dostawca, dopilnowanie, by informacje, o których mowa w załączniku VIII*** sekcja A, ***były prawidłowe.***

Pełnomocnictwo daje upoważnionemu przedstawicielowi prawo do tego, aby właściwe organy mogły się zwracać do niego, obok albo zamiast do dostawcy, we wszystkich kwestiach dotyczących zapewnienia zgodności z niniejszym rozporządzeniem.

4. ***Upoważniony przedstawiciel wypowiada pełnomocnictwo, jeśli sądzi lub ma powody sądzić, że dostawca działa w sposób sprzeczny ze swoimi obowiązkami wynikającymi z niniejszego rozporządzenia. W takim przypadku niezwłocznie informuje on również o wypowiedzeniu pełnomocnictwa i jego przyczynach organ nadzoru rynku państwa członkowskiego, w którym znajduje się lub ma siedzibę, a także, w stosownych przypadkach, odpowiednią jednostkę notyfikowaną.***

Artykuł 23

Obowiązki importerów

1. Przed wprowadzeniem do obrotu systemu AI wysokiego ryzyka importerzy zapewniają ***zgodność tego systemu z niniejszym rozporządzeniem, sprawdzając, czy:***

a) dostawca tego systemu AI wysokiego ryzyka przeprowadził ***odpowiednią*** procedurę oceny zgodności, o ***której mowa w art. 43***;

b) dostawca sporządził dokumentację techniczną zgodnie z ***art. 11*** i załącznikiem IV;

c) system opatrzono wymaganym oznakowaniem ***CE*** oraz dołączono do niego ***deklarację zgodności UE*** oraz instrukcję obsługi;

d) dostawca wyznaczył upoważnionego przedstawiciela zgodnie z art. 22 ust. 1.

2. W przypadku gdy importer ***ma wystarczający*** powód, aby uważać, że system AI wysokiego ryzyka jest niezgodny z niniejszym rozporządzeniem ***lub został sfałszowany lub sfałszowana została jego dokumentacja***, nie wprowadza tego systemu do obrotu, dopóki nie zostanie zapewniona jego zgodność z przepisami niniejszego rozporządzenia. W przypadku gdy system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1, importer informuje o tym dostawcę systemu, ***upoważnionych przedstawicieli*** oraz organy nadzoru rynku.

3. Importerzy podają swoją nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy i adres, pod którym można się z nimi skontaktować w sprawie danego systemu AI wysokiego ryzyka, na opakowaniu tego systemu lub, w stosownych przypadkach, w towarzyszącej mu dokumentacji.

4. Importerzy zapewniają, aby w okresie, w którym ponoszą odpowiedzialność za system AI wysokiego ryzyka, warunki jego – stosownie do przypadku – przechowywania lub transportu nie zagrażały jego zgodności z wymogami określonymi w sekcji 2.

5. Importerzy, przez okres 10 lat od wprowadzenia systemu AI wysokiego ryzyka do obrotu lub oddania go do użytku, przechowują kopię certyfikatu wydanego przez jednostkę notyfikowaną, w stosownych przypadkach, kopię instrukcji obsługi oraz deklaracji zgodności UE.

6. Na uzasadniony wniosek właściwych organów krajowych importerzy przekazują im wszelkie niezbędne informacje i dokumentację, ***w tym te przechowywane zgodnie z ust. 5***, w celu wykazania zgodności systemu AI wysokiego ryzyka z wymogami określonymi w sekcji 2, w języku łatwo zrozumiałym dla ***tych organów***. ***W tym celu zapewniają*** również ***możliwość udostępnienia temu organowi dokumentacji technicznej.***

7. Importerzy współpracują z właściwymi organami krajowymi w zakresie wszelkich działań, które organy te podejmują w odniesieniu do wprowadzonego przez tych importerów do obrotu systemu AI wysokiego ryzyka, w szczególności aby ograniczyć lub złagodzić stwarzane przez ten system ryzyko.

Artykuł 24

Obowiązki dystrybutorów

1. Przed udostępnieniem na rynku systemu AI wysokiego ryzyka dystrybutorzy upewniają się, że został on opatrzony wymaganym oznakowaniem zgodności CE, że załączono do niego ***kopię deklaracji zgodności UE*** i instrukcję obsługi oraz że dostawca oraz – w stosownych przypadkach – importer systemu wywiązali się ze ***swoich*** odpowiednich obowiązków ustanowionych w ***art. 16 lit. b) i c) oraz w art. 23 ust. 3.***

2. W przypadku gdy dystrybutor – ***na podstawie dostępnych mu informacji*** – uważa lub ma powód, aby uważać, że system AI wysokiego ryzyka nie jest zgodny z wymogami ustanowionymi w sekcji 2 niniejszego tytułu, nie udostępnia na rynku tego systemu AI wysokiego ryzyka, dopóki nie zostanie zapewniona zgodność systemu z tymi wymogami. Ponadto jeżeli system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1, dystrybutor informuje o tym stosownie do przypadku dostawcę lub importera systemu.

3. Dystrybutorzy zapewniają, aby w okresie, w którym ponoszą odpowiedzialność za system AI wysokiego ryzyka, warunki jego przechowywania lub transportu – stosownie do przypadku – nie zagrażały zgodności systemu z wymogami ustanowionymi w sekcji 2.

4. Dystrybutor, który uważa lub ma powód, aby – ***na podstawie dostępnych mu informacji*** – uważać, że system AI wysokiego ryzyka udostępniony przez niego na rynku jest niezgodny z wymogami ustanowionymi w sekcji 2, 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. W przypadku gdy system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1, dystrybutor niezwłocznie informuje o tym fakcie ***dostawcę lub importera systemu oraz*** 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 AI wysokiego ryzyka*** przekazują temu organowi wszelkie informacje i dokumentację ***dotyczące ich działań zgodnie z ust. 1–4***, niezbędne do wykazania zgodności tego systemu z wymogami określonymi w sekcji 2. ▌

6. Dystrybutorzy współpracują z właściwymi organami krajowymi w zakresie wszelkich działań, które organy te podejmują w odniesieniu do udostępnionego na rynku przez tych dystrybutorów systemu AI wysokiego ryzyka, w szczególności aby ograniczyć lub złagodzić stwarzane przez ten system ryzyko.

Artykuł 25

Odpowiedzialność w całym łańcuchu wartości AI

1. Do celów niniejszego rozporządzenia za dostawcę ***systemu AI wysokiego ryzyka*** uznaje się i obejmuje obowiązkami dostawcy na podstawie art. 16 każdego dystrybutora, importera, ***podmiot stosujący AI*** lub inną stronę trzecią w dowolnym z poniższych przypadków:

   a) ***umieszczają oni swoją nazwę lub znak towarowy w systemie AI wysokiego ryzyka, który został już wprowadzony*** do obrotu lub oddany do użytku, ***bez uszczerbku dla ustaleń umownych przewidujących, że podział zawartych w nich obowiązków następuje w inny sposób;***

   b) we wprowadzonym już do obrotu lub oddanym do użytku systemie AI wysokiego ryzyka ***dokonują oni istotnej zmiany w taki sposób, że pozostaje on systemem AI wysokiego ryzyka zgodnie z art. 6***;

c) przeznaczenie systemu AI, w tym systemu AI ogólnego przeznaczenia, który nie został sklasyfikowany jako system AI wysokiego ryzyka i który został już wprowadzony do obrotu lub oddany do użytku, zmieniają oni w taki sposób, że system AI staje się systemem AI wysokiego ryzyka zgodnie z art. 6.

▌

2. W przypadku zaistnienia okoliczności, o których mowa w ust. 1, dostawcy, który pierwotnie ten system AI ▌ wprowadził do obrotu lub oddał do użytku, nie uznaje się już do celów niniejszego rozporządzenia za dostawcę ***tego konkretnego systemu AI***. ***Ten pierwotny dostawca ściśle współpracuje z nowymi dostawcami i udostępnia niezbędne informacje oraz udziela racjonalnie oczekiwanego dostępu technicznego i innego wsparcia niezbędnych do wypełnienia obowiązków określonych w niniejszym rozporządzeniu, w szczególności w odniesieniu do spełniania przez systemy AI wysokiego ryzyka kryteriów oceny zgodności. Niniejszy ustęp nie ma zastosowania w przypadkach, gdy pierwotny dostawca wyraźnie określił, że jego system AI nie może zostać przekształcony w system AI wysokiego ryzyka, a zatem nie dotyczy go obowiązek przekazania dokumentacji.***

3. ***W przypadku systemów AI wysokiego ryzyka, które stanowią związane z bezpieczeństwem elementy produktów*** objętych zakresem unijnego prawodawstwa harmonizacyjnego ***wymienionego w załączniku I sekcja A, producenta tych produktów uznaje się za dostawcę systemu AI wysokiego ryzyka i podlega on obowiązkom na podstawie w art. 16 w którymkolwiek z poniższych przypadków:***

a) system AI wysokiego ryzyka jest wprowadzany do obrotu wraz z produktem pod nazwą lub znakiem towarowym producenta produktu;

b) system AI wysokiego ryzyka jest oddawany do użytku pod nazwą lub znakiem towarowym producenta produktu po wprowadzeniu produktu do obrotu.

4. ***Dostawca systemu AI wysokiego ryzyka i osoba trzecia dostarczająca system AI, narzędzia, usługi, komponenty lub procesy, które są wykorzystywane w systemie AI wysokiego ryzyka lub z nim zintegrowane, zapewniają, w drodze pisemnej umowy, informacje, zdolności, dostęp techniczny i innego rodzaju pomoc opartą na powszechnie uznanym stanie wiedzy technicznej wymagane, aby umożliwić dostawcy systemu AI wysokiego ryzyka pełne wypełnienie obowiązków określonych w niniejszym rozporządzeniu. Niniejszy ustęp nie ma zastosowania do osób trzecich udostępniających publicznie na podstawie bezpłatnej i otwartej licencji narzędzia, usługi, procesy lub komponenty inne niż modele AI ogólnego przeznaczenia.***

Urząd ds. AI może opracować i zalecić wzory dobrowolnych postanowień umownych dla umów zawieranych między dostawcami systemów AI wysokiego ryzyka a osobami trzecimi dostarczającymi narzędzia, usługi, komponenty lub procesy, które są wykorzystywane na potrzeby systemów AI wysokiego ryzyka lub zintegrowane z tymi systemami. Przy opracowywaniu wzorów dobrowolnych postanowień umownych, Urząd ds. AI powinien też brać pod uwagę ewentualne wymogi umowne mające zastosowanie w określonych sektorach lub przypadkach biznesowych. Wzory dobrowolnych postanowień umownych są publikowane i udostępniane bezpłatnie w łatwym w użyciu formacie elektronicznym.

5. ***Ust. 2 i 3 pozostają bez uszczerbku dla konieczności przestrzegania i ochrony praw własności intelektualnej, poufnych informacji handlowych i tajemnic przedsiębiorstwa zgodnie z prawem Unii i prawem krajowym.***

Artykuł 26

Obowiązki ***podmiotów stosujących*** *systemy AI wysokiego ryzyka*

1. ***Podmioty stosujące*** systemy AI wysokiego ryzyka ***podejmują – na podstawie ust. 3 i 6 – odpowiednie środki techniczne i organizacyjne, aby zapewnić, że*** użytkują takie systemy zgodnie z dołączoną do nich instrukcją obsługi.

2. ***Podmioty stosujące AI powierzają sprawowanie nadzoru ze strony człowieka osobom fizycznym, które mają niezbędne kompetencje, ukończone szkolenia i uprawnienia, a także niezbędne wsparcie.***

.

3. Obowiązki określone w ust. 1 ***i 2*** pozostają bez uszczerbku dla innych obowiązków ***podmiotu stosującego AI*** wynikających z prawa Unii lub prawa krajowego oraz dla przysługującej ***podmiotowi stosującemu AI*** swobody organizowania swoich zasobów własnych i działań w celu wdrożenia wskazanych przez dostawcę środków nadzoru ze strony człowieka.

4. Nie naruszając przepisów ust. 1 ***i*** 2, w zakresie, w jakim ***podmiot stosujący AI*** sprawuje kontrolę nad danymi wejściowymi, ***podmiot ten*** zapewnia adekwatność ***i wystarczającą reprezentatywność*** danych wejściowych w odniesieniu do przeznaczenia systemu AI wysokiego ryzyka.

5. ***Podmioty stosujące AI*** monitorują działanie systemu AI wysokiego ryzyka w oparciu o instrukcję obsługi ***i w stosownych przypadkach informują dostawców zgodnie z art. 72.*** W przypadku gdy podmioty stosujące AI mają powody sądzić, że wykorzystanie systemu AI wysokiego ryzyka zgodnie z instrukcją obsługi może stwarzać ryzyko w rozumieniu art. 79 ust. 1, ***bez zbędnej zwłoki*** informują o tym dostawcę lub dystrybutora ***oraz odpowiedni organ nadzoru rynku i*** zawieszają użytkowanie systemu. W przypadku gdy podmioty stosujące AI stwierdziły wystąpienie poważnego incydentu, ***niezwłocznie*** informują o tym incydencie ***najpierw*** dostawcę, ***a następnie importera*** lub dystrybutora ***oraz odpowiednie organy nadzoru rynku. Jeżeli podmiot stosujący AI nie jest w stanie skontaktować się z dostawcą, stosuje się odpowiednio przepisy art. 73. Obowiązek ten nie obejmuje wrażliwych danych operacyjnych podmiotów stosujących AI będących organami ścigania.***

   W odniesieniu do ***podmiotów stosujących AI będących*** instytucjami ***finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych***, obowiązek w zakresie monitorowania, o którym mowa w akapicie pierwszym, uznaje się za spełniony w przypadku zapewnienia zgodności z przepisami dotyczącymi uzgodnień, procedur i mechanizmów zarządzania wewnętrznego na podstawie ***odpowiednich przepisów dotyczących usług finansowych***.

6. ***Podmioty stosujące*** systemy AI wysokiego ryzyka przechowują generowane automatycznie przez system AI wysokiego ryzyka rejestry zdarzeń ▌ – w zakresie, w jakim rejestry te znajdują się one pod ich kontrolą ▌ – przez zgodny z przeznaczeniem danego systemu AI wysokiego ryzyka okres ***wynoszący co najmniej sześć miesięcy, o ile w mającym zastosowanie prawie Unii lub prawie krajowym, w szczególności prawie Unii dotyczącym ochrony danych osobowych, nie przewidziano inaczej***.

Podmioty stosujące AI będące instytucjami ***finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych***, prowadzą rejestry zdarzeń jako część dokumentacji prowadzonej na podstawie ***odpowiednich unijnych przepisów dotyczących usług finansowych***.

7. Przed oddaniem do użytku lub wykorzystaniem systemu AI wysokiego ryzyka w miejscu pracy podmioty stosujące AI będące pracodawcami informują przedstawicieli pracowników i pracowników, których to dotyczy, że będą objęci działaniem systemu AI wysokiego ryzyka. Informacje te przekazuje się, w stosownych przypadkach, zgodnie z zasadami i procedurami ustanowionymi w unijnym i krajowym prawie i praktykach w zakresie informowania pracowników i ich przedstawicieli.

8. Podmioty stosujące systemy AI wysokiego ryzyka, będące przy tym publicznymi organami lub instytucjami, organami i jednostkami organizacyjnymi Unii, spełniają obowiązki rejestracji, o których mowa w art. 49. Jeżeli takie podmioty stosujące AI stwierdzą, że system AI wysokiego ryzyka, który zamierzają stosować, nie został zarejestrowany w bazie danych UE, o której mowa w art. 71, nie stosują tego systemu i informują o tym dostawcę lub dystrybutora.

9. ***W stosownych przypadkach, podmioty stosujące*** systemy AI wysokiego ryzyka korzystają z informacji przekazanych na podstawie art. 13 niniejszego rozporządzenia, aby wywiązać się ze spoczywającego na nich obowiązku przeprowadzenia oceny skutków dla ochrony danych zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680. ▌

10. ***Bez uszczerbku dla dyrektywy (UE) 2016/680, w ramach postępowania przygotowawczego w sprawie ukierunkowanego poszukiwania osoby podejrzanej o popełnienie przestępstwa lub skazanej za popełnienie przestępstwa podmiot stosujący system AI*** wysokiego ryzyka ***do celów zdalnej identyfikacji biometrycznej*** **post factum** ***zwraca się –*** **ex ante** ***lub bez zbędnej zwłoki, nie później jednak niż w ciągu 48 godzin – do organu sądowego lub organu administracyjnego, którego decyzja jest wiążąca i podlega kontroli sądowej, o zezwolenie na korzystanie z tego systemu, z wyjątkiem sytuacji, gdy jest on wykorzystywany do wstępnej identyfikacji potencjalnego podejrzanego w oparciu o obiektywne i możliwe do zweryfikowania fakty bezpośrednio związane z przestępstwem. Każde użycie jest ograniczone do tego, co jest ściśle niezbędne do prowadzenia postępowań przygotowawczych w sprawie konkretnego przestępstwa.***

W przypadku gdy wniosek o zezwolenie, o którym mowa w akapicie pierwszym, zostanie odrzucony, wykorzystanie z systemu zdalnej identyfikacji biometrycznej **post factum,** ***będące przedmiotem wniosku o zezwolenie, zostaje wstrzymane ze skutkiem natychmiastowym, a dane osobowe związane z wykorzystaniem systemu AI*** wysokiego ryzyka, w ***odniesieniu do którego złożono wniosek o zezwolenie, zostają usunięte.***

W żadnym wypadku taki system AI wysokiego ryzyka ***służący do zdalnej identyfikacji biometrycznej*** **post factum** ***nie może być wykorzystywany do celów ścigania przestępstw w sposób nieukierunkowany, bez związku z przestępstwem, postępowaniem karnym, rzeczywistym i obecnym lub rzeczywistymi przewidywalnym zagrożeniem popełnieniem przestępstwa lub poszukiwaniem konkretnej osoby zaginionej. Należy zapewnić, by żadna decyzja wywołująca niepożądane skutki prawne dla danej osoby nie mogła zostać podjęta przez organy ścigania wyłącznie na podstawie wyników uzyskanych z systemu zdalnej identyfikacji biometrycznej*** **post factum.**

Niniejszy ustęp pozostaje bez uszczerbku dla art. 9 rozporządzenia (UE) 2016/679 i art. 10 dyrektywy (UE) 2016/680 w odniesieniu do przetwarzania danych biometrycznych.

Niezależnie od celu lub podmiotu stosującego AI każde wykorzystanie takich systemów AI wysokiego ryzyka ***jest dokumentowane w odpowiednich aktach policyjnych i jest udostępniane na żądanie właściwemu organowi nadzoru rynku i krajowemu organowi ochrony danych, z wyłączeniem ujawniania szczególnie chronionych danych operacyjnych związanych ze ściganiem przestępstw. Niniejszy akapit pozostaje bez uszczerbku dla uprawnień powierzonych organom nadzorczym dyrektywą (UE) 2016/680.***

Podmioty stosujące AI przedkładają właściwym organom nadzoru rynku i krajowym organom ochrony danych roczne sprawozdania dotyczące korzystania przez nie z systemów zdalnej identyfikacji biometrycznej* post factum*, z wyłączeniem ujawniania szczególnie chronionych danych operacyjnych związanych ze ściganiem przestępstw. Sprawozdania te mogą zostać zagregowane w celu uwzględnienia stosowania więcej niż jednego systemu.

Państwa członkowskie mogą wprowadzić, zgodnie z prawem Unii, bardziej restrykcyjne przepisy dotyczące korzystania z systemów zdalnej identyfikacji biometrycznej post factum.

11. Bez uszczerbku dla art. 50 niniejszego rozporządzenia podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniku III, które to podmioty podejmują decyzje lub uczestniczą w podejmowaniu decyzji dotyczących osób fizycznych, informują osoby fizyczne o tym, że jest w odniesieniu do nich wykorzystywany system AI wysokiego ryzyka. W przypadku systemów AI wysokiego ryzyka wykorzystywanych do celów ścigania przestępstw zastosowanie ma art. 13 dyrektywy (UE) 2016/680.

12. Podmioty stosujące AI współpracują z odpowiednimi właściwymi organami krajowymi przy wszelkich działaniach, które organy te podejmują w odniesieniu do systemu AI wysokiego ryzyka, aby wdrożyć niniejsze rozporządzenie.

Artykuł 27

Ocena skutków systemów AI wysokiego ryzyka dla przestrzegania praw podstawowych

1. ***Przed zastosowaniem systemu AI wysokiego ryzyka, o którym mowa w art. 6 ust. 2, z wyjątkiem systemów AI wysokiego ryzyka przeznaczonych do stosowania w obszarze wymienionym w załączniku III pkt 2, podmioty stosujące AI będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w*** załączniku III pkt 5 lit. b) i c), ***przeprowadzają ocenę wpływu na prawa podstawowe, jaki może wywołać wykorzystanie takiego systemu. W tym celu podmioty stosujące AI przeprowadzają ocenę obejmującą:***

a) ***opis procesów podmiotu stosującego AI, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem;***

b) ***opis okresu, w którym każdy system AI wysokiego ryzyka ma być wykorzystywany i opis częstotliwości teg wykorzystywania;***

c) ***kategorie osób fizycznych i grup, na które wykorzystanie systemu może mieć wpływ;***

d) szczególne ryzyko szkody, które może mieć wpływ na kategorie osób lub grupy osób zidentyfikowane zgodnie z lit. c) niniejszego ustępu, z uwzględnieniem informacji przekazanych przez dostawcę zgodnie z art. 13;

e) opis wdrożenia środków nadzoru ze strony człowieka, zgodnie z instrukcją obsługi;

f) środki, jakie należy podjąć w przypadku potwierdzenia się tego ryzyka, w tym ustalenia dotyczące zarządzania wewnętrznego i mechanizmów rozpatrywania skarg.

2. Obowiązek ustanowiony w ust. 1 ma zastosowanie do wykorzystania systemu AI wysokiego ryzyka po raz pierwszy. W podobnych przypadkach podmiot stosujący AI może polegać na wcześniej przeprowadzonych ocenach skutków dla przestrzegania praw podstawowych lub na istniejących ocenach skutków przeprowadzonych przez dostawcę. Jeżeli w trakcie korzystania z systemu AI wysokiego ryzyka podmiot stosujący AI uzna, że którykolwiek z elementów wymienionych w ust. 1 uległ zmianie lub nie jest już aktualny, podmiot ten podejmuje niezbędne kroki w celu aktualizacji informacji.

3. Po przeprowadzeniu oceny, o której mowa w ust. 1 niniejszego artykułu, podmiot stosujący AI powiadamia organ nadzoru rynku o jej wynikach, w tym w ramach tego powiadomienia wypełnia i przekazuje kwestionariusz, o którym mowa w ust. 5 niniejszego artykułu. W przypadku, o którym mowa w art. 46 ust. 1, podmioty stosujące AI mogą zostać zwolnione z tego obowiązku.

4. ***Jeżeli którykolwiek z obowiązków ustanowionych w niniejszym artykule został już spełniony w wyniku oceny skutków dla ochrony danych przeprowadzonej zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680, ocena skutków dla przestrzegania praw podstawowych, o której mowa w ust. 1 niniejszego artykułu, jest uzupełnieniem tej oceny skutków dla ochrony danych.***

5. ***Urząd ds. AI opracowuje wzór kwestionariusza, w tym za pomocą zautomatyzowanego narzędzia, aby ułatwić podmiotom stosującym AI wypełnianie ich obowiązków wynikających z niniejszego artykułu w sposób uproszczony.***

Sekcja 4

Organy notyfikujące i jednostki notyfikowane

Artykuł 28

Organy notyfikujące

1. Każde państwo członkowskie wyznacza lub ustanawia ***przynajmniej jeden*** organ notyfikujący odpowiedzialny za opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność oraz za ich monitorowanie. ***Procedury te są opracowywane wspólnie przez organy notyfikujące wszystkich państw członkowskich.***

2. Państwa członkowskie mogą ***zdecydować, że ocena oraz monitorowanie, o których mowa w ust. 1, są prowadzone przez*** krajową jednostkę akredytującą w ***rozumieniu*** rozporządzenia (WE) nr 765/2008 ▌ ***oraz zgodnie z tym rozporządzeniem***.

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 otrzymywanych informacji ***zgodnie z art. 78.***

7. Organy notyfikujące muszą dysponować ***odpowiednią*** liczbą kompetentnych pracowników, aby należycie wykonywać powierzone im zadania. ***Kompetentni pracownicy mają wiedzę fachową niezbędną do pełnienia danej funkcji odpowiednio w dziedzinach takich jak technologie informacyjne, AI i prawo, w tym nadzór nad prawami podstawowymi.***

Artykuł 29

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 ***rodzajów systemów AI***, 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. 31.

   Do wniosku załącza się również wszelkie ważne dokumenty dotyczące obowiązującego wyznaczenia – na podstawie wszelkiego innego unijnego prawodawstwa harmonizacyjnego – występującej z wnioskiem jednostki notyfikowanej.

3. Jeżeli dana jednostka oceniająca zgodność nie jest w stanie przedstawić certyfikatu akredytacji, przekazuje organowi notyfikującemu ***wszystkie*** dowody w postaci dokumentów niezbędne do zweryfikowania, potwierdzenia i regularnego monitorowania przestrzegania przez tę jednostkę wymogów ustanowionych w art. 31.

4. W odniesieniu do jednostek notyfikowanych wyznaczonych na podstawie wszelkiego innego unijnego prawodawstwa harmonizacyjnego w stosownych przypadkach dopuszcza się możliwość wykorzystania wszelkich dokumentów i certyfikatów dotyczących takiego wyznaczenia w charakterze dowodów w toku procedury wyznaczania przeprowadzanej zgodnie z niniejszym rozporządzeniem. ***Jednostka notyfikowana aktualizuje dokumentację, o której mowa w ust. 2 i 3 niniejszego artykułu, gdy tylko wystąpią istotne zmiany, aby organowi odpowiedzialnemu za jednostki notyfikowane umożliwić monitorowanie i weryfikowanie ciągłej zgodności ze wszystkimi wymogami ustanowionymi w art. 31.***

Artykuł 30

Procedura notyfikacyjna

1. Organy notyfikujące mogą ▌ dokonywać ***notyfikacji*** wyłącznie w odniesieniu do tych jednostek oceniających zgodność, które spełniają wymogi ustanowione w art. 31.

2. Organy notyfikujące dokonują notyfikacji na rzecz Komisji i pozostałych państw członkowskich, za pomocą narzędzia do notyfikacji elektronicznej opracowanego i obsługiwanego przez Komisję, ***o każdej jednostce oceniającej zgodność, o której mowa w ust. 1***.

3. Notyfikacja, o ***której mowa w ust. 2 niniejszego artykułu***, zawiera wyczerpujące, szczegółowe informacje na temat czynności z zakresu oceny zgodności, modułu lub modułów oceny zgodności i przedmiotowych rodzajów ***systemów AI oraz odpowiednie poświadczenie kompetencji***. ***W przypadku gdy podstawą notyfikacji nie jest certyfikat akredytacji, o którym mowa w art. 29 ust. 2, organ notyfikujący przedkłada Komisji i państwom członkowskim dowody w postaci dokumentów potwierdzające kompetencje jednostki oceniającej zgodność oraz wdrożone rozwiązania zapewniające regularne monitorowanie tej jednostki i ciągłe spełnianie przez nią wymagań ustanowionych w art. 31.***

4. Dana jednostka oceniająca zgodność może wykonywać działania jednostki notyfikowanej tylko wówczas, gdy Komisja lub pozostałe państwa członkowskie nie zgłosiły zastrzeżeń ***w terminie dwóch tygodni od notyfikacji przez organ notyfikujący, w przypadku gdy notyfikacja ta obejmuje certyfikat akredytacji, o którym mowa w art. 29 ust. 2, lub w terminie dwóch miesięcy od*** notyfikacji ***przez organ notyfikujący, w przypadku gdy notyfikacja ta obejmuje dowody w postaci dokumentów, o których mowa w art. 29 ust. 3***.

5. ***W przypadku zgłoszenia zastrzeżeń Komisja niezwłocznie przystępuje do konsultacji z odpowiednim państwem członkowskim i jednostką oceniającą zgodność. Na tej podstawie Komisja podejmuje decyzję, czy dane zezwolenie jest uzasadnione. Komisja kieruje swoją decyzję do zainteresowanego państwa członkowskiego i odpowiedniej jednostki oceniającej zgodność.***

Artykuł 31

Wymogi dotyczące jednostek notyfikowanych

1. ***Jednostka*** notyfikowana ***jest ustanawiana zgodnie z prawem krajowym danego państwa członkowskiego i ma osobowość prawną.***

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, ***jak również odpowiednie wymogi w zakresie cyberbezpieczeństwa.***

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

4. Jednostki notyfikowane muszą być niezależne od dostawcy systemu AI wysokiego ryzyka, wobec którego podejmują czynności z zakresu oceny zgodności. Jednostki notyfikowane muszą być również niezależne od wszelkich innych operatorów, których interes gospodarczy wiąże się z systemami AI wysokiego ryzyka będącymi przedmiotem oceny, a także od wszelkich innych konkurentów dostawcy. ***Nie wyklucza to wykorzystania ocenianych systemów AI wysokiego ryzyka, które są niezbędne do prowadzenia działalności jednostki oceniającej zgodność, ani wykorzystania takich systemów AI wysokiego ryzyka do celów prywatnych.***

5. Jednostka oceniająca zgodność, jej kierownictwo najwyższego szczebla ani pracownicy odpowiedzialni za realizację zadań związanych z oceną zgodności nie mogą być bezpośrednio zaangażowani w projektowanie, opracowanie, sprzedaż ani wykorzystywanie systemów AI wysokiego ryzyka, nie mogą też reprezentować stron zaangażowanych w taką działalność. Nie angażują się oni w żadną działalność, która może zagrozić niezależności ich osądów i wiarygodności w związku z działalnością w zakresie oceny zgodności, do której zostali notyfikowani. Dotyczy to w szczególności usług konsultingowych.

6. 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.

7. Jednostki notyfikowane dysponują udokumentowanymi procedurami, które zapewniają zachowanie poufności informacji – ***zgodnie z art. 78*** – przez ich personel, komitety, jednostki zależne, podwykonawców oraz wszelkie stowarzyszone z nimi jednostki lub pracowników podmiotów zewnętrznych, które to informacje 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, jednak nie w stosunku do organów notyfikujących państwa członkowskiego, w którym jednostki notyfikowane prowadzą działalność.

8. Jednostki notyfikowane dysponują procedurami prowadzenia czynności z uwzględnieniem rozmiaru dostawcy, sektora, w którym prowadzi on działalność, jego struktury oraz stopnia złożoności danego systemu AI.

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

10. Jednostki notyfikowane posiadają zdolność wykonywania wszystkich zadań wynikających z 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.

11. Jednostki notyfikowane dysponują wystarczającymi kompetencjami wewnętrznymi pozwalającymi im skutecznie oceniać zadania wykonywane w ich imieniu przez podmioty zewnętrzne. ▌ Jednostka notyfikowana zapewnia stałą dostępność wystarczającej liczby pracowników odpowiedzialnych za aspekty administracyjne, techniczne, ***prawne*** i naukowe dysponujących doświadczeniem i wiedzą w zakresie odnośnych ***rodzajów systemów*** AI, danych i metod przetwarzania danych oraz w zakresie wymogów ustanowionych w sekcji 2.

12. 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 same posiadały znajomość odpowiednich norm i dysponowały zawsze aktualną wiedzą na ich temat.

Artykuł 32

Domniemanie zgodności z wymogami dotyczącymi jednostek notyfikowanych

W przypadku gdy jednostka oceniająca zgodność wykaże swoją zgodność z kryteriami ustanowionymi w odpowiednich normach zharmonizowanych lub częściach tych norm, do których odniesienia opublikowano w Dzienniku Urzędowym Unii Europejskiej, zakłada się, że spełnia ona wymogi ustanowione w art. 31 w zakresie, w jakim mające zastosowanie normy zharmonizowane obejmują te wymogi.

Artykuł 33

Jednostki zależne i podwykonawcy jednostek notyfikowanych

1. W przypadku gdy 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. 31 oraz informuje o tym organ notyfikujący.

2. Jednostki notyfikowane ponoszą pełną odpowiedzialność za swoje zadania wykonywane przez podwykonawców lub jednostki zależne.

3. Zadania mogą być zlecane podwykonawcy lub wykonywane przez jednostkę zależną wyłącznie za zgodą dostawcy. ***Jednostki notyfikowane podają do wiadomości publicznej wykaz swoich jednostek zależnych.***

4. ▌ Odpowiednie dokumenty dotyczące oceny kwalifikacji podwykonawcy lub jednostki zależnej oraz prac wykonywanych przez nich na podstawie niniejszego rozporządzenia ***przechowuje się do dyspozycji organu notyfikującego przez okres 5 lat od daty zakończenia działalności podwykonawczej***.

Artykuł 34

Obowiązki operacyjne jednostek notyfikowanych

1. *Jednostki notyfikowane weryfikują zgodność systemów AI wysokiego ryzyka zgodnie z procedurami oceny zgodności określonymi w art. 43.*

2. *Jednostki notyfikowane unikają niepotrzebnych obciążeń dla dostawców podczas wykonywania swoich czynności oraz należycie uwzględniają rozmiar dostawcy, sektor jego działania, strukturę oraz stopień złożoności danego systemu AI wysokiego ryzyka, w szczególności w celu zminimalizowania obciążeń administracyjnych i kosztów przestrzegania przepisów dla mikroprzedsiębiorstw i małych przedsiębiorstw w rozumieniu zalecenia 2003/361/WE. Jednostka notyfikowana zachowuje jednak odpowiednią rygorystyczność i poziom ochrony wymagane dla zagwarantowania zgodności danego systemu AI wysokiego ryzyka z wymogami niniejszego rozporządzenia.*

   .

3. *Na żądanie organu notyfikującego, o którym mowa w art. 28, jednostki notyfikowane udostępniają i przekazują temu organowi wszystkie stosowne dokumenty, uwzględniając dokumentację dostawców, aby zapewnić temu organowi możliwość przeprowadzania czynności w zakresie oceny, wyznaczania, notyfikacji i monitorowania oraz aby ułatwić mu przeprowadzenie oceny opisanej w niniejszej sekcji.*

Artykuł 35

Numery identyfikacyjne i wykazy jednostek notyfikowanych

1. Komisja przydziela każdej jednostce notyfikowanej jeden numer identyfikacyjny, nawet jeżeli jednostkę tę notyfikowano na podstawie kilku aktów Unii.

2. Komisja podaje do wiadomości publicznej wykaz jednostek notyfikowanych na podstawie niniejszego rozporządzenia, łącznie z ich numerami identyfikacyjnymi oraz informacją na temat czynności będących przedmiotem notyfikacji. Komisja zapewnia aktualność tego wykazu.

Artykuł 36

Zmiany w notyfikacjach

1. Organ notyfikujący powiadamia Komisję i pozostałe państwa członkowskie za pomocą systemu notyfikacji elektronicznej, o którym mowa w art. 30 ust. 2, o wszelkich istotnych zmianach w notyfikacji danej jednostki notyfikowanej.

2. Procedury ustanowione w art. 29 i 30 mają zastosowanie do rozszerzenia zakresu notyfikacji.

W przypadku zmian w notyfikacji innych niż rozszerzenie jej zakresu stosuje się procedury ustanowione w ustępach poniżej.

3. W przypadku gdy jednostka notyfikowana podejmie decyzję o zaprzestaniu prowadzenia czynności z zakresu oceny zgodności, jak najszybciej informuje o tym organ notyfikujący i odnośnych dostawców, a w przypadku planowanego zaprzestania działalności – na co najmniej rok przed zaprzestaniem działalności. Certyfikaty wydane przez jednostkę notyfikowaną mogą pozostać ważne tymczasowo przez okres dziewięciu miesięcy po zaprzestaniu działalności jednostki notyfikowanej, pod warunkiem że inna jednostka notyfikowana potwierdzi na piśmie, że przejmie odpowiedzialność za objęte tymi certyfikatami systemy AI wysokiego ryzyka. Przed upływem tego okresu dziewięciu miesięcy nowa jednostka notyfikowana przeprowadza pełną ocenę odnośnych systemów AI, zanim wyda nowe certyfikaty dla tych systemów. W przypadku gdy jednostka notyfikowana zaprzestała działalności, organ notyfikujący wycofuje jej wyznaczenie.

4. W przypadku gdy organ notyfikujący ma ***wystarczające powody, by sądzić,*** że jednostka notyfikowana przestała spełniać wymogi określone w art. 31 lub nie wypełnia swoich obowiązków, organ ***notyfikujący*** 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 [redacted] przestała spełniać wymogi ustanowione w art. 31 lub nie wypełnia swoich obowiązków, organ ten, stosownie do przypadku, ogranicza, zawiesza lub cofa [redacted] wyznaczenie, w zależności od powagi ***niespełnienia tych wymogów lub niewypełnienia tych obowiązków.*** Niezwłocznie informuje on [redacted] o tym fakcie odpowiednio Komisję i pozostałe państwa członkowskie.

5. W przypadku gdy wyznaczenie ***zostało zawieszone, ograniczone lub całkowicie lub częściowo cofnięte, jednostka notyfikowana najpóźniej w ciągu 10 dni informuje o tym zainteresowanych dostawców***.

6. W przypadku ograniczenia, zawieszenia lub cofnięcia wyznaczenia organ notyfikujący podejmuje odpowiednie kroki w celu zapewnienia, by zachowana została dokumentacja danej jednostki notyfikowanej i była udostępniana organom notyfikującym w pozostałych państwach członkowskich oraz organom nadzoru rynku na ich wniosek.

7. W przypadku ograniczenia, zawieszenia lub cofnięcia wyznaczenia organ notyfikujący:

a) ocenia wpływ na certyfikaty wydane przez daną jednostkę notyfikowaną;

b) przedkłada Komisji i pozostałym państwom członkowskim sprawozdanie ze swoich ustaleń w ciągu trzech miesięcy od powiadomienia o zmianach w wyznaczeniu;

c) zwraca się do jednostki notyfikowanej, by w celu zapewnienia ciągłości zgodności systemów AI na rynku zawiesiła lub cofnęła, w rozsądnym terminie ustalonym przez ten organ, wszelkie certyfikaty, które zostały nienależnie wydane;

d) informuje Komisję i państwa członkowskie o certyfikatach, których zawieszenia lub cofnięcia zażądał;

e) przekazuje właściwym organom krajowym państwa członkowskiego, w którym dostawca ma zarejestrowane miejsce prowadzenia działalności, wszelkie istotne informacje na temat certyfikatów, w odniesieniu do których zażądał zawieszenia lub cofnięcia. Organy te podejmują w stosownych przypadkach odpowiednie środki w celu uniknięcia potencjalnego zagrożenia zdrowia, bezpieczeństwa lub praw podstawowych.

8. Z wyjątkiem certyfikatów nienależnie wydanych, w przypadkach, w których zawieszono lub ograniczono wyznaczenie, certyfikaty pozostają ważne jeżeli wystąpiła jedna z następujących okoliczności:

a) organ notyfikujący potwierdził, w terminie jednego miesiąca od zawieszenia lub ograniczenia, że w odniesieniu do certyfikatów, na które wpływ ma to zawieszenie lub ograniczenie, nie występuje zagrożenie zdrowia, bezpieczeństwa lub praw podstawowych i określił czas działań służących temu, by zaradzić temu zawieszeniu lub ograniczeniu; lub

b) organ notyfikujący potwierdził, że w czasie trwania zawieszenia lub ograniczenia nie będą wydawane, zmieniane ani wydawane ponownie żadne certyfikaty powiązane z danym zawieszeniem, oraz stwierdza, czy dana jednostka notyfikowana jest zdolna do dalszego monitorowania i bycia odpowiedzialną za wydane już certyfikaty obowiązujące w okresie pokrywającym się z tym zawieszeniem lub ograniczeniem. W przypadku gdy organ *notyfikujący ustali, że jednostka notyfikowana nie posiada zdolności do obsługi wydanych certyfikatów, dostawca systemu objętego danym certyfikatem – w terminie trzech miesięcy od zawieszenia lub ograniczenia – przekazuje właściwym organom krajowym w państwie członkowskim, w którym ma zarejestrowane miejsce prowadzenia działalności, potwierdzenie na piśmie, że inna wykwalifikowana jednostka notyfikowana tymczasowo przejmuje funkcje jednostki notyfikowanej w zakresie monitorowania certyfikatów i pozostanie ona odpowiedzialna za te certyfikaty w okresie zawieszenia lub ograniczenia wyznaczenia, o którym mowa powyżej.*

9. Z wyjątkiem certyfikatów nienależnie wydanych, w przypadkach, w których wyznaczenie zostało cofnięte, certyfikaty pozostają ważne przez okres dziewięciu miesięcy w następujących okolicznościach:

a) właściwy organ krajowy w państwie członkowskim, w którym dostawca systemu AI objętego certyfikatem ma zarejestrowane miejsce prowadzenia działalności, potwierdził, że nie występuje zagrożenie zdrowia, bezpieczeństwa lub praw podstawowych związane z danymi systemami AI wysokiego ryzyka; oraz

b) inna jednostka notyfikowana potwierdziła na piśmie, że przejmie bezpośrednią odpowiedzialność za ocenę tych systemów AI i zakończy swoją ocenę w terminie dwunastu miesięcy od cofnięcia wyznaczenia.

W okolicznościach, o których mowa w akapicie pierwszym, właściwy organ krajowy w państwie członkowskim, w którym dostawca systemu objętego certyfikatem ma zarejestrowane miejsce prowadzenia działalności, może przedłużyć tymczasową ważność tych certyfikatów na dodatkowe trzymiesięczne okresy, które łącznie nie przekraczają dwunastu miesięcy.

Właściwy organ krajowy lub jednostka notyfikowana przejmująca funkcje jednostki notyfikowanej, której wyznaczenie zostało zmienione, niezwłocznie powiadamiają o tym Komisję, pozostałe państwa członkowskie i pozostałe jednostki notyfikowane.

Artykuł 37

Kwestionowanie kompetencji jednostek notyfikowanych

1. W razie konieczności Komisja bada wszystkie sytuacje, w których ma podstawy wątpić ***w kompetencje*** jednostki notyfikowanej ***lub w ciągłość spełniania przez jednostkę notyfikowaną*** wymogów ustanowionych w art. 31 ***oraz wypełnianie mających zastosowanie obowiązków***.

2. Organ notyfikujący przekazuje Komisji, na żądanie, wszystkie istotne informacje dotyczące notyfikacji ***lub utrzymania kompetencji*** przez daną jednostkę notyfikowaną.

3. Komisja zapewnia zgodnie z art. 78 poufność wszystkich informacji ***wrażliwych*** uzyskanych w toku postępowań wyjaśniających prowadzonych zgodnie z niniejszym artykułem.

4. W przypadku gdy Komisja stwierdzi, że jednostka notyfikowana nie spełnia wymogów ***notyfikacji*** lub przestała je spełniać, ***informuje o tym fakcie*** notyfikujące państwo członkowskie ***i zwraca się do niego*** o wprowadzenie koniecznych środków naprawczych, włącznie z ***zawieszeniem lub*** cofnięciem notyfikacji, jeżeli zachodzi taka potrzeba. ***W przypadku niewprowadzenia przez państwo członkowskie koniecznych środków naprawczych Komisja może w drodze aktu wykonawczego zawiesić, ograniczyć lub cofnąć wyznaczenie.*** Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

Artykuł 38

Koordynacja jednostek notyfikowanych

1. Komisja zapewnia – w odniesieniu do ***systemów AI wysokiego ryzyka*** – wprowadzenie i właściwy przebieg odpowiedniej koordynacji i współpracy jednostek notyfikowanych prowadzących działalność w zakresie procedur oceny zgodności ▌ zgodnie z niniejszym rozporządzeniem – w formie sektorowej grupy jednostek notyfikowanych.

2. Każdy ***organ notyfikujący*** zapewnia, aby notyfikowane przez niego jednostki uczestniczyły bezpośrednio lub za pośrednictwem wyznaczonych przedstawicieli w pracach grupy, o której mowa w ust. 1.

3. Komisja jest zobowiązana zapewnić wymianę wiedzy i najlepszych praktyk między organami notyfikującymi państw członkowskich.

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, ***pod warunkiem, że spełniają wymogi określone w art. 31 lub zapewniają równoważny poziom zgodności.***

Sekcja 5

Normy, ocena zgodności, certyfikaty, rejestracja

Artykuł 40

Normy zharmonizowane ***i dokumenty normalizacyjne***

1. Systemy AI wysokiego ryzyka spełniające normy zharmonizowane lub części tych norm, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej* ***zgodnie z rozporządzeniem (UE) nr 1025/2012*** uznaje się za spełniające wymogi określone w sekcji 2 niniejszego rozdziału ***lub, w stosownych przypadkach, wymogi określone w*** rozdziale IV ***niniejszego rozporządzenia***, w zakresie, w jakim wspomniane normy obejmują te wymogi lub obowiązki.

2. Komisja bez zbędnej zwłoki wydaje wnioski o normalizację obejmujące wszystkie wymogi określone w sekcji 2 niniejszego rozdziału oraz, w stosownych przypadkach, ***obowiązki określone w*** rozdziale ***IV niniejszego rozporządzenia, zgodnie z art. 10 rozporządzenia (UE) nr 1025/2012. We wniosku o normalizację zwraca się również o przedstawienie wyników sprawozdawczości i procesów dokumentowania w celu poprawy wydajności zasobów systemów AI, takich jak zmniejszenie zużycia energii i innych zasobów systemu AI wysokiego ryzyka w jego cyklu życia, oraz wyników dotyczących efektywnego energetycznie rozwoju modeli AI ogólnego przeznaczenia. Przygotowując wniosek o normalizację, Komisja konsultuje się z Radą ds. AI i odpowiednimi zainteresowanymi stronami, w tym z forum doradczym.***

Wystosowując wniosek o normalizację do europejskich organizacji normalizacyjnych, Komisja określa, że normy muszą być jasne, spójne, w tym z normami opracowanymi w poszczególnych sektorach dla produktów objętych zakresem stosowania istniejącego unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I, i mieć na celu zapewnienie, by systemy lub modele AI wprowadzane do obrotu lub oddawane do użytku w Unii spełniały odpowiednie wymogi ustanowione w niniejszym rozporządzeniu.

Komisja zwraca się do europejskich organizacji normalizacyjnych o przedstawienie dowodów, że dokładają wszelkich starań, aby osiągnąć cele, o których mowa w akapicie pierwszym i drugim niniejszego ustępu, zgodnie z art. 24 rozporządzenia (UE) nr 1025/2012.

3. Uczestnicy procesu normalizacji dążą do promowania inwestycji i innowacji w dziedzinie AI, w tym poprzez zwiększenie pewności prawa, a także konkurencyjności i wzrostu rynku unijnego oraz przyczyniają się do wzmocnienia globalnej współpracy w zakresie normalizacji i z uwzględnieniem istniejących w dziedzinie AI norm międzynarodowych zgodnych z wartościami Unii, prawami podstawowymi i interesem Unii, a także poprawiają zarządzanie wielostronne, zapewniając wyważoną reprezentację interesów i skuteczny udział wszystkich odpowiednich zainteresowanych stron zgodnie z art. 5, 6 i 7 rozporządzenia (UE) nr 1025/2012.

Artykuł 41

Wspólne specyfikacje

1. ***Komisja jest uprawniona do przyjmowania aktów wykonawczych ustanawiających wspólne specyfikacje w odniesieniu do wymogów określonych w*** sekcji 2 ***niniejszego rozdziału lub, w stosownych przypadkach,*** obowiązków określonych w rozdziale IV, w ***przypadku gdy spełnione są następujące warunki:***

   a) Komisja wystąpiła zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012 do jednej lub kilku europejskich organizacji normalizacyjnych z wnioskiem o opracowanie normy zharmonizowanej w odniesieniu do wymogów określonych w sekcji ***2 niniejszego rozdziału,*** oraz:

      (i) wniosek ten nie został przyjęty przez żadną z europejskich organizacji normalizacyjnych; lub

      (ii) normy zharmonizowane stanowiące odpowiedź na ten wniosek nie zostały wydane w terminie określonym zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012; lub

      (iii) odpowiednie normy zharmonizowane w niewystarczającym stopniu uwzględniają obawy dotyczące praw podstawowych; lub

      (iv) normy zharmonizowane nie są zgodne z wnioskiem; oraz

b) w Dzienniku Urzędowym Unii Europejskiej nie opublikowano odniesienia do zharmonizowanych norm obejmujących wymogi określone w sekcji 2 niniejszego tytułu zgodnie z przepisami rozporządzenia (UE) nr 1025/2012 i nie przewiduje się opublikowania takiego odniesienia w rozsądnym terminie.

Akty wykonawcze, o których mowa w akapicie pierwszym niniejszego ustępu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2, po konsultacji z forum doradczym, o którym mowa w art. 67.

2. Przed przygotowaniem projektu aktu wykonawczego Komisja informuje komitet, o którym mowa w art. 22 rozporządzenia (UE) nr 1025/2012, że uznaje warunki ustanowione w ust. 1 niniejszego artykułu za spełnione.

3. Systemy AI wysokiego ryzyka zgodne ze wspólnymi specyfikacjami, o których mowa w ust. 1, ***lub z częściami tych specyfikacji*** uznaje się za spełniające wymogi ustanowione w sekcji 2 w zakresie, w jakim wspomniane wspólne specyfikacje obejmują te wymogi.

4. W przypadku gdy europejska organizacja normalizacyjna przyjmuje normę zharmonizowaną i proponuje Komisji opublikowanie odniesienia do niej w Dzienniku Urzędowym Unii Europejskiej, Komisja ocenia normę zharmonizowaną zgodnie z rozporządzeniem (UE) nr 1025/2012. W przypadku opublikowania odniesienia do normy zharmonizowanej w Dzienniku Urzędowym Unii Europejskiej Komisja uchyla akty wykonawcze, o których mowa w ust. 1, lub ich części, które obejmują te same zasadnicze wymogi określone w sekcji ***2 niniejszego rozdziału***.

5. W przypadku gdy dostawcy ***systemów AI wysokiego ryzyka*** nie zapewnią zgodności ze wspólnymi specyfikacjami, o których mowa w ust. 1, należycie wykazują oni, że przyjęli rozwiązania techniczne, które ***spełniają wymogi, o których mowa w*** sekcji ***2, na poziomie*** co najmniej równoważnym tym wspólnym specyfikacjom.

6. ***W przypadku gdy państwo członkowskie uzna, że wspólna specyfikacja niecałkowicie spełnia zasadnicze wymogi określone w*** sekcji ***2, informuje o tym Komisję, przedstawiając szczegółowe wyjaśnienie. Komisja ocenia te informacje i w stosownym przypadku zmienia akt wykonawczy ustanawiający daną wspólną specyfikację.***

Artykuł 42

Domniemanie zgodności z określonymi wymogami

1. Systemy AI wysokiego ryzyka, które zostały wytrenowane i przetestowane przy użyciu danych ***odzwierciedlających*** określone otoczenie geograficzne, behawioralne, ***kontekstualne lub*** funkcjonalne, w którym planuje się z nich korzystać, uznaje się za spełniające ***odpowiednie wymogi*** ustanowione w art. 10 ust. 4.

2. Systemy AI wysokiego ryzyka, które uzyskały certyfikację lub w odniesieniu do których wydano deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 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 AI wysokiego ryzyka wymienionych w załączniku III pkt 1, w przypadku gdy do wykazania zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2 dostawca zastosował normy zharmonizowane, o których mowa w art. 40, lub, w stosownych przypadkach, wspólne specyfikacje, o których mowa w art. 41, dostawca ***wybiera*** jedną z następujących procedur oceny zgodności w oparciu o:

   a) kontrolę wewnętrzną, o której mowa w załączniku VI; ***lub***

   b) ocenę systemu zarządzania jakością i ocenę dokumentacji technicznej przeprowadzaną z udziałem jednostki notyfikowanej, o której to procedurze mowa w załączniku VII.

▌ Przy wykazywaniu zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2 dostawca ***stosuje procedurę oceny zgodności określoną w załączniku VII w przypadku gdy***:

   a) normy zharmonizowane, o których mowa w art. 40, ▌ nie istnieją, a wspólne specyfikacje, o których mowa w art. 41, nie są dostępne;

   b) dostawca ***nie zastosował normy zharmonizowanej lub zastosował jedynie jej część;***

   c) wspólne specyfikacje, o których mowa w lit. a), istnieją, ale dostawca ich nie zastosował;

   d) co najmniej jedna z norm zharmonizowanych, o których mowa w lit. a), została opublikowana z ograniczeniem i jedynie w odniesieniu do tej części normy, której dotyczy ograniczenie.

Na potrzeby procedury oceny zgodności, o której mowa w załączniku VII, dostawca może wybrać dowolną jednostkę notyfikowaną. Jednak w przypadku gdy system ma zostać oddany do użytku przez organy ścigania, organy imigracyjne lub organy azylowe lub przez instytucje, organy i jednostki organizacyjne Unii, funkcję jednostki notyfikowanej pełni organ nadzoru rynku, o którym mowa odpowiednio w art. 74 ust. 8 lub ust. 9.

2. W przypadku systemów AI wysokiego ryzyka, o których mowa w załączniku III ▌ pkt 2–8, dostawcy postępują zgodnie z procedurą oceny zgodności opierającą się na kontroli wewnętrznej, o której mowa w załączniku VI i która nie przewiduje udziału jednostki notyfikowanej. ▌

3. W przypadku systemów AI wysokiego ryzyka objętych zakresem stosowania unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A, dostawca przeprowadza odpowiednią procedurę oceny zgodności wymaganą na podstawie tych aktów prawnych. W odniesieniu do tego rodzaju systemów AI wysokiego ryzyka zastosowanie mają wymogi ustanowione w sekcji 2 niniejszego rozdziału 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 AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2, o ile zgodność tych jednostek notyfikowanych z wymogami ustanowionymi w art. 31 ust. 4, 10 i 11 została oceniona w kontekście procedury notyfikacyjnej przewidzianej w tych aktach prawnych.

W przypadku gdy akt prawny wymieniony w załączniku I sekcja A zapewnia producentowi produktu możliwość zrezygnowania z oceny zgodności przeprowadzanej przez stronę trzecią, o ile zapewnił on zgodność ze wszystkimi normami zharmonizowanymi obejmującymi wszystkie stosowne wymogi, taki producent może skorzystać z tej możliwości 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 sekcji 2 niniejszego rozdziału.

4. Systemy AI wysokiego ryzyka, ***które poddano już procedurze oceny zgodności***, poddaje się nowej procedurze oceny zgodności w przypadku gdy wprowadza się w nich istotne zmiany, niezależnie od tego, czy zmieniony system ma być przedmiotem dalszej dystrybucji lub czy ma być nadal wykorzystywany przez obecny ***podmiot stosujący AI***.

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

5. Komisja przyjmuje akty delegowane zgodnie z art. 97 w celu aktualizacji załączników VI i VII▌ z uwagi na postęp techniczny.

6. Komisja przyjmuje akty delegowane zgodnie z art. 97 w celu zmiany ust. 1 i 2 niniejszego artykułu, aby objąć systemy AI 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 zdrowia i bezpieczeństwa oraz zagrożeniom związanym z ochroną 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 wydane przez jednostki notyfikowane zgodnie z załącznikiem VII są sporządzane ***w języku łatwo zrozumiałym dla odpowiednich organów w*** państwie członkowskim, w którym jednostka notyfikowana ma siedzibę.

2. Certyfikaty zachowują ważność przez wskazany w nich okres, który nie może przekraczać pięciu lat **–** ***w odniesieniu do systemów AI objętych zakresem stosowania załącznika I oraz czterech lat – w odniesieniu do systemów AI objętych zakresem stosowania załącznika III.*** Na wniosek dostawcy ważność certyfikatu można przedłużyć na kolejne okresy, które nie mogą każdorazowo przekraczać pięciu lat **–** ***w odniesieniu do systemów AI objętych zakresem stosowania załącznika I oraz czterech lat – w odniesieniu do systemów AI objętych zakresem stosowania załącznika III***, w oparciu o wyniki ponownej oceny przeprowadzonej zgodnie z mającymi zastosowanie procedurami oceny zgodności. ***Wszelkie uzupełnienia do certyfikatu pozostają ważne, pod warunkiem, że uzupełniany certyfikat pozostaje ważny.***

3. Jeżeli jednostka notyfikowana stwierdzi, że system AI przestał spełniać wymogi ustanowione w sekcji 2, 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.

▌ Dostępna jest procedura odwoławcza od decyzji jednostek notyfikowanych, w tym w odniesieniu do wydanych certyfikatów zgodności.

Artykuł 45

Obowiązki jednostek notyfikowanych w zakresie informowania

1. Jednostki notyfikowane informują organ notyfikujący:

   a) o wszelkich unijnych certyfikatach oceny dokumentacji technicznej, wszelkich uzupełnieniach 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 uzupełnieniach 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 uzupełnieniach certyfikatów.

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

4. Obowiązki, o których mowa w ust. 1, 2 i 3 niniejszego artykułu, są wypełniane zgodnie z art. 78.

Artykuł 46

Odstępstwo od procedury oceny zgodności

1. Na zasadzie odstępstwa od art. 43 ***i w odpowiedzi na należycie uzasadniony wniosek*** każdy organ nadzoru rynku może wydać zezwolenie na wprowadzenie do obrotu lub oddanie do użytku konkretnych systemów AI wysokiego ryzyka na terytorium danego państwa członkowskiego w związku z wystąpieniem nadzwyczajnych względów dotyczących bezpieczeństwa publicznego lub ochrony zdrowia i życia osób, ochrony środowiska lub ochrony kluczowych aktywów przemysłowych i infrastrukturalnych. Wspomniane zezwolenie wydaje się tymczasowo ▌ na okres przeprowadzenia niezbędnych procedur oceny zgodności, ***uwzględniając nadzwyczajne względy uzasadniające przedmiotowe odstępstwo.*** Dokłada się starań, aby procedury te ukończono bez zbędnej zwłoki.

2. W należycie uzasadnionej sytuacji spowodowanej nadzwyczajnymi względami bezpieczeństwa publicznego lub w przypadku konkretnego, istotnego i bezpośredniego zagrożenia życia lub bezpieczeństwa fizycznego osób fizycznych, organy ścigania lub organy ochrony ludności mogą oddać do użytku określony system AI wysokiego ryzyka bez zezwolenia, o którym mowa w ust. 1, pod warunkiem że wniosek o takie zezwolenie zostanie bez zbędnej zwłoki złożony w trakcie korzystania z tego systemu lub tuż po nim. Jeśli zezwolenie, o którym mowa w ust. 1, nie zostanie wydane, korzystanie z tego systemu AI wysokiego ryzyka zostanie natychmiast przerwane i wszystkie wyniki i rezultaty tego wykorzystania zostaną niezwłocznie zniszczone.

3. Zezwolenie, o którym mowa w ust. 1, wydaje się wyłącznie wówczas, gdy organ nadzoru rynku stwierdzi, że system AI wysokiego ryzyka spełnia wymogi ustanowione w sekcji 2. Organ nadzoru rynku informuje Komisję i pozostałe państwa członkowskie o wszelkich zezwoleniach wydanych zgodnie z ust. 1. ***Obowiązek ten nie obejmuje szczególnie chronionych danych operacyjnych dotyczących działań organów ścigania.***

4. Jeżeli w terminie 15 dni kalendarzowych od dnia otrzymania informacji, o której mowa w ust. 3, 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.

5. W przypadku gdy w terminie 15 dni kalendarzowych od dnia otrzymania informacji, o której mowa w ust. 3, państwo członkowskie zgłosi zastrzeżenia dotyczące zezwolenia wydanego przez organ nadzoru rynku innego państwa członkowskiego lub w przypadku gdy Komisja uzna zezwolenie za sprzeczne z prawem Unii lub uzna za bezpodstawne dokonane przez państwo członkowskie stwierdzenie zgodności systemu z wymogami, o czym mowa w ust. 3, 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. Komisja kieruje swoją decyzję do zainteresowanego państwa członkowskiego i zainteresowanych operatorów.

6. W przypadku gdy Komisja uzna zezwolenie za bezpodstawne, zostaje ono wycofane przez organ nadzoru rynku zainteresowanego państwa członkowskiego.

7. W przypadku systemów AI wysokiego ryzyka ***powiązanych z produktami*** objętymi zakresem stosowania ***unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A zastosowanie mają wyłącznie odstępstwa od oceny zgodności ustanowione w tym unijnym prawodawstwie harmonizacyjnym.***

Artykuł 47

Deklaracja zgodności UE

1. Dostawca sporządza pisemną i ***nadającą się do odczytu maszynowego, podpisaną fizycznie lub elektronicznie,*** deklarację zgodności UE dla każdego systemu AI ***wysokiego ryzyka*** i przechowuje ją do dyspozycji właściwych organów krajowych przez okres 10 lat od dnia wprowadzenia systemu AI ***wysokiego ryzyka*** do obrotu lub oddania go do użytku. W deklaracji zgodności UE wskazuje się system AI ***wysokiego ryzyka***, dla którego ją sporządzono. Kopię deklaracji zgodności UE ***przedkłada się*** odpowiednim właściwym organom krajowym na ich żądanie.

2. W deklaracji zgodności UE potwierdza się, że dany system AI wysokiego ryzyka spełnia wymogi ustanowione w sekcji 2. Deklaracja zgodności UE zawiera informacje przedstawione w załączniku V i musi zostać przetłumaczona na ***język łatwo zrozumiały*** dla ***właściwych organów krajowych*** państw członkowskich, w których dany system AI wysokiego ryzyka jest ***wprowadzany do obrotu lub*** udostępniany.

3. W przypadku gdy systemy AI 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 AI 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 sekcji 2. Dostawca odpowiednio zapewnia aktualność deklaracji zgodności UE.

5. Komisja przyjmuje akty delegowane zgodnie z art. 97, aby zaktualizować treść deklaracji zgodności UE określoną w załączniku V w celu wprowadzenia elementów, które stały się konieczne z uwagi na postęp techniczny.

Artykuł 48

Oznakowanie CE

1. Oznakowanie CE ***podlega ogólnym zasadom określonym w art. 30 rozporządzenia (WE) nr 765/2008.***

2. ***W przypadku systemów AI wysokiego ryzyka dostarczanych cyfrowo cyfrowe oznakowanie CE stosuje się wyłącznie wtedy, gdy można do niego łatwo dotrzeć za pośrednictwem interfejsu, poprzez który uzyskuje się dostęp do tego systemu, lub za pomocą łatwo dostępnego kodu nadającego się do odczytu maszynowego lub innych środków elektronicznych.***

3. Oznakowanie CE ***umieszcza się na systemie AI wysokiego ryzyka w sposób widoczny, czytelny i trwały. W przypadku gdy z uwagi na charakter systemu AI wysokiego ryzyka oznakowanie systemu w powyższy sposób nie jest możliwe lub pożądane, oznakowanie to umieszcza się na opakowaniu lub – w stosownych przypadkach – w dokumentacji towarzyszącej systemowi.***

4. W stosownych przypadkach oznakowaniu CE towarzyszy również numer identyfikacyjny jednostki notyfikowanej odpowiedzialnej za przeprowadzenie procedur oceny zgodności ustanowionych w art. 43. Numer identyfikacyjny ***jednostki notyfikowanej umieszcza sama jednostka lub dostawca lub jego upoważniony przedstawiciel według wskazówek jednostki notyfikowanej. Numer identyfikacyjny*** umieszcza się również na wszelkich materiałach promocyjnych zawierających informacje o tym, że system AI wysokiego ryzyka spełnia wymogi konieczne do opatrzenia go oznakowaniem CE.

5. ***W przypadku gdy systemy AI wysokiego ryzyka podlegają innym przepisom Unii, które również przewidują umieszczenie oznakowania CE, oznakowanie CE wskazuje, że dany system AI wysokiego ryzyka spełnia także wymogi zawarte w tych innych przepisach.***

Artykuł 49

Rejestracja

1. Przed wprowadzeniem do obrotu jednego z systemów AI wysokiego ryzyka ***wymienionych w załączniku III, z wyjątkiem systemów AI wysokiego ryzyka***, o których mowa w ***załączniku III pkt 2***, lub przed oddaniem go do użytku dostawca lub – w stosownych przypadkach – jego upoważniony przedstawiciel rejestrują ***siebie i swój*** system w unijnej bazie danych, o której mowa w art. 71.

2. ***Przed wprowadzeniem do obrotu lub oddaniem do użytku systemu AI, co do którego dostawca stwierdził, że nie jest systemem wysokiego ryzyka zgodnie z art. 6 ust. 3, dostawca ten lub – w stosownych przypadkach – jego upoważniony przedstawiciel rejestrują siebie i swój system w unijnej bazie danych, o której mowa w art. 71.***

3. ***Przed oddaniem do użytku lub wykorzystaniem systemu AI wysokiego ryzyka wymienionego w załączniku III, z wyjątkiem systemów AI wysokiego ryzyka wymienionych w załączniku III pkt 2, podmioty stosujące AI będące publicznymi organami, agencjami lub jednostkami organizacyjnymi lub osobami działającymi w ich imieniu rejestrują się w unijnej bazie danych, o której mowa w art. 71, wybierają system, z którego zamierzają skorzystać i rejestrują jego wykorzystanie.***

4. ***W przypadku systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7, w obszarach ścigania przestępstw, migracji, azylu i zarządzania kontrolą graniczną, rejestracja, o której mowa w ust. 1, 2 i 3 niniejszego artykułu, ma miejsce w bezpiecznej niepublicznej sekcji unijnej bazy danych, o której mowa w art. 71, i – stosownie do przypadku – zawiera wyłącznie następujące informacje, o których mowa w:***

   a) załącznik VIII sekcja A pkt 1–10, z wyjątkiem pkt 5a, 7 i 8;

   b) załącznik VIII sekcja C pkt 1–3;

   c) załącznik VIII sekcja B ***pkt 1–5 oraz pkt 8 i 9;***

   d) załącznik IX pkt 1–3 oraz pkt 5.

   Do zastrzeżonych sekcji unijnej bazy danych wymienionych w akapicie pierwszym niniejszego ustępu dostęp mają jedynie Komisja i organy krajowe, o których mowa w art. 74 ust. 8.

5. Systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 2, rejestruje się na szczeblu krajowym.

ROZDZIAŁ IV

OBOWIĄZKI W ZAKRESIE PRZEJRZYSTOŚCI DLA *DOSTAWCÓW I PODMIOTÓW STOSUJĄCYCH* NIEKTÓRE SYSTEMY AI

Artykuł 50

Obowiązki w zakresie przejrzystości dla dostawców i użytkowników niektórych systemów AI

1. Dostawcy zapewniają, aby systemy AI przeznaczone do wchodzenia w ***bezpośrednią*** interakcję z osobami fizycznymi projektowano i opracowywano w taki sposób, aby ***zainteresowane*** osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem AI, chyba że jest to oczywiste z ***punktu widzenia osoby fizycznej, która jest dostatecznie poinformowana, uważna i ostrożna, z uwzględnieniem*** okoliczności i kontekstu korzystania. Obowiązek ten nie ma zastosowania do systemów AI zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia postępowań przygotowawczych w związku z przestępstwami lub ścigania ich sprawców, z ***zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich***, chyba że systemy te udostępnia się ogółowi społeczeństwa na potrzeby składania zawiadomień o popełnieniu przestępstwa.

2. ***Dostawcy systemów AI, w tym systemów AI ogólnego zastosowania, generujących treści w postaci syntetycznych dźwięków, obrazów, wideo lub tekstu, zapewniają, aby wyniki działania systemu AI zostały oznakowane w formacie nadającym się do odczytu maszynowego i były wykrywalne jako sztucznie wygenerowane lub zmanipulowane. Dostawcy zapewniają skuteczność, interoperacyjność, solidność i niezawodność swoich rozwiązań technicznych w zakresie, w jakim jest to technicznie wykonalne, uwzględniając przy tym specyfikę i ograniczenia różnych rodzajów treści, koszty wdrażania oraz powszechnie uznany stan wiedzy technicznej, co może być odzwierciedlone w odpowiednich normach technicznych. Obowiązek ten nie ma zastosowania w zakresie, w jakim systemy AI pełnią funkcję wspomagającą w zakresie standardowej edycji lub nie zmieniają w istotny sposób przekazywanych przez podmiot stosujący AI danych wejściowych lub ich semantyki, ani w zakresie, w jakim jest to dozwolone na mocy prawa do celów wykrywania przestępstw, zapobiegania im, prowadzenia postępowań przygotowawczych w ich sprawie lub ścigania sprawców.***

3. ***Podmioty stosujące*** systemy rozpoznawania emocji lub systemy kategoryzacji biometrycznej informują osoby fizyczne, wobec których systemy te są stosowane, o fakcie ich stosowania ***i przetwarzają dane osobowe zgodnie z rozporządzeniami (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywą 2016/680, stosownie do przypadku.*** Obowiązek ten nie ma zastosowania do zatwierdzonych z mocy prawa systemów AI wykorzystywanych do ***kategoryzacji*** biometrycznej ***i rozpoznawania emocji*** do celów wykrywania przestępstw, przeciwdziałania przestępstwom i prowadzenia postępowań przygotowawczych w związku z przestępstwami, ***z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich oraz zgodnie z prawem Unii.***

4. ***Podmioty stosujące*** system AI, który generuje obrazy, treści audio lub wideo ***stanowiące treści deepfake lub który manipuluje takimi obrazami lub treściami, ujawniają, że treści te zostały sztucznie wygenerowane lub poddane manipulacji. Obowiązek ten nie ma zastosowania, w przypadku gdy wykorzystywanie jest dozwolone na mocy prawa w celu wykrywania przestępstw, zapobiegania im, prowadzenia postępowań przygotowawczych lub ścigania sprawców. W przypadku gdy treść stanowi część pracy lub programu o wyraźnie artystycznym, twórczym, satyrycznym, fikcyjnym lub analogicznym charakterze obowiązki w zakresie przejrzystości określone w niniejszym ustępie ograniczają się do ujawnienia istnienia takich*** wygenerowanych lub zmanipulowanych ***treści w odpowiedni sposób, który nie utrudnia wyświetlania lub korzystania z utworu.***

Podmioty stosujące system AI, który generuje tekst publikowany w celu informowania społeczeństwa o sprawach leżących w interesie publicznym lub manipuluje takim tekstem, ujawniają, że tekst został sztucznie wygenerowany lub poddany manipulacji. Obowiązek ten nie ma zastosowania, w przypadku gdy wykorzystywanie jest dozwolone na mocy prawa w celu wykrywania przestępstw, zapobiegania im, prowadzenia postępowań przygotowawczych lub ścigania sprawców ***lub w przypadku gdy treści wygenerowane przez AI zostały poddane procesowi weryfikacji przez człowieka lub kontroli redakcyjnej i gdy za publikację treści odpowiedzialność redakcyjną ponosi osoba fizyczna lub prawna.***

5. ***Informacje, o których mowa w ust. 1–4, są przekazywane zainteresowanym osobom fizycznym w jasny i wyraźny sposób, najpóźniej w momencie pierwszej interakcji lub kontaktu. Informacje te muszą spełniać mające zastosowanie wymogi w zakresie dostępności.***

6. Ust. 1–4 nie mają wpływu na wymogi i obowiązki określone w rozdziale III ***i pozostają bez uszczerbku dla innych obowiązków w zakresie przejrzystości ustanowionych w prawie Unii lub prawie krajowym w odniesieniu do podmiotów stosujących systemy AI.***

7. ***Urząd ds. AI wspiera i ułatwia opracowywanie kodeksów praktyk na szczeblu Unii, aby ułatwić skuteczne wykonywanie obowiązków w zakresie wykrywania i oznaczania treści sztucznie wygenerowanych lub poddanych manipulacji. Komisja jest uprawniona do przyjmowania aktów wykonawczych dotyczących zatwierdzenia tych kodeksów praktyk zgodnie z procedurą ustanowioną w art. 56 ust. 6, 7 i 8. Jeżeli Komisja uzna, że kodeks nie jest odpowiedni, jest zgodnie z procedurą sprawdzającą ustanowioną w art. 98 ust. 2 uprawniona do przyjęcia aktu wykonawczego określającego wspólne zasady wykonywania tych obowiązków.***

ROZDZIAŁ V
MODELE AI OGÓLNEGO PRZEZNACZENIA

Sekcja 1
Zasady klasyfikacji

Artykuł 51
Klasyfikacja modeli AI ogólnego przeznaczenia jako modeli AI ogólnego przeznaczenia z ryzykiem systemowym

1. Model AI ogólnego przeznaczenia jest klasyfikowany jako model AI ogólnego przeznaczenia z ryzykiem systemowym, jeżeli spełnia którekolwiek z następujących kryteriów:

a) ma zdolności dużego oddziaływania ocenione w oparciu o odpowiednie narzędzia i metodologie techniczne, w tym wskaźniki i poziomy odniesienia;

b) w oparciu o decyzję Komisji – z urzędu lub w następstwie ostrzeżenia kwalifikowanego wydanego przez panel naukowy – ma zdolności lub oddziaływanie równoważne z tymi, które określono w lit. a), przy uwzględnieniu kryteriów określonych w załączniku XIII.

2. Model AI ogólnego przeznaczenia uznaje się za mający zdolności dużego oddziaływania zgodnie z ust. 1 lit. a), jeśli łączna liczba obliczeń wykorzystywanych do jego trenowania mierzona we FLOP jest większa niż 10^25.

3. Komisja przyjmuje akty delegowane zgodnie z art. 97 w celu zmiany progów wymienionych w ust. 2 i 3 niniejszego artykułu, a także w celu uzupełnienia poziomów odniesienia i wskaźników w świetle rozwoju technologicznego obejmującego na przykład ulepszenia algorytmiczne lub zwiększoną wydajność sprzętu, w miarę konieczności, by progi te odzwierciedlały aktualny stan techniki.

Artykuł 52

Procedura

1. W przypadku gdy model AI ogólnego przeznaczenia spełnia kryteria, o których mowa w art. 51 ust. 1 lit. a), odpowiedni dostawca powiadamia Komisję niezwłocznie, a w każdym przypadku w ciągu dwóch tygodni od spełnienia tego kryterium lub od kiedy wiadomo, że zostanie on spełniony. Powiadomienie to zawiera informacje niezbędne do wykazania, że dane kryterium jest spełnione. Jeśli Komisja dowie się o stwarzającym ryzyko systemowe modelu AI ogólnego przeznaczenia, o którym nie została powiadomiona, może zdecydować o uznaniu go za model z ryzykiem systemowym.

2. Dostawca spełniającego kryterium, o którym mowa w art. 51 ust. 1 lit. a), modelu AI ogólnego przeznaczenia z ryzykiem systemowym może wraz ze swoim zgłoszeniem przedstawić wystarczająco uzasadnione argumenty wykazujące, że wyjątkowo, pomimo spełniania przez ten model AI ogólnego przeznaczenia przedmiotowego kryterium, nie stwarza on – z uwagi na swoje szczególne cechy – ryzyka systemowego i nie powinien być w związku z tym klasyfikowany jako model AI ogólnego przeznaczenia z ryzykiem systemowym.

3. W przypadku gdy Komisja stwierdzi, że argumenty przedstawione zgodnie z ust. 2 nie są wystarczająco uzasadnione i że dany dostawca nie był w stanie wykazać, że dany model AI ogólnego przeznaczenia nie stwarza – z uwagi na swoje szczególne cechy – ryzyka systemowego, odrzuca te argumenty i dany model AI ogólnego przeznaczenia zostaje uznany za model AI ogólnego przeznaczenia z ryzykiem systemowym.

4. Komisja może – z urzędu lub w następstwie ostrzeżenia kwalifikowanego wydanego przez panel naukowy zgodnie z art. 90 ust. 1 lit. a) – uznać model AI ogólnego przeznaczenia za model stwarzający ryzyko systemowe na podstawie kryteriów określonych w załączniku XIII.

Komisja przyjmuje akty delegowane zgodnie z art. 97 w celu określenia i aktualizacji kryteriów określonych w załączniku XIII.

5. Na uzasadniony wniosek dostawcy, którego model został zgodnie z ust. 4 uznany za model AI ogólnego przeznaczenia z ryzykiem systemowym, Komisja odnosi się do tego wniosku i może zdecydować o ponownej ocenie w celu stwierdzenia, czy dany model AI ogólnego przeznaczenia może być nadal uznawany za stwarzający ryzyko systemowe na podstawie kryteriów określonych w załączniku XIII. Wniosek taki zawiera obiektywne, szczegółowe i nowe powody, które pojawiły się po podjęciu decyzji o uznaniu. Dostawcy mogą zwrócić się o ponowną ocenę najwcześniej sześć miesięcy po podjęciu decyzji o uznaniu. W przypadku gdy w wyniku ponownej oceny Komisja zdecyduje się utrzymać klasyfikację modelu AI ogólnego przeznaczenia z ryzykiem systemowym, dostawcy mogą zwrócić się o ponowną ocenę najwcześniej sześć miesięcy po tej decyzji.

6. Komisja zapewnia publikację i aktualizację wykazu modeli AI ogólnego przeznaczenia z ryzykiem systemowym, bez uszczerbku dla konieczności przestrzegania i ochrony praw własności intelektualnej oraz poufnych informacji handlowych lub tajemnic przedsiębiorstwa zgodnie z prawem Unii i prawem krajowym.

Sekcja 2

Obowiązki dostawców modeli AI ogólnego przeznaczenia

Artykuł 53

Obowiązki dostawców modeli AI ogólnego przeznaczenia

1. Dostawcy modeli AI ogólnego przeznaczenia:

a) sporządzają i aktualizują dokumentację techniczną modelu, w tym proces jego trenowania i testowania oraz wyniki jego oceny, zawierającą jako minimum elementy określone w załączniku XI do celów przekazania jej, na życzenie, Urzędowi ds. AI i właściwym organom krajowym;

b) sporządzają, aktualizują i udostępniają informacje i dokumentację dostawcom systemów AI, którzy zamierzają zintegrować dany model AI ogólnego przeznaczenia ze swoimi systemami AI. Bez uszczerbku dla potrzeby poszanowania i ochrony praw własności intelektualnej i poufnych informacji handlowych lub tajemnic przedsiębiorstwa zgodnie prawem Unii i prawem krajowym te informacje i dokumentacja:

(i) umożliwiają dostawcom systemów AI dobre zrozumienie możliwości i ograniczeń danego modelu AI ogólnego przeznaczenia oraz wypełnianie ich obowiązków zgodnie z niniejszym rozporządzeniem; oraz

(ii) zawierają co najmniej elementy określone w załączniku XII;

c) wprowadzają politykę służącą zapewnieniu zgodności z unijnym prawem autorskim, w szczególności z myślą o identyfikacji i przestrzeganiu, w tym poprzez najnowocześniejsze technologie, zastrzeżenia praw wyrażonego zgodnie z art. 4 ust. 3 dyrektywy (UE) 2019/790;

d) sporządzają i podają do wiadomości publicznej wystarczająco szczegółowe streszczenie na temat treści wykorzystanych do trenowania danego modelu AI ogólnego przeznaczenia, zgodnie ze wzorem dostarczonym przez Urząd ds. AI.

2. Obowiązki określone w ust. 1 lit. a) i b) nie dotyczą dostawców modeli AI, które są udostępniane na podstawie bezpłatnej i otwartej licencji umożliwiającej dostęp, wykorzystanie, modyfikację i dystrybucję modelu i których parametry, w tym wagi, informacje o architekturze modelu oraz informacje o wykorzystaniu modelu są podawane do wiadomości publicznej. Wyjątek ten nie dotyczy modeli AI ogólnego przeznaczenia z ryzykiem systemowym.

3. Dostawcy modeli AI ogólnego przeznaczenia współpracują w razie konieczności z Komisją i właściwymi organami krajowymi przy wykonywaniu ich kompetencji i uprawnień zgodnie z niniejszym rozporządzeniem.

4. Do czasu opublikowania normy zharmonizowanej dostawcy modeli AI ogólnego przeznaczenia mogą opierać się na kodeksach praktyk w rozumieniu art. 56 w celu wykazania spełnienia obowiązków określonych w ust. 1 niniejszego artykułu. Uznaje się, że dostawcy, którzy spełniają wymogi europejskiej normy zharmonizowanej, spełniają obowiązki określone w ust. 1 niniejszego artykułu. Dostawcy modeli AI ogólnego przeznaczenia, którzy nie zobowiązują się do przestrzegania zatwierdzonego kodeksu praktyk, przedstawiają Komisji do zatwierdzenia adekwatne alternatywne środki służące zapewnieniu zgodności.

5. Do celu ułatwienia zgodności z załącznikiem XI, w szczególności jego pkt 2 lit. d) i e), Komisja przyjmuje zgodnie z art. 97 akty delegowane dotyczące szczegółowego określenia metod pomiaru i obliczeń umożliwiających porównywalną i weryfikowalną dokumentację.

6. Komisja przyjmuje akty delegowane zgodnie z art. 97 ust. 2 w celu zmiany załączników XI i XII ▌ w świetle postępu technicznego.

7. Wszelkie informacje lub dokumentację uzyskane zgodnie z niniejszym artykułem, w tym tajemnice przedsiębiorstwa, traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 78.

Artykuł 54

Upoważnieni przedstawiciele dostawców modeli AI ogólnego przeznaczenia

1. *Przed wprowadzeniem swoich modeli AI ogólnego przeznaczenia do obrotu w Unii dostawcy mający siedzibę w państwach trzecich wyznaczają – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego siedzibę w Unii.*

2. *Dostawca umożliwia swojemu upoważnionemu przedstawicielowi wykonywanie zadań powierzonych mu na mocy pełnomocnictwa udzielonego przez dostawcę.*

2. *Upoważniony przedstawiciel wykonuje zadania powierzone mu na mocy pełnomocnictwa udzielonego przez dostawcę. Na żądanie przekazuje on Urzędowi ds. AI kopię pełnomocnictwa w jednym z oficjalnych języków instytucji Unii. Do celów niniejszego rozporządzenia pełnomocnictwo uprawnia upoważnionego przedstawiciela do wykonywania następujących zadań:*

   a) *sprawdzenie, czy dostawca sporządził dokumentację techniczną określoną w załączniku XI oraz czy wypełnił wszystkie obowiązki, o których mowa w art. 53, oraz, w stosownych przypadkach, w art. 55;*

   b) *przechowywanie kopii dokumentacji technicznej określonej w załączniku XI do dyspozycji Urzędu ds. AI i właściwych organów krajowych przez okres 10 lat od czasu wprowadzenia danego modelu AI ogólnego przeznaczenia do obrotu oraz dysponowanie aktualnymi danymi kontaktowymi dostawcy, który wyznaczył danego upoważnionego przedstawiciela;*

c) przekazywanie Urzędowi ds. AI na uzasadniony wniosek wszystkich informacji i dokumentacji, w tym określonych w lit. b), niezbędnych do wykazania wypełniania przez niego obowiązków ustanowionych w niniejszym rozdziale;

d) współpraca z Urzędem ds. AI i właściwymi organami krajowymi, na uzasadniony wniosek, we wszelkich podejmowanych przez nie działaniach odnoszących się do modelu AI ogólnego przeznaczenia z ryzykiem systemowym, w tym kiedy model ten jest zintegrowany z systemami AI wprowadzanymi do obrotu lub oddawanymi do użytku w Unii.

3. Pełnomocnictwo daje upoważnionemu przedstawicielowi prawo do tego, aby Urząd ds. AI lub właściwe organy krajowe mogły się zwracać do niego, obok albo zamiast do dostawcy, we wszystkich kwestiach dotyczących zapewnienia zgodności z niniejszym rozporządzeniem.

4. Upoważniony przedstawiciel wypowiada pełnomocnictwo, jeśli sądzi lub ma powody sądzić, że dostawca działa w sposób sprzeczny z jego obowiązkami wynikającymi z niniejszego rozporządzenia. W takim przypadku informuje on również niezwłocznie Urząd ds. AI o wypowiedzeniu pełnomocnictwa i o jego przyczynach.

5. Obowiązek określony w niniejszym artykule nie dotyczy dostawców modeli AI ogólnego przeznaczenia, które są udostępniane na podstawie bezpłatnej i otwartej licencji umożliwiającej dostęp, wykorzystanie, modyfikację i dystrybucję modelu i których parametry, w tym wagi, informacje o architekturze modelu oraz informacje o wykorzystaniu modelu są podawane do wiadomości publicznej, chyba że te modele AI ogólnego przeznaczenia stwarzają ryzyko systemowe.

Sekcja 3

Obowiązki dostawców modeli AI ogólnego przeznaczenia z ryzykiem systemowym

Artykuł 55

Obowiązki dostawców modeli AI ogólnego przeznaczenia z ryzykiem systemowym

1. Oprócz obowiązków wymienionych w art. 53 dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym:

a) dokonują oceny modelu zgodnie ze znormalizowanymi protokołami i narzędziami odzwierciedlającymi najaktualniejszy stan wiedzy technicznej, w tym przeprowadzają i dokumentują kontradyktoryjne testy modelu z myślą o zidentyfikowaniu ryzyka systemowego i jego ograniczenia;

b) oceniają i ograniczają ewentualne ryzyko systemowe na poziomie Unii, w tym jego źródła, które może wynikać z opracowywania, wprowadzania do obrotu lub wykorzystywania modeli AI ogólnego przeznaczenia z ryzykiem systemowym;

c) rejestrują, dokumentują i niezwłocznie zgłaszają Urzędowi ds. AI oraz, w stosownych przypadkach, właściwym organom krajowym odpowiednie informacje dotyczące poważnych incydentów i ewentualnych środków naprawczych służących zaradzeniu im;

d) zapewniają odpowiedni poziom cyberochrony modelu AI ogólnego przeznaczenia z ryzykiem systemowym oraz infrastruktury fizycznej tego modelu.

2. Do czasu opublikowania normy zharmonizowanej dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym mogą opierać się na kodeksach praktyk w rozumieniu art. 56 w celu wykazania spełnienia obowiązków określonych w ust. 1 niniejszego artykułu. Uznaje się, że dostawcy, którzy spełniają wymogi europejskiej normy zharmonizowanej, spełniają obowiązki określone w ust. 1 niniejszego artykułu. Dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym, którzy nie zobowiązują się do przestrzegania zatwierdzonego kodeksu praktyk, przedstawiają Komisji do zatwierdzenia adekwatne alternatywne środki służące zapewnieniu zgodności.

3. Wszelkie informacje lub dokumentację uzyskane zgodnie z niniejszym artykułem, w tym tajemnice przedsiębiorstwa, traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 78.

Artykuł 56

Kodeksy praktyk

1. ***Urząd ds. AI zachęca do sporządzania kodeksów praktyk na szczeblu Unii i ułatwia ich sporządzanie w celu przyczyniania się do właściwego stosowania niniejszego rozporządzenia, przy uwzględnieniu podejść międzynarodowych.***

2. ***Urząd ds. AI i Rada ds. AI dążą do zapewnienia, by kodeksy praktyk obejmowały co najmniej obowiązki przewidziane w art. 53 i 55, w tym następujące kwestie:***

a) ***środki na rzecz zapewnienia, by informacje, o których mowa w*** art. 53 ust. 1 lit. a) i b), ***były aktualne w świetle rozwoju rynku i technologii;***

b) ***odpowiedni poziom szczegółowości streszczenia na temat treści wykorzystywanych do trenowania;***

c) ***identyfikacja rodzaju i charakteru ryzyka systemowego na szczeblu Unii, w tym, w stosownych przypadkach, jego źródła;***

d) środki, procedury i sposoby oceny ryzyka systemowego i zarządzania nim na szczeblu Unii, w tym ich dokumentacja, które muszą być proporcjonalne do ryzyka, uwzględniać jego stopień ciężkości i prawdopodobieństwo oraz uwzględniać szczególne wyzwania w zakresie radzenia sobie z tym ryzykiem w świetle potencjalnych sposobów pojawienia się takie ryzyka i jego urzeczywistnienia w łańcuchu wartości AI.

3. Urząd ds. AI może zachęcić wszystkich dostawców modeli AI ogólnego przeznaczenia oraz odpowiednie właściwe organy krajowe do udziału w opracowywaniu kodeksów praktyk. Organizacje społeczeństwa obywatelskiego, przedstawiciele przemysłu, środowisko akademickie oraz inne odpowiednie zainteresowane strony, takie jak dostawcy niższego szczebla i niezależni eksperci, mogą wspierać ten proces.

4. Urząd ds. AI i Rada ds. AI starają się zapewnić, by kodeksy praktyk wyraźnie określały swoje cele szczegółowe i zawierały zobowiązania lub środki, w tym, w stosownych przypadkach, kluczowe wskaźniki skuteczności działania zapewniające realizację tych celów, oraz by uwzględniały w należytym stopniu potrzeby i interesy wszystkich zainteresowanych stron, w tym osób, na które AI ma wpływ, na szczeblu Unii.

5. Urząd ds. AI stara się zapewnić, by uczestnicy kodeksów praktyk regularnie składali Urzędowi ds. AI sprawozdania z realizacji podjętych zobowiązań i środków oraz z ich wyników, w tym, w odpowiednich przypadkach, mierzonych w odniesieniu do kluczowych wskaźników skuteczności działania. Kluczowe wskaźniki skuteczności działania i zobowiązania w zakresie sprawozdawczości są adekwatne do różnic w wielkości i zdolnościach poszczególnych uczestników.

6. Urząd ds. AI i Rada ds. AI regularnie monitorują i oceniają realizację przez uczestników celów kodeksów praktyk oraz wkład tych kodeksów w należyte stosowanie niniejszego rozporządzenia. Urząd ds. AI i Rada ds. AI oceniają, czy kodeksy praktyk obejmują swoim zakresem obowiązki przewidziane w art. 53 i 55 oraz zagadnienia wymienione w ust. 2 niniejszego artykułu, i regularnie monitorują i oceniają realizację ich celów. Swoją ocenę adekwatności kodeksów praktyk podają do wiadomości publicznej.

Komisja może w drodze aktu wykonawczego zatwierdzić kodeks praktyk i nadać mu ogólną ważność w Unii. Taki akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

7. Urząd ds. AI może zachęcać wszystkich dostawców modeli AI ogólnego przeznaczenia, by przestrzegali kodeksów praktyk. W przypadku dostawców modeli AI ogólnego przeznaczenia, które nie stwarzają ryzyka systemowego, przestrzeganie kodeksów może być ograniczone do obowiązków przewidzianych w art. 53, chyba że wyraźnie zadeklarują oni zainteresowanie przystąpieniem do pełnego kodeksu.

8. Urząd ds. AI w stosownych przypadkach zachęca również i ułatwia prowadzenie przeglądów i dostosowywanie kodeksów praktyk, w szczególności w świetle nowych norm. Urząd ds. AI udziela wsparcia w ocenie dostępnych norm.

9. Kodeksy praktyk będą gotowe najpóźniej do dnia ... [dziewięć miesięcy od daty wejścia w życie niniejszego rozporządzenia] r. Urząd ds. AI podejmuje niezbędne kroki, w tym kieruje zachęty do dostawców zgodnie z ust. 7.

Jeśli do dnia ... [12 miesięcy od daty wejścia w życie] kodeks praktyk nie może zostać ukończony lub Urząd ds. AI w wyniku swojej oceny *na podstawie ust. 6 niniejszego artykułu uzna, że nie jest on odpowiedni, Komisja może w drodze aktów wykonawczych ustanowić wspólne przepisy dotyczące wdrażania obowiązków przewidzianych w art. 53 i 55, z uwzględnieniem kwestii określonych w ust. 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.*

ROZDZIAŁ VI
ŚRODKI WSPIERAJĄCE INNOWACYJNOŚĆ

Artykuł 57

Piaskownice regulacyjne w zakresie AI

1. ***Państwa członkowskie zapewniają, by ich właściwe organy ustanowiły na szczeblu krajowym przynajmniej jedną piaskownicę regulacyjną w zakresie AI, która zostanie uruchomiona do dnia ... [24 miesiące od daty wejścia w życie niniejszego rozporządzenia]. Piaskownica ta może zostać ustanowiona wspólnie z właściwymi organami innego państwa członkowskiego lub większej ich liczby. Komisja może zapewniać wsparcie techniczne, doradztwo i narzędzia do celów ustanowienia i funkcjonowania piaskownic regulacyjnych w zakresie AI.***

   Obowiązek określony w akapicie pierwszym może również zostać wypełniony poprzez uczestnictwo w istniejącej piaskownicy w zakresie, w jakim udział ten przewiduje równoważny poziom zasięgu krajowego dla uczestniczących państw członkowskich.

2. Można również ustanowić dodatkowe piaskownice regulacyjne w zakresie AI na szczeblu regionalnym lub lokalnym lub wspólnie z właściwymi organami innych państw członkowskich.

3. Europejski Inspektor Ochrony Danych może również ustanowić piaskownicę regulacyjną w zakresie AI dla instytucji, organów i jednostek organizacyjnych Unii i może pełnić role i wykonywać zadania właściwych organów krajowych zgodnie z niniejszym rozdziałem.

4. Państwa członkowskie zapewniają, by właściwe organy, o których mowa w ust. 1 i 2, przeznaczały wystarczające zasoby do skutecznego i terminowego osiągnięcia zgodności z niniejszym artykułem. W stosownych przypadkach właściwe organy krajowe współpracują z innymi odpowiednimi organami i mogą zezwolić na zaangażowanie innych podmiotów z ekosystemu AI. Niniejszy artykuł nie ma wpływu na inne piaskownice regulacyjne ustanowione zgodnie z prawem unijnym lub krajowym. Państwa członkowskie zapewniają odpowiedni poziom współpracy między organami nadzorującymi te inne piaskownice a właściwymi organami krajowymi.

5. ***Piaskownice regulacyjne w zakresie AI ustanowione na podstawie ust. 1 zapewniają kontrolowane środowisko sprzyjające innowacjom oraz ułatwiające opracowywanie, trenowanie, testowanie i walidację innowacyjnych systemów AI przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem ich do użytku zgodnie z określonym planem działania piaskownicy uzgodnionym między potencjalnymi dostawcami a właściwym organem. Takie piaskownice regulacyjne mogą obejmować testy w warunkach rzeczywistych nadzorowane w ramach danej piaskownicy.***

6. ***Właściwe organy zapewniają, w stosownych przypadkach, wskazówki, nadzór i wsparcie w ramach piaskownicy regulacyjnej w zakresie AI, mając na celu identyfikację ryzyka, w szczególności dla praw podstawowych, zdrowia i bezpieczeństwa, testowania, środków zaradczych oraz ich skuteczności w odniesieniu do obowiązków i wymogów niniejszego rozporządzenia oraz, w stosownych przypadkach, innych nadzorowanych w ramach danej piaskownicy przepisów Unii i państw członkowskich.***

7. ***Właściwe organy zapewniają dostawcom i potencjalnym dostawcom*** korzystającym z piaskownicy regulacyjnej w zakresie AI ***wskazówki dotyczące oczekiwań regulacyjnych oraz sposobów realizacji wymogów i obowiązków określonych w niniejszym rozporządzeniu.***

Na wniosek dostawcy lub potencjalnego dostawcy systemu AI właściwy organ przygotowuje pisemny dowód skutecznie przeprowadzonych w ramach piaskownicy działań. Właściwy organ przygotowuje również sprawozdanie końcowe zawierające szczegółowe informacje na temat działań przeprowadzonych w ramach piaskownicy oraz powiązanych wyników i efektów uczenia się. Dostawcy mogą wykorzystywać taką dokumentację do wykazania swojej zgodności z niniejszym rozporządzeniem w ramach procesu oceny zgodności lub odpowiednich działań z zakresu nadzoru rynku. W tym względzie sprawozdania końcowe oraz pisemne dowody przedstawione przez właściwy organ krajowy są uwzględniane jako pozytywny dowód przez organy nadzoru rynku i jednostki notyfikowane, z myślą o przyspieszeniu procedur oceny zgodności w rozsądnym zakresie.

8. *Z zastrzeżeniem przepisów dotyczących poufności określonych w art. 78 i za zgodą dostawcy lub potencjalnego dostawcy Komisja i Rada ds. AI są upoważnione, by uzyskać dostęp do sprawozdań końcowych i – w stosownych przypadkach – uwzględniają je przy wykonywaniu swoich zadań na podstawie niniejszego rozporządzenia. Jeżeli zarówno dostawca lub przyszły dostawca, jak i właściwy organ krajowy wyraźnie wyrażą na to zgodę, sprawozdanie końcowe może zostać podane do wiadomości publicznej za pośrednictwem jednolitej platformy informacyjnej, o której mowa w niniejszym artykule.*

9. *Ustanowienie piaskownic regulacyjnych w zakresie AI ma na celu przyczynienie się do osiągnięcia następujących celów:*

   a) *zwiększenie pewności prawa z myślą o osiągnięciu zgodności regulacyjnej z niniejszym rozporządzeniem lub, w stosownych przypadkach, innym mającym zastosowanie prawem unijnym i krajowym;*

b) wspieranie wymiany najlepszych praktyk poprzez współpracę z organami uczestniczącymi w piaskownicy regulacyjnej w zakresie AI;

c) wzmacnianie innowacyjności i konkurencyjności oraz ułatwianie rozwoju ekosystemu AI;

d) wniesienie wkładu w oparte na dowodach uczenie się działań regulacyjnych;

e) ułatwianie i przyspieszanie dostępu do unijnego rynku dla systemów AI, w szczególności gdy są one dostarczane przez MŚP, w tym przedsiębiorstwa typu start-up.

10. ***Właściwe organy krajowe*** zapewniają, aby – w zakresie, w jakim innowacyjne systemy AI 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 osobowych lub wsparcie w uzyskaniu dostępu do tych danych – krajowe organy ochrony danych oraz te inne organy krajowe włączono w działalność piaskownicy regulacyjnej w zakresie AI ***oraz zaangażowano w kontrolę nad tymi aspektami w zakresie wynikającym z ich odpowiednich zadań i uprawnień.***

11. Piaskownice regulacyjne w zakresie AI pozostaje bez wpływu na uprawnienia w zakresie nadzoru lub stosowania środków naprawczych przynależne właściwym organom ***nadzorującym te piaskownice, w tym na szczeblu regionalnym lub lokalnym.*** Stwierdzenie istnienia jakiegokolwiek istotnego ryzyka dla zdrowa i bezpieczeństwa oraz dla praw podstawowych na etapie opracowywania i testowania takich systemów ***AI*** powoduje konieczność ***właściwego*** zaradzenia temu ryzyku. ***Właściwe organy krajowe są uprawnione do tymczasowego lub trwałego zawieszenia procesu testowania lub udziału w piaskownicy, jeżeli skuteczne zaradzenie ryzyku nie jest możliwe, oraz informują o takiej decyzji Urząd ds. AI. Właściwe organy krajowe wykonują swoje uprawnienia nadzorcze w granicach określonych w odpowiednich przepisach, wykorzystując swoje uprawnienia dyskrecjonalne przy stosowaniu przepisów prawnych w odniesieniu do konkretnego projektu piaskownicy w zakresie AI, w celu wspierania innowacji w dziedzinie AI w Unii.***

12. ***Dostawcy lub potencjalni dostawcy*** uczestniczący w piaskownicy regulacyjnej w zakresie AI ponoszą odpowiedzialność, przewidzianą w mających zastosowanie przepisach dotyczących odpowiedzialności przyjętych na szczeblu Unii i na szczeblu krajowym, za wszelkie ***szkody*** wyrządzone osobom trzecim w wyniku eksperymentów prowadzonych w piaskownicy. ***O ile jednak potencjalny dostawca respektuje konkretny plan oraz warunki uczestnictwa, a także w dobrej wierze stosuje się do wytycznych właściwych organów krajowych, nie nakłada się administracyjnych kar pieniężnych w związku z naruszeniem niniejszego rozporządzenia. W zakresie, w jakim inne właściwe organy odpowiedzialne za inne przepisy unijne lub krajowe uczestniczyły aktywnie w nadzorze nad systemem AI w ramach piaskownicy regulacyjnej i udzielały wskazówek w zakresie zgodności, w odniesieniu do tego prawa nie nakłada się administracyjnych kar pieniężnych.***

13. ***Piaskownice regulacyjne w zakresie AI opracowuje się i wdraża w taki sposób, by w stosownych przypadkach ułatwiały współpracę transgraniczną między właściwymi organami krajowymi.***

14. Właściwe organy ***krajowe*** ▌ koordynują swoje działania i prowadzą współpracę w ramach ▌ Rady ds. AI. ▌

15. ***Właściwe organy krajowe informują Urząd ds. AI i Radę ds. AI o utworzeniu piaskownicy oraz mogą zwrócić się do nich o wsparcie i wytyczne. Urząd ds. AI podaje do wiadomości publicznej i aktualizuje wykaz planowanych i istniejących piaskownic w zakresie AI, aby zachęcić do większej interakcji w ramach piaskownic regulacyjnych w zakresie AI i do współpracy transgranicznej.***

16. ***Właściwe organy krajowe przedkładają Urzędowi ds. AI i Radzie ds. AI sprawozdania roczne – po upływie jednego roku od ustanowienia piaskownicy regulacyjnej w zakresie AI, a następnie co roku, aż do jej zakończenia – oraz sprawozdanie końcowe. Wspomniane sprawozdania zawierają informacje o postępach i wynikach wdrażania piaskownic, w tym również o najlepszych praktykach, incydentach, wyciągniętych wnioskach i zaleceniach dotyczących tworzenia piaskownic regulacyjnych, a w stosownych przypadkach – zalecenia dotyczące stosowania i ewentualnego przeglądu niniejszego rozporządzenia, w tym związanych z nim aktów delegowanych i wykonawczych, oraz innych przepisów Unii objętych nadzorem właściwych organów w ramach danej piaskownicy. Właściwe organy krajowe podają te roczne sprawozdania lub ich streszczenia do wiadomości publicznej w internecie. Komisja w stosownych przypadkach uwzględnia sprawozdania roczne przy wykonywaniu swoich zadań na podstawie niniejszego rozporządzenia.***

17. ***Komisja opracowuje jednolity i specjalny interfejs zawierający wszystkie istotne informacje dotyczące piaskownic regulacyjnych w zakresie AI, aby zgodnie z art. 62 ust. 1 lit. c) umożliwić zainteresowanym stronom interakcję z piaskownicami regulacyjnymi w zakresie AI i zwracanie się do właściwych organów z pytaniami oraz poszukiwanie niewiążących wskazówek w zakresie zapewnienia zgodności innowacyjnych produktów, usług i modeli biznesowych obejmujących technologie AI. W stosownych przypadkach Komisja proaktywnie koordynuje swoje działania z właściwymi organami krajowymi.***

Artykuł 58

Szczegółowe zasady dotyczące piaskownic regulacyjnych w zakresie AI i ich funkcjonowania

1. Aby uniknąć fragmentacji w całej Unii, Komisja przyjmuje akty wykonawcze określające szczegółowe ustalenia dotyczące ustanawiania, opracowywania, wdrażania, funkcjonowania piaskownic regulacyjnych w zakresie AI i nadzoru nad nimi. Te akty wykonawcze określają wspólne zasady dotyczące następujących kwestii:

a) kwalifikowalności i kryteriów wyboru do uczestnictwa w piaskownicy regulacyjnej w zakresie AI;

b) procedur składania wniosków, uczestnictwa, monitorowania, wychodzenia z piaskownicy regulacyjnej w zakresie AI i jej zakończenia, w tym planu działania piaskownicy i sprawozdania końcowego;

c) warunków mających zastosowanie do uczestników.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

2. Akty wykonawcze, o których mowa w ust. 1, zapewniają, aby:

a) piaskownice regulacyjne w zakresie AI były otwarte dla każdego zgłaszającego się potencjalnego dostawcy systemu AI spełniającego kryteria kwalifikowalności i wyboru, które są przejrzyste i sprawiedliwe, a właściwe organy krajowe informują wnioskodawców o swojej decyzji w terminie trzech miesięcy od złożenia wniosku;

b) piaskownice regulacyjne w zakresie AI umożliwiały szeroki i równy dostęp oraz nadążały za popytem, jeżeli chodzi o uczestnictwo; potencjalni dostawcy mogą również składać wnioski we współpracy z użytkownikami oraz innymi odpowiednimi osobami trzecimi;

c) szczegółowe ustalenia i warunki dotyczące piaskownic regulacyjnych w zakresie AI w możliwie najlepszym stopniu wspierały elastyczność właściwych organów krajowych w zakresie ustanawiania własnych piaskownic regulacyjnych w zakresie AI i zarządzania nimi;

d) dostęp do piaskownic regulacyjnych w zakresie AI był nieodpłatny dla MŚP, w tym przedsiębiorstw typu start-up, bez uszczerbku dla nadzwyczajnych kosztów, do których odzyskania w sprawiedliwy i proporcjonalny sposób mogą być uprawnione właściwe organy krajowe;

e) ułatwiały one potencjalnym dostawcom, za pomocą efektów uczenia się uzyskanych dzięki piaskownicom regulacyjnym w zakresie AI, spełnianie wynikających z niniejszego rozporządzenia wymogów w zakresie oceny zgodności oraz dobrowolnego stosowania kodeksów postępowania, o których mowa w art. 95;

f) piaskownice regulacyjne w zakresie AI ułatwiały zaangażowanie innych odpowiednich podmiotów w ekosystemie sztucznej inteligencji, takich jak jednostki notyfikowane i organizacje normalizacyjne, MŚP, przedsiębiorstwa typu start-up, inne przedsiębiorstwa, innowatorzy, ośrodki testowo-doświadczalne, laboratoria badawcze i eksperymentalne, europejskie centra innowacji cyfrowych, centra doskonałości i poszczególni naukowcy, aby umożliwić i ułatwić współpracę z sektorem publicznym i prywatnym;

g) procedury, procesy i wymogi administracyjne dotyczące składania wniosków, wyboru, uczestnictwa i wyjścia z piaskownicy regulacyjnej w zakresie AI były proste, łatwe do zrozumienia, jasno podane do wiadomości w celu ułatwienia uczestnictwa MŚP, w tym przedsiębiorstwom typu start-up, o ograniczonych zdolnościach prawnych i administracyjnych, a także by były ujednolicone w całej Unii, aby uniknąć fragmentacji, oraz aby uczestnictwo w piaskownicy regulacyjnej w zakresie AI ustanowionej przez jedno z państw członkowskich lub Europejskiego Inspektora Ochrony Danych było wzajemnie i powszechnie uznawane i miało takie same skutki prawne w całej Unii;

h) uczestnictwo w piaskownicy regulacyjnej w zakresie AI było ograniczone do okresu odpowiedniego dla złożoności i skali projektu, który to okres może zostać przedłużony przez właściwy organ krajowy;

i) piaskownice regulacyjne w zakresie AI ułatwiały tworzenie narzędzi i infrastruktury do testowania, analizy porównawczej, oceny i wyjaśniania aspektów systemów AI istotnych w kontekście uczenia się działań regulacyjnych, które to aspekty obejmują dokładność, solidność i cyberbezpieczeństwo, a także tworzenie środków służących ograniczaniu ryzyka dla praw podstawowych i ogółu społeczeństwa.

3. Potencjalni dostawcy w piaskownicach regulacyjnych w zakresie AI, w szczególności MŚP i przedsiębiorstwa typu start-up, są w stosownych przypadkach kierowani do usług przedwdrożeniowych, takich jak doradztwo w zakresie wdrażania niniejszego rozporządzenia, do innych usług o wartości dodanej, takich jak pomoc w zakresie dokumentów normalizacyjnych i certyfikacji, czy pomoc świadczona przez ośrodki testowo-doświadczalne, europejskie centra innowacji cyfrowych oraz centra doskonałości.

4. W przypadku gdy właściwe organy krajowe rozważają udzielenie zezwolenia na przeprowadzenie testów w warunkach rzeczywistych nadzorowanych w ramach piaskownicy w zakresie AI, która ma zostać ustanowiona na mocy niniejszego artykułu, szczegółowo uzgadniają one z uczestnikami warunki takich testów, a w szczególności odpowiednie gwarancje zabezpieczające ochronę praw podstawowych, zdrowia i bezpieczeństwa. W stosownych przypadkach współpracują one z innymi właściwymi organami krajowymi w celu zapewnienia spójnych praktyk w całej Unii.

Artykuł 59

Dalsze przetwarzanie danych osobowych

na potrzeby opracowywania w interesie publicznym określonych systemów AI w ramach piaskownicy regulacyjnej w zakresie AI

1. Dane osobowe zgromadzone zgodnie z prawem w innych celach ***można*** w piaskownicy regulacyjnej w zakresie AI przetwarzać ***wyłącznie*** do celów opracowywania, ***trenowania*** i testowania ▌ w ramach piaskownicy niektórych systemów AI, ***gdy spełnione są wszystkie*** następujące warunki:

   a) ▌ systemy AI opracowuje się w celu zapewnienia ***przez organ publiczny lub inną osobę fizyczną lub prawną*** ochrony ważnego interesu publicznego w co najmniej jednym z następujących obszarów:

      (i) bezpieczeństwo publiczne i zdrowie publiczne, w tym ***wykrywanie, diagnozowanie***, profilaktyka, kontrola i leczenie chorób ***oraz poprawa systemów opieki zdrowotnej***;

      (ii) wysoki poziom ochrony środowiska i poprawa jego jakości, ***ochrona różnorodności biologicznej, ochrona przed zanieczyszczeniem, środki w zakresie transformacji ekologicznej, środki w zakresie łagodzenia zmiany klimatu i przystosowania się do niej;***

*(iii) **zrównoważoność energetyczna;***

*(iv) **bezpieczeństwo i odporność systemów transportowych i mobilności, infrastruktury krytycznej i sieci;***

*(v) **wydajność i jakość administracji publicznej i usług publicznych;***

b) przetwarzane dane są niezbędne do spełnienia co najmniej jednego z wymogów, o których mowa w rozdziale III sekcja 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 ***praw i wolności*** osób, których dane dotyczą, ***określone w art. 35 rozporządzenia (UE) 2016/679 i art. 39 rozporządzenia (UE) 2018/1725***, jakie mogą wystąpić w trakcie przeprowadzania eksperymentów w ramach piaskownicy, a także mechanizmy reagowania zapewniające 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 ***potencjalnego dostawcy*** korzystającego z piaskownicy, a dostęp do ***tych*** danych posiadają wyłącznie upoważnione osoby;

e) ***dostawcy mogą dalej udostępniać pierwotnie zgromadzone dane wyłącznie zgodnie z unijnym prawem ochrony danych;*** wszelkie dane osobowe ***opracowane w piaskownicy nie mogą być udostępniane poza piaskownicą***;

f) żadne przypadki przetwarzania danych osobowych w kontekście piaskownicy nie prowadzą do wdrożenia środków lub podjęcia decyzji wywierających wpływ na osoby, których dane dotyczą, ***ani nie wpływają na stosowanie ich praw określonych w prawie Unii dotyczącym ochrony danych osobowych;***

g) wszelkie dane osobowe przetwarzane w kontekście piaskownicy ***chroni się za pomocą odpowiednich środków technicznych i organizacyjnych oraz*** usuwa się po zakończeniu uczestnictwa w piaskownicy lub po upływie okresu przechowywania danych osobowych;

h) rejestry przetwarzania danych osobowych w kontekście piaskownicy przechowuje się przez cały czas uczestnictwa w piaskownicy, ***chyba że*** prawo Unii ***lub prawo krajowe stanowią inaczej***;

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

j) krótkie podsumowanie projektu w zakresie AI opracowanego w ramach piaskownicy, jego celów i oczekiwanych rezultatów opublikowano na stronie internetowej właściwych organów; ***obowiązek ten nie obejmuje szczególnie chronionych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych.***

2. Do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania przestępstw lub egzekwowania sankcji karnych, w tym ochrony przed zagrożeniami bezpieczeństwa publicznego i zapobiegania takim zagrożeniom pod nadzorem organów ścigania i na ich odpowiedzialność, przetwarzanie danych osobowych w piaskownicach regulacyjnych w zakresie AI prowadzone jest w oparciu o konkretne przepisy unijne lub krajowe i podlega tym samym łącznym warunkom, o których mowa w ust. 1.

3. Ust. 1 pozostaje bez uszczerbku dla prawa Unii lub prawa krajowego, które wyklucza przetwarzanie danych osobowych do celów innych niż wskazane wprost w tym prawie, ***jak również bez uszczerbku dla prawa Unii lub prawa krajowego ustanawiającego podstawy przetwarzania danych osobowych niezbędnego do celów opracowywania, testowania lub trenowania innowacyjnych systemów AI lub dla jakiejkolwiek innej podstawy prawnej, zgodnie z prawem Unii dotyczącym ochrony danych osobowych.***

Artykuł 60

Testy systemów AI wysokiego ryzyka w warunkach rzeczywistych poza piaskownicami regulacyjnymi w zakresie AI

1. Testy systemów AI wysokiego ryzyka w warunkach rzeczywistych prowadzone poza piaskownicami regulacyjnymi w zakresie AI mogą być przeprowadzane przed dostawców lub potencjalnych dostawców systemów AI wysokiego ryzyka, wymienionych w załączniku III, zgodnie z niniejszym artykułem i planem testów w warunkach rzeczywistych, o którym mowa w niniejszym artykule, bez uszczerbku dla zakazów przewidzianych w art. 5.

Szczegółowe elementy planu testów w warunkach rzeczywistych określa się w aktach wykonawczych przyjmowanych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

Przepis ten pozostaje bez uszczerbku dla przepisów Unii lub prawa krajowego dotyczących testów w warunkach rzeczywistych systemów AI wysokiego ryzyka związanych z produktami objętymi unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I.

2. Dostawcy lub potencjalni dostawcy mogą przeprowadzać testy w warunkach rzeczywistych systemów AI wysokiego ryzyka, o których to systemach mowa w załączniku III, w dowolnym momencie przed wprowadzeniem systemu AI do obrotu lub oddaniem go do użytku, samodzielnie lub we współpracy z jednym potencjalnym podmiotem stosującym AI lub większą liczbą tych podmiotów.

3. Testy w warunkach rzeczywistych systemów AI wysokiego ryzyka na podstawie niniejszego artykułu pozostają bez uszczerbku dla oceny etycznej wymaganej prawem krajowym lub unijnym.

4. Dostawcy lub potencjalni dostawcy mogą przeprowadzać testy w warunkach rzeczywistych tylko wtedy, gdy spełnione są wszystkie następujące warunki:

a) dostawca lub potencjalny dostawca sporządził plan testów w warunkach rzeczywistych i przedłożył go organowi nadzoru rynku w państwie członkowskim, w którym mają być przeprowadzane te testy;

b) krajowy organ nadzoru rynku w państwie członkowskim, w którym mają być prowadzone testy w warunkach rzeczywistych, zatwierdził te testy w warunkach rzeczywistych i plan testów w warunkach rzeczywistych. W przypadku gdy organ nadzoru rynku nie udzielił odpowiedzi w ciągu 30 dni, testy w warunkach rzeczywistych i plan testów w warunkach rzeczywistych uznaje się za zatwierdzone. W przypadku gdy prawo krajowe nie przewiduje milczącej zgody, testy w warunkach rzeczywistych nadal podlegają obowiązkowi uzyskania zezwolenia;

c) dostawca lub potencjalny dostawca – z wyjątkiem dostawców lub potencjalnych dostawców systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7 w obszarach ścigania przestępstw, zarządzania migracją, azylem i kontrolą graniczną, oraz systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 2 – zarejestrował testy w warunkach rzeczywistych w niepublicznej części unijnej bazy danych, o której mowa w art. 71 ust. 3, pod ogólnounijnym niepowtarzalnym numerem identyfikacyjnym, podając informacje określone w załączniku IX;

d) dostawca lub potencjalny dostawca przeprowadzający testy w warunkach rzeczywistych ma siedzibę w Unii lub wyznaczył przedstawiciela prawnego, który ma siedzibę w Unii;

e) dane zebrane i przetwarzane do celów testów w warunkach rzeczywistych przekazuje się do państw trzecich wyłącznie pod warunkiem wdrożenia odpowiednich zabezpieczeń mających zastosowanie na podstawie prawa Unii;

f) testy w warunkach rzeczywistych trwają nie dłużej, niż to konieczne do osiągnięcia ich celów, a w każdym razie nie dłużej niż sześć miesięcy, z możliwością przedłużenia o dodatkowe sześć miesięcy, z zastrzeżeniem uprzedniego powiadomienia organu nadzoru rynku przez dostawcę, wraz z uzasadnieniem konieczności takiego przedłużenia;

g) uczestnicy testów w warunkach rzeczywistych, którzy z ***uwagi na swój wiek, niepełnosprawność fizyczną lub umysłową należą do grup szczególnie wrażliwych, są w odpowiednio chronieni;***

h) ***w przypadku gdy dostawca lub potencjalny dostawca organizuje testy w warunkach rzeczywistych we współpracy z co najmniej jednym podmiotem stosującym AI lub potencjalnym podmiotem stosującym AI, ten ostatni zostaje uprzednio poinformowany o wszystkich aspektach testów, które są istotne dla jego decyzji o uczestnictwie, oraz otrzymuje odpowiednie instrukcje obsługi systemu AI, o których mowa w art. 13; dostawca lub potencjalny dostawca oraz potencjalny podmiot stosujący AI zawierają umowę określającą ich role i obowiązki w celu zapewnienia zgodności z przepisami dotyczącymi testów w warunkach rzeczywistych na podstawie niniejszego rozporządzenia oraz na podstawie innego mającego zastosowanie prawa unijnego i krajowego;***

i) ***uczestnicy testów w warunkach rzeczywistych wyrazili świadomą zgodę zgodnie z art. 61 lub – w przypadku ścigania przestępstw – gdy uzyskanie świadomej zgody uniemożliwiłoby testy systemu AI, same testy w warunkach rzeczywistych oraz ich wynik nie mogą mieć negatywnego wpływu na uczestników testów, a ich dane osobowe są usuwane po przeprowadzeniu testów;***

j) testy w warunkach rzeczywistych są skutecznie nadzorowane przez dostawcę lub potencjalnego dostawcę i podmioty stosujące AI lub potencjalne podmioty stosujące AI przy udziale osób posiadających odpowiednie kwalifikacje w danej dziedzinie oraz zdolności, przygotowanie szkoleniowe i uprawnienia niezbędne do wykonywania ich zadań;

k) predykcje, zalecenia lub decyzje systemu AI można skutecznie odwrócić i zignorować.

5. Uczestnicy testów w warunkach rzeczywistych, lub, w stosownych przypadkach, ich wyznaczony zgodnie z prawem przedstawiciel mogą – bez konsekwencji i bez konieczności przedstawiania jakiegokolwiek uzasadnienia – zdecydować o wycofaniu w dowolnym momencie z testów poprzez odwołanie świadomej zgody; mogą również zażądać natychmiastowego i trwałego usunięcia ich danych osobowych. Wycofanie świadomej zgody nie wpływa na zgodność z prawem lub ważność przeprowadzonych już działań.

6. Zgodnie z art. 75 państwa członkowskie powierzają swoim organom nadzoru rynku uprawnienia w zakresie wymagania od dostawców i potencjalnych dostawców podawania informacji, przeprowadzania niezapowiedzianych kontroli zdalnie lub na miejscu oraz sprawdzania stanu rozwoju testów w warunkach rzeczywistych i powiązanych produktów. Organy nadzoru rynku wykorzystują te uprawnienia do zapewnienia bezpiecznego rozwoju testów w warunkach rzeczywistych.

7. Każdy poważny incydent stwierdzony w trakcie testów w warunkach rzeczywistych zgłasza się krajowemu organowi nadzoru rynku zgodnie z art. 73. Dostawca lub potencjalny dostawca przyjmuje natychmiastowe środki zaradcze lub, w przypadku gdy jest to niemożliwe, zawiesza testy w warunkach rzeczywistych do czasu zaradzenia incydentowi albo też kończy testy. Dostawca lub potencjalny dostawca ustanawia procedurę niezwłocznego wycofania systemu AI od użytkowników po takim zakończeniu testów w warunkach rzeczywistych.

8. Dostawcy lub potencjalni dostawcy powiadamiają krajowy organ nadzoru rynku w państwie członkowskim, w którym prowadzone są testy w warunkach rzeczywistych, o zawieszeniu lub zakończeniu tych testów i o ostatecznych wynikach.

9. Dostawcy lub potencjalni dostawcy ponoszą, na podstawie mającego zastosowanie prawa unijnego i krajowego dotyczącego odpowiedzialności, odpowiedzialność za wszelkie szkody spowodowane w trakcie testów w warunkach rzeczywistych.

Artykuł 61

Świadoma zgoda na uczestnictwo w testach w warunkach rzeczywistych poza piaskownicami regulacyjnymi w zakresie AI

1. Do celów prowadzonych na podstawie art. 60 testów w warunkach rzeczywistych od uczestników testów należy uzyskać dobrowolną świadomą zgodę przed ich udziałem w takich testach i po należytym poinformowaniu ich w sposób zwięzły, jasny, adekwatny i zrozumiały o:

a) charakterze i celach testów w warunkach rzeczywistych oraz ewentualnych niedogodnościach, które mogą być związane z udziałem w tych testach;

b) warunkach, na jakich mają być prowadzone testy w warunkach rzeczywistych, w tym o przewidywanym czasie trwania udziału danego uczestnika lub uczestników w testach;

c) ich prawach i gwarancjach dotyczących udziału w testach, w szczególności o prawie do odmowy udziału w testach oraz o prawie do wycofania się z testów w warunkach rzeczywistych – w dowolnym momencie, bez konsekwencji i bez konieczności przedstawiania jakiegokolwiek uzasadnienia;

d) zasadach zwracania się o odwrócenie lub zignorowanie predykcji, zaleceń lub decyzji wydanych przez system AI;

e) ogólnounijnym niepowtarzalnym numerze identyfikacyjnym testów w warunkach rzeczywistych nadanym zgodnie z art. 60 ust. 4 ***lit.*** c) i ***o danych kontaktowych dostawcy lub jego przedstawiciela prawnego, od których można uzyskać dalsze informacje.***

2. Świadoma zgoda jest opatrzona datą i udokumentowana, a uczestnicy testów lub ich przedstawiciel prawny otrzymują jej kopię.

Artykuł 62

Środki na rzecz ▌ dostawców i ***podmiotów stosujących AI, w szczególności MŚP, w tym przedsiębiorstw typu start-up***

1. Państwa członkowskie podejmują następujące działania:

a) zapewniają MŚP, w tym przedsiębiorstwom typu start-up, ***które mają siedzibę statutową lub oddział w Unii***, dostęp do piaskownic regulacyjnych w zakresie AI na zasadzie pierwszeństwa, o ile spełniają oni warunki kwalifikowalności ***i kryteria wyboru***. ***Dostęp na zasadzie pierwszeństwa nie wyklucza dostępu do piaskownicy regulacyjnej w zakresie AI dla innych MŚP, w tym przedsiębiorstw typu start-up, innych niż te, o których mowa w akapicie pierwszym, pod warunkiem, że również spełniają one warunki kwalifikowalności i kryteria wyboru;***

b) organizują specjalne wydarzenia informacyjne ***i szkoleniowe*** poświęcone stosowaniu przepisów niniejszego rozporządzenia dostosowane do potrzeb ***MŚP, w tym przedsiębiorstw typu start-up, użytkowników i w stosownych przypadkach lokalnych organów publicznych***;

c) ***wykorzystują istniejące specjalne kanały oraz,*** w stosownych przypadkach, ustanawiają ***nowe kanały*** komunikacji z ***MŚP, w tym przedsiębiorstwami typu start-up, użytkownikami, innymi innowatorami oraz, w stosownych przypadkach, z lokalnymi organami publicznymi*** – w celu zapewnienia ***poradnictwa*** i udzielania odpowiedzi na zapytania w zakresie wdrażania niniejszego rozporządzenia, ***w tym odnośnie do udziału w piaskownicach regulacyjnych w zakresie AI;***

d) ułatwiają udział MŚP i innych odpowiednich stron w procesie opracowywania norm;

2. Przy ustalaniu wysokości opłat z tytułu oceny zgodności przeprowadzanej zgodnie z art. 43 bierze się pod uwagę szczególne interesy i potrzeby dostawców będących ***MŚP, w tym przedsiębiorstwami typu start-up***, obniżając te opłaty proporcjonalnie do wielkości tych przedsiębiorstw, ***wielkości rynku i innych odpowiednich wskaźników.***

3. Urząd ds. AI podejmuje następujące działania:

a) zapewnia ujednolicone wzory w obszarach objętych zakresem stosowania niniejszego rozporządzenia, zgodnie ze specyfikacją określoną przez Radę ds. AI w jej uzasadnionym wniosku;

b) opracowuje i obsługuje jednolitą platformę informacyjną zapewniającą wszystkim operatorom w całej Unii przystępne informacje na temat niniejszego rozporządzenia;

c) organizuje odpowiednie kampanie informacyjne w celu podnoszenia świadomości na temat obowiązków wynikających z niniejszego rozporządzenia;

d) ocenia i propaguje zbieżność najlepszych praktyk w postępowaniach o udzielenie zamówienia publicznego w odniesieniu do systemów AI.

Artykuł 63

Odstępstwa dla określonych operatorów

1. Mikroprzedsiębiorstwa w rozumieniu zalecenia 2003/361/WE mogą stosować niektóre elementy systemu zarządzania jakością wymaganego zgodnie z art. 17 niniejszego rozporządzenia w sposób uproszczony, pod warunkiem że nie mają przedsiębiorstw partnerskich ani przedsiębiorstw powiązanych w rozumieniu tego zalecenia. Do tego celu Komisja opracowuje wytyczne dotyczące tych elementów systemu zarządzania jakością, które można stosować w sposób uproszczony, zważywszy na potrzeby mikroprzedsiębiorstw, bez wpływania na poziom ochrony lub potrzebę zgodności z wymogami w odniesieniu do systemów AI wysokiego ryzyka.

2. Ustępu 1 niniejszego artykułu ***nie należy interpretować jako zwalniającego tych operatorów z wszelkich innych wymogów i obowiązków określonych w niniejszym rozporządzeniu, w tym tych ustanowionych w art. 9, 10, 11, 12, 13, 14, 15, 72 i 73.***

ROZDZIAŁ VII
ZARZĄDZANIE

Sekcja 1

Zarządzanie na szczeblu Unii

Artykuł 64

Urząd ds. AI

1. Komisja rozwija unijną wiedzę fachową i zdolności w dziedzinie AI poprzez Urząd ds. AI.

2. Państwa członkowskie ułatwiają wykonywanie zadań powierzonych Urzędowi ds. AI, jak odzwierciedlono w niniejszym rozporządzeniu.

Artykuł 65

Ustanowienie i struktura Europejskiej Rady ds. Sztucznej Inteligencji

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

2. W skład Rady ds. AI wchodzi po jednym przedstawicielu z każdego państwa członkowskiego. Europejski Inspektor Ochrony Danych uczestniczy w charakterze obserwatora. W posiedzeniach Rady ds. AI uczestniczy również Urząd ds. AI, który nie bierze udziału w głosowaniach. Do udziału w posiedzeniach Rada ds. AI może zapraszać w poszczególnych przypadkach inne krajowe i unijne organy, jednostki organizacyjne lub ekspertów, w przypadku gdy omawiane kwestie są dla nich istotne.

3. Każdy przedstawiciel jest wyznaczany przez swoje państwo członkowskie na okres trzech lat, z możliwością jednokrotnego przedłużenia.

4. Państwa członkowskie zapewniają, by ich przedstawiciele w Radzie ds. AI:

a) mieli w swoim państwie członkowskim odpowiednie kompetencje i uprawnienia, tak aby aktywnie przyczyniać się do realizacji zadań Rady ds. AI, o których mowa w art. 66;

b) zostali wyznaczeni jako pojedynczy punkt kontaktowy do kontaktów z Radą ds. AI lub – w stosownych przypadkach i przy uwzględnieniu potrzeb państw członkowskich – jako pojedynczy punkt kontaktowy dla zainteresowanych stron;

c) mieli prawo uczestniczyć w zapewnianiu spójności i koordynacji między właściwymi organami krajowymi w swoich państwach członkowskich w odniesieniu do wdrażania niniejszego rozporządzenia, w tym – do celów wykonywania swoich zadań na forum Rady ds. AI – poprzez gromadzenie odpowiednich danych i informacji.

5. Wyznaczeni przedstawiciele państw członkowskich przyjmują regulamin wewnętrzny Rady ds. AI większością dwóch trzecich głosów. W regulaminie wewnętrznym ustanawia się w szczególności procedury wyboru, czas trwania mandatu i specyfikację zadań przewodniczącego, szczegółowe zasady głosowania oraz organizację działalności Rady ds. AI i jej podgrup.

6. Rada ds. AI powinna ustanowić dwie stałe podgrupy służące jako platforma współpracy i wymiany między organami nadzoru rynku oraz służące powiadamianiu organów w kwestiach dotyczących nadzoru rynku i jednostek notyfikowanych.

Stała podgrupa ds. nadzoru rynku powinna do celów niniejszego rozporządzenia pełnić rolę grupy ds. współpracy administracyjnej (ADCO) w rozumieniu art. 30 rozporządzenia (UE) 2019/1020.

W stosownych przypadkach Rada ds. AI może również tworzyć inne stałe lub tymczasowe podgrupy na potrzeby zbadania konkretnych kwestii. W stosownych przypadkach przedstawiciele forum doradczego, o którym mowa w art. 67, mogą być zapraszani do udziału w takich podgrupach lub na konkretne posiedzenia tych podgrup jako obserwatorzy.

7. ***Rada ds. AI jest zorganizowana i zarządzana w sposób gwarantujący obiektywizm i bezstronność podejmowanych przez nią działań.***

8. ***Przewodniczącym Rady ds. AI jest jeden z przedstawicieli państw członkowskich. Urząd ds. AI pełni funkcję sekretariatu dla Rady ds. AI, zwołuje na żądanie przewodniczącego posiedzenia i przygotowuje porządek obrad zgodnie z zadaniami Rady ds. AI określonymi w niniejszym rozporządzeniu oraz z jej regulaminem wewnętrznym.***

Artykuł 66

Zadania Rady ds. AI

Rada ds. AI doradza Komisji i państwom członkowskim oraz udziela im wsparcia w celu ułatwienia spójnego i skutecznego stosowania niniejszego rozporządzenia. W tym celu Rada ds. AI ***może*** w szczególności:

a) ***przyczyniać się do koordynacji między właściwymi organami krajowymi odpowiedzialnymi za stosowanie niniejszego rozporządzenia oraz, we współpracy i z zastrzeżeniem zgody zainteresowanego organu nadzoru rynku, wspierać wspólne działania organów nadzoru rynku, o których mowa w art.*** 74 ust. 11;

b) ***gromadzić fachową wiedzę techniczną i*** regulacyjną ***oraz najlepsze praktyki i udostępniać je państwom członkowskim;***

c) zapewniać doradztwo w zakresie wdrażania niniejszego rozporządzenia, w szczególności w odniesieniu do egzekwowania przepisów dotyczących modeli AI ogólnego przeznaczenia;

d) przyczyniać się do harmonizacji praktyk administracyjnych w państwach członkowskich, w tym w odniesieniu do odstępstwa od procedur oceny zgodności, o którym mowa w art. 46, funkcjonowania piaskownic regulacyjnych oraz testów w warunkach rzeczywistych, o których mowa w art. 57, 59 i 60;

e) na żądanie Komisji lub z własnej inicjatywy wydawać zalecenia i pisemne ***opinie na temat wszelkich istotnych*** zagadnień związanych z wdrażaniem niniejszego rozporządzenia ***oraz z jego spójnym i skutecznym stosowaniem, w tym:***

(i) w zakresie rozwoju i stosowania kodeksów postępowania i kodeksów praktyk zgodnie z niniejszym rozporządzeniem, jak również wytycznych Komisji;

(ii) dotyczące oceny i przeglądu niniejszego rozporządzenia zgodnie z art. 112, w tym w odniesieniu do zgłoszeń poważnych incydentów, o których mowa w art. 73, i funkcjonowania bazy danych, o której mowa w art. 71, przygotowania aktów delegowanych lub wykonawczych oraz w odniesieniu do ewentualnego dostosowania niniejszego rozporządzenia do aktów prawnych wymienionych w załączniku I;

(iii) w kwestii specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w rozdziale III sekcja 2;

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

(v) na temat tendencji, takich jak europejska globalna konkurencyjność w dziedzinie AI, absorpcja AI w Unii oraz rozwój umiejętności cyfrowych;

(vi) na temat tendencji w zakresie zmieniającej się typologii łańcuchów wartości AI, w szczególności w odniesieniu do wynikających z nich skutków w zakresie odpowiedzialności;

(vii) w kwestii potencjalnej potrzeby zmiany załącznika III zgodnie z art. 7 oraz potencjalnej potrzeby ewentualnej zmiany artykułu 5 zgodnie z art. 112, z uwzględnieniem odpowiednich dostępnych dowodów i najnowszych osiągnięć technologicznych;

f) wspierać Komisję w promowaniu narzędzi rozwijających kompetencje w zakresie AI, świadomości społecznej oraz zrozumienia w odniesieniu do korzyści, ryzyka, zabezpieczeń, praw i obowiązków związanych z korzystaniem z systemów AI;

g) ułatwiać opracowywanie wspólnych kryteriów i wspólnego rozumienia przez podmioty gospodarcze i właściwe organy odpowiednich pojęć przewidzianych w niniejszym rozporządzeniu, w tym poprzez udział w opracowywaniu poziomów odniesienia;

h) współpracować, w stosownych przypadkach, z innymi instytucjami, organami i jednostkami organizacyjnymi Unii, jak również unijnymi grupami ekspertów i sieciami, w szczególności w dziedzinie bezpieczeństwa produktów, cyberbezpieczeństwa, konkurencyjności, usług cyfrowych i medialnych, usług finansowych, ochrony konsumentów, ochrony danych oraz ochrony praw podstawowych;

i) przyczyniać się do skutecznej współpracy z właściwymi organami państw trzecich i z organizacjami międzynarodowymi;

j) wspierać właściwe organy krajowe i Komisję w rozwijaniu organizacyjnej i technicznej wiedzy fachowej wymaganej do wdrożenia niniejszego rozporządzenia, w tym poprzez przyczynianie się do oceny potrzeb szkoleniowych personelu państw członkowskich uczestniczącego we wdrażaniu niniejszego rozporządzenia;

k) wspierać Urząd ds. AI w udzielaniu wsparcia właściwym organom krajowym w ustanawianiu i rozwoju piaskownic regulacyjnych oraz ułatwiać współpracę i wymianę informacji między piaskownicami regulacyjnymi;

l) wnosić wkład w opracowanie dokumentów zawierających wytyczne i udzielać stosownych porad w tym zakresie;

m) doradzać Komisji w odniesieniu do międzynarodowych kwestii dotyczących AI;

n) przedstawiać Komisji opinie na temat ostrzeżeń kwalifikowanych dotyczących modeli AI ogólnego przeznaczenia;

o) przyjmować od państw członkowskich opinie dotyczące ostrzeżeń kwalifikowanych dotyczących modeli AI ogólnego przeznaczenia oraz opinie na temat krajowych doświadczeń i praktyk w zakresie monitorowania i zgodnego z prawem wdrażania systemów AI, w szczególności systemów integrujących modele AI ogólnego przeznaczenia.

Artykuł 67

Forum doradcze

1. Ustanawia się forum doradcze, które ma za zadanie dostarczać fachowej wiedzy technicznej i doradzać Radzie ds. AI i Komisji oraz wnosić wkład w ich zadania wynikające z niniejszego rozporządzenia.

2. Skład forum doradczego stanowi wyważony wybór zainteresowanych stron, w tym przemysłu, przedsiębiorstw typu start-up, MŚP, społeczeństwa obywatelskiego i środowisk akademickich. Skład forum doradczego jest zrównoważony pod względem interesów handlowych i niehandlowych, a w ramach kategorii interesów handlowych – w odniesieniu do MŚP i innych przedsiębiorstw.

3. Komisja zgodnie z kryteriami określonymi w ust. 2 mianuje członków forum doradczego spośród zainteresowanych podmiotów dysponujących uznaną wiedzą fachową w dziedzinie AI.

4. Kadencja członków forum doradczego trwa dwa lata i może zostać przedłużona o maksymalnie cztery lata.

5. Stałymi członkami forum doradczego są: Agencja Praw Podstawowych, ENISA, Europejski Komitet Normalizacyjny (CEN), Europejski Komitet Normalizacyjny Elektrotechniki (CENELEC) oraz Europejski Instytut Norm Telekomunikacyjnych (ETSI).

6. Forum doradcze sporządza swój regulamin. Wybiera dwóch współprzewodniczących spośród swoich członków, zgodnie z kryteriami określonymi w ust. 2. Kadencja współprzewodniczących trwa dwa lata z możliwością jednokrotnego odnowienia.

7. Forum doradcze odbywa posiedzenia co najmniej dwa razy w roku. Forum doradcze może zapraszać na swoje posiedzenia ekspertów i inne zainteresowane strony.

8. Forum doradcze może na wniosek Rady ds. AI lub Komisji przygotowywać opinie, zalecenia i pisemne uwagi.

9. W stosownych przypadkach forum doradcze może tworzyć stałe lub tymczasowe podgrupy do badania konkretnych kwestii związanych z celami niniejszego rozporządzenia.

10. Forum doradcze przygotowuje roczne sprawozdanie ze swoich działań. Sprawozdanie to jest podawane do wiadomości publicznej.

Artykuł 68

Panel naukowy niezależnych ekspertów

1. *Komisja w drodze aktu wykonawczego ustanawia przepisy dotyczące utworzenia panelu naukowego niezależnych ekspertów („panel naukowy"), którego celem jest udzielanie wsparcia w egzekwowaniu działań na podstawie niniejszego rozporządzenia. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.*

2. *Panel naukowy składa się z ekspertów, którzy zostali wybrani przez Komisję na podstawie aktualnej wiedzy naukowej lub technicznej w dziedzinie AI niezbędnej do realizacji zadań określonych w ust. 3 i którzy są w stanie wykazać, że spełniają wszystkie następujące warunki:*

   a) *posiadanie szczególnej wiedzy fachowej i kompetencji oraz naukowej lub technicznej wiedzy fachowej w dziedzinie AI;*

b) niezależność od dostawców systemów AI lub modeli lub systemów AI ogólnego przeznaczenia;

c) zdolność do wykonywania zadań w sposób staranny, dokładny i obiektywny. Komisja w porozumieniu z Radą ds. AI określa liczbę ekspertów wchodzących w skład panelu w zależności od potrzeb i zapewnia sprawiedliwą reprezentację pod względem płci i zakresu geograficznego.

3. Panel naukowy doradza i wspiera Urząd ds. AI, w szczególności w odniesieniu do następujących zadań:

a) wspieranie wdrażania i egzekwowania niniejszego rozporządzenia w odniesieniu do modeli i systemów AI ogólnego przeznaczenia, w szczególności poprzez:

(i) ostrzeganie Urzędu ds. AI zgodnie z art. 90 o potencjalnym ryzyku systemowym na poziomie Unii związanym z modelami AI ogólnego przeznaczenia;

(ii) przyczynianie się do rozwoju narzędzi i metodologii oceny zdolności modeli i systemów AI ogólnego przeznaczenia, w tym za pomocą poziomów odniesienia;

(iii) świadczenie doradztwa w zakresie klasyfikacji modeli AI ogólnego przeznaczenia z ryzykiem systemowym;

(iv) świadczenie doradztwa w zakresie klasyfikacji różnych modeli i systemów AI ogólnego przeznaczenia;

(v) przyczynianie się do opracowywania narzędzi i wzorów;

b) wspieranie organów nadzoru rynku – na ich wniosek;

c) wspieranie transgranicznych działań w zakresie nadzoru rynku, o których mowa w art. 74 ust. 11, *bez uszczerbku dla uprawnień organów nadzoru rynku;*

d) wspieranie Urzędu ds. AI w wykonywaniu jego obowiązków w kontekście klauzuli ochronnej zgodnie z art. 81.

4. Eksperci uczestniczący w panelu naukowym wykonują swoje zadania w sposób bezstronny i obiektywny oraz zapewniają poufność informacji i danych uzyskanych podczas wykonywania swoich zadań i działań. Przy wykonywaniu swoich zadań zgodnie z ust. 3 nie zwracają się do nikogo o instrukcje, ani ich od nikogo nie przyjmują. Każdy ekspert sporządza deklarację o braku konfliktu interesów, którą podaje się do wiadomości publicznej. Urząd ds. AI ustanawia systemy i procedury mające na celu aktywne zaradzanie i zapobieganie potencjalnym konfliktom interesów.

5. Akt wykonawczy, o którym mowa w ust. 1, zawiera przepisy dotyczące warunków, procedur i szczegółowych ustaleń w zakresie wydawania ostrzeżeń przez panel naukowy i jego członków oraz zwracania się do Urzędu ds. AI o pomoc w realizacji zadań panelu naukowego.

Artykuł 69

Dostęp państw członkowskich do zasobów eksperckich

1. *Państwa członkowskie mogą zwracać się do ekspertów panelu naukowego o wsparcie ich działań w zakresie egzekwowania przepisów na podstawie niniejszego rozporządzenia.*

2. *Państwa członkowskie mogą być zobowiązane do uiszczania opłat za doradztwo i wsparcie świadczone przez ekspertów. Struktura i poziom opłat, jak również skala i struktura kosztów podlegających zwrotowi są określane w akcie wykonawczym, o którym mowa w art. 68 ust. 1, z uwzględnieniem celów odpowiedniego wdrożenia niniejszego rozporządzenia, efektywności kosztowej i konieczności zapewnienia skutecznego dostępu do ekspertów wszystkim państwom członkowskim.*

3. *Komisja ułatwia państwom członkowskim terminowy dostęp do ekspertów, stosownie do potrzeb, i zapewnia, by połączenie działań wspierających prowadzonych przez unijne struktury wsparcia testowania AI zgodnie z art.* 84 i *przez ekspertów zgodnie z niniejszym artykułem było sprawnie zorganizowane i przynosiło możliwie największą wartość dodaną.*

Sekcja 2

Właściwe organy krajowe

Artykuł 70

Wyznaczanie właściwych organów krajowych ***oraz pojedynczych punktów kontaktowych***

1. ***Do celów niniejszego rozporządzenia*** każde państwo członkowskie ***ustanawia lub*** wyznacza ***co najmniej jeden organ notyfikujący i co najmniej jeden*** organ nadzoru rynku ***jako właściwe organy krajowe. Te właściwe organy*** krajowe ***wykonują swoje uprawnienia w sposób niezależny, bezstronny i nietendencyjny, tak aby chronić obiektywizm ich działań i zadań oraz zapewnić stosowanie i wdrożenie niniejszego rozporządzenia. Członkowie tych organów powstrzymują się od wszelkich czynności niezgodnych z charakterem ich funkcji. Takie działania i zadania mogą być wykonywane przez jeden lub kilka wyznaczonych organów zgodnie z potrzebami organizacyjnymi państwa członkowskiego, pod warunkiem poszanowania tych zasad.***

2. Państwa członkowskie ***przekazują*** Komisji ***dane organów notyfikujących i organów nadzoru rynku oraz informacje o zadaniach tych organów, jak również o wszelkich późniejszych zmianach w tym zakresie. Państwa członkowskie za pośrednictwem środków komunikacji elektronicznej podają do wiadomości publicznej informacje o sposobach kontaktu z właściwymi organami i pojedynczymi punktami kontaktowymi do dnia ... [12 miesięcy od daty wejścia w życie niniejszego rozporządzenia]. Państwa członkowskie wyznaczają organ nadzoru rynku, który będzie pełnił funkcję pojedynczego punktu kontaktowego do celów niniejszego rozporządzenia, i przekazuje Komisji dane tego pojedynczego punktu kontaktowego. Komisja podaje do wiadomości publicznej wykaz pojedynczych punktów kontaktowych.***

3. Państwa członkowskie dbają o to, aby ***ich*** właściwe organy krajowe dysponowały odpowiednimi zasobami ***technicznymi***, finansowymi i ludzkimi, a ***także infrastrukturą*** niezbędnymi do ***skutecznego*** wykonywania 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 AI, danych i metod przetwarzania danych, ***ochrony danych osobowych, cyberbezpieczeństwa***, praw podstawowych, zagrożeń dla zdrowia i bezpieczeństwa oraz wiedzę na temat obowiązujących norm i wymogów prawnych. ***Państwa członkowskie co roku oceniają i w razie potrzeby aktualizują wymogi dotyczące kompetencji i zasobów, o których mowa w niniejszym ustępie.***

4. Właściwe organy krajowe wprowadzają odpowiedni poziom środków w zakresie cyberbezpieczeństwa.

5. Wykonując swoje zadania, właściwe organy krajowe działają zgodnie z obowiązkami w zakresie poufności określonymi w art. 78.

6. ***Do dnia ... [jeden rok od daty wejścia w życie niniejszego rozporządzenia], a następnie co dwa lata*** państwa członkowskie ▌ przekazują Komisji sprawozdania dotyczące stanu zasobów finansowych i ludzkich właściwych organów krajowych wraz z oceną ich adekwatności. Komisja przekazuje te informacje Radzie ds. AI w celu ich omówienia i ewentualnego wydania zaleceń.

7. Komisja ułatwia wymianę doświadczeń między właściwymi organami krajowymi.

8. Właściwe organy krajowe mogą udzielać wskazówek i porad w zakresie wdrażania niniejszego rozporządzenia, ***w szczególności MŚP, w tym przedsiębiorstwom typu start-up, przy uwzględnieniu, w stosownych przypadkach, wskazówek i porad Rady ds. AI i Komisji.*** Jeżeli właściwe organy krajowe zamierzają udzielić wskazówek i porad dotyczących systemu AI w dziedzinach objętych innymi przepisami Unii, są zobowiązane – w stosownych przypadkach – każdorazowo zasięgnąć opinii właściwych organów krajowych wyznaczonych na podstawie tych przepisów Unii. ▌

9. W przypadku gdy 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.

ROZDZIAŁ VIII
UNIJNA BAZA DANYCH DLA ▌SYSTEMÓW AI WYSOKIEGO RYZYKA

Artykuł 71

Unijna baza danych dla systemów AI wysokiego ryzyka umieszczonych w załączniku III

1. Komisja – we współpracy z państwami członkowskimi – tworzy i prowadzi unijną bazę danych zawierającą informacje, o których mowa w ***ust. 2 i 3 niniejszego artykułu***, dotyczącą systemów AI wysokiego ryzyka, o których mowa w art. 6 ust. 2, które podlegają rejestracji zgodnie z ***art. 49 i 60***. Przy ustalaniu specyfikacji funkcjonalnych takiej bazy danych Komisja konsultuje się z odpowiednimi ekspertami, a przy aktualizacji specyfikacji funkcjonalnych takiej bazy danych Komisja konsultuje się z Radą ds. AI.

2. Dane wymienione w załączniku VIII ***sekcja A*** są wprowadzane do unijnej bazy danych przez ***dostawcę, lub – w stosownych przypadkach – przez upoważnionego przedstawiciela.***

3. Dane wymienione w załączniku VIII sekcja C są wprowadzane do unijnej bazy danych przez podmiot stosujący AI będący organem publicznym, agencją lub jednostką organizacyjną zgodnie z art. 49 ust. 2 i 3, lub działający w imieniu takiego organu, agencji lub jednostki.

4. ***Z wyjątkiem sekcji, o której mowa w art. 49 ust. 4 i art. 60 ust. 5,*** informacje zawarte w unijnej bazie danych ***zarejestrowane zgodnie z art. 49*** są dostępne ***publicznie w sposób przyjazny dla użytkownika. Informacje powinny być łatwe w nawigacji i nadawać się do odczytu maszynowego. Informacje zarejestrowane zgodnie z art. 60 są dostępne wyłącznie dla organów nadzoru rynku i dla Komisji, chyba że potencjalny dostawca lub dostawca wyrazili zgodę na udostępnienie tych informacji również opinii*** publicznej.

5. 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 ***lub, w stosownych przypadkach, podmiotu stosującego AI.***

6. Komisja pełni funkcję administratora unijnej bazy danych. ***Zapewnia dostawcom, potencjalnym*** dostawcom ***oraz podmiotom stosującym AI*** odpowiednie wsparcie techniczne i administracyjne. ***Baza danych UE musi spełniać mające zastosowanie wymogi w zakresie dostępności.***

ROZDZIAŁ IX
MONITOROWANIE PO WPROWADZENIU DO OBROTU, WYMIANA INFORMACJI, NADZÓR RYNKU

Sekcja 1
Monitorowanie po wprowadzeniu do obrotu

Artykuł 72

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

1. Dostawcy ustanawiają i dokumentują – w sposób proporcjonalny do charakteru technologii AI i ryzyka związanego ze stosowaniem danego systemu AI wysokiego ryzyka – system monitorowania po wprowadzeniu do obrotu.

2. W ramach systemu monitorowania po wprowadzeniu do obrotu w aktywny i systematyczny sposób gromadzi się, dokumentuje i analizuje stosowne dane dotyczące skuteczności działania systemów AI wysokiego ryzyka w całym cyklu ich życia, ***które to dane mogą być*** przekazywane przez ***podmioty stosujące AI lub mogą być*** gromadzone z innych źródeł; system ten pozwala dostawcy oceniać ciągłość spełniania przez systemy AI wymogów ustanowionych w rozdziale III sekcja 2. ***W stosownych przypadkach monitorowanie po wprowadzeniu do obrotu obejmuje analizę interakcji z innymi systemami AI. Obowiązek ten nie obejmuje wrażliwych danych operacyjnych podmiotów stosujących AI będących organami ścigania.***

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 do dnia ... ***[sześć miesięcy od daty rozpoczęcia stosowania niniejszego rozporządzenia]. Ten akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.***

4. W odniesieniu do systemów AI wysokiego ryzyka objętych unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I ***sekcja A***, w przypadku gdy zgodnie z tym prawodawstwem ustanowiono już system i plan monitorowania po wprowadzeniu do obrotu, ***w celu zapewnienia spójności, unikania powielania prac i zminimalizowania dodatkowych obciążeń, dostawcy mogą się w stosownych przypadkach zdecydować na zintegrowanie – korzystając ze wzoru, o którym mowa w ust. 3 – niezbędnych*** elementów opisanych w ust. 1, 2 i 3 z systemami i planami istniejącymi już ***na podstawie tego prawodawstwa, pod warunkiem że zapewniają one równoważny poziom ochrony***.

   Akapit pierwszy niniejszego artykułu ma również zastosowanie ▌ do systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt ***5***, wprowadzonych do obrotu lub oddanych do użytku przez instytucje ***finansowe objęte na podstawie unijnych przepisów dotyczących usług finansowych wymogami dotyczącymi ich systemu zarządzania wewnętrznego, uzgodnień lub procedur.***

Sekcja 2

Wymiana informacji na temat poważnych incydentów

Artykuł 73

Zgłaszanie poważnych incydentów

1. Dostawcy systemów AI wysokiego ryzyka wprowadzonych do obrotu na rynku unijnym zgłaszają wszelkie poważne incydenty ***organom nadzoru rynku tego państwa członkowskiego, w którym wystąpił dany incydent.***

.

2. Zgłoszenie, o ***którym mowa w ust. 1***, przekazuje się niezwłocznie po ustaleniu przez dostawcę związku przyczynowego między systemem AI a ***poważnym*** incydentem lub ▌ dostatecznie wysokiego prawdopodobieństwa występowania takiego związku, nie później jednak niż w terminie 15 dni od dnia, w którym ***dostawca lub, w stosownych przypadkach, podmiot stosujący AI*** dowiedzieli się o wystąpieniu poważnego incydentu.

Termin na przesłanie zgłoszenia, o którym mowa w akapicie pierwszym, uwzględnia stopień ciężkości danego poważnego incydentu ▌ .

3. ***Niezależnie od ust. 2 niniejszego artykułu w przypadku powszechnego naruszenia lub poważnego incydentu zdefiniowanego w art. 3 pkt 44 lit. b) zgłoszenie, o którym mowa w ust. 1 niniejszego artykułu, przekazuje się niezwłocznie, nie później jednak niż w terminie dwóch dni od dnia, w którym dostawca lub, w stosownych przypadkach, podmiot stosujący AI dowiedzieli się o wystąpieniu tego incydentu.***

5. Niezależnie od ust. 2 w przypadku gdy nastąpi śmierć osoby, zgłoszenie przekazuje się niezwłocznie po stwierdzeniu przez dostawcę lub podmiot stosujący AI występowania lub podejrzenia występowania związku przyczynowego między systemem AI wysokiego ryzyka a poważnym incydentem, nie później jednak niż w terminie 10 dni od dnia, w którym dostawca lub, w stosownych przypadkach, podmiot stosujący AI dowiedzieli się o wystąpieniu danego poważnego incydentu.

6. W przypadku gdy jest to konieczne do zapewnienia terminowego zgłoszenia, dostawca lub, w stosownych przypadkach, podmiot stosujący AI mogą przedłożyć niepełne zgłoszenie wstępne, a następnie zgłoszenie kompletne.

7. W następstwie zgłoszenia poważnego incydentu zgodnie z ust. 1 dostawca niezwłocznie przeprowadza niezbędne postępowanie wyjaśniające dotyczące poważnego incydentu oraz przedmiotowego systemu AI. Obejmuje ono ocenę ryzyka danego incydentu oraz działania naprawcze.

Podczas postępowania wyjaśniającego, o którym mowa w akapicie pierwszym, dostawca współpracuje z właściwymi organami oraz – w stosownych przypadkach – z zainteresowaną jednostką notyfikowaną i nie podejmuje żadnego działania, które obejmowałoby zmianę danego systemu AI w taki sposób, który mógłby wpłynąć na późniejszą ocenę przyczyn incydentu, dopóki nie poinformuje o takim działaniu właściwego organu.

8. Po otrzymaniu zgłoszenia dotyczącego ***poważnego incydentu, o którym mowa w art. 3 pkt 44 lit. c), odpowiedni*** organ nadzoru rynku informuje o tym fakcie krajowe organy publiczne lub organy, o których mowa w art. 77 ust. 1. Komisja opracowuje specjalne wskazówki ułatwiające zapewnienie zgodności z obowiązkami określonymi w ust. 1 niniejszego artykułu. Wskazówki wydaje się do dnia ... [12 miesięcy od dnia wejścia w życie niniejszego rozporządzenia] ***i prowadzi ich regularną ocenę.***

9. Organ nadzoru rynku w ciągu siedmiu dni od daty otrzymania powiadomienia, o którym mowa w ust. 1 niniejszego artykułu podejmuje odpowiednie środki, jak przewidziano w art. 19 rozporządzenia (UE) 2019/1020, i przestrzega procedur powiadamiania przewidzianych w tym rozporządzeniu.

10. W przypadku systemów AI wysokiego ryzyka, o których mowa w załączniku III ▌, wprowadzanych do obrotu lub oddawanych do użytku przez dostawców ***podlegających unijnym instrumentom prawnym ustanawiającym obowiązki w zakresie zgłaszania równoważne obowiązkom określonym w niniejszym rozporządzeniu***, ▌ zgłaszanie poważnych incydentów ogranicza się do tych z nich, ***o których mowa w art. 3 pkt 44 lit. c)***.

11. W przypadku systemów AI wysokiego ryzyka będących związanymi z bezpieczeństwem elementami wyrobów podlegających przepisom rozporządzeń (UE) 2017/745 i (UE) 2017/746 lub które same są takimi wyrobami, zgłaszanie poważnych incydentów ogranicza się do incydentów, o których mowa w art. 3 pkt 44) lit. c) niniejszego rozporządzenia, i jest dokonywane do właściwego organu krajowego wybranego do tego celu przez państwo członkowskie, w którym wystąpił dany incydent.

12. Właściwe organy krajowe niezwłocznie powiadamiają Komisję o każdym poważnym incydencie zgodnie z art. 20 rozporządzenia (UE) 2019/1020, niezależnie od tego, czy podjęły w związku z nim jakiekolwiek działania.

Sekcja 3

Egzekwowanie

Artykuł 74

Nadzór rynku i kontrola systemów AI na rynku Unii

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

   a) wszelkie odniesienia do podmiotu gospodarczego w rozporządzeniu (UE) 2019/1020 należy rozumieć jako obejmujące wszystkich operatorów zidentyfikowanych w ***art. 2 ust. 1*** niniejszego rozporządzenia;

   b) wszelkie odniesienia do produktu w rozporządzeniu (UE) 2019/1020 należy rozumieć jako obejmujące wszystkie systemy AI wchodzące w zakres niniejszego rozporządzenia.

2. ***W ramach swoich obowiązków informacyjnych na podstawie art. 34 ust. 4 rozporządzenia (UE) 2019/1020 organy*** nadzoru rynku ***co roku*** przekazują Komisji i odpowiednim krajowym organom ochrony konkurencji wszelkie informacje zebrane w wyniku działań w zakresie nadzoru rynku, które potencjalnie mogą być istotne z punktu widzenia stosowania reguł konkurencji przewidzianych w prawie Unii. ***Co roku składają również Komisji sprawozdania dotyczące stwierdzonego w danym roku stosowania zakazanych praktyk oraz podjętych w tym względzie środków.***

3. W przypadku systemów AI wysokiego ryzyka powiązanych z produktami objętymi unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I sekcja A, za organ nadzoru rynku do celów niniejszego rozporządzenia uznaje się odpowiedzialny za działania w zakresie nadzoru rynku organ wyznaczony na podstawie tych aktów prawnych. ***W drodze odstępstwa od ust. 2 i w odpowiednich okolicznościach państwa członkowskie mogą do pełnienia funkcji organu nadzoru rynku wyznaczyć inny odpowiedni organ, pod warunkiem że zapewnią koordynację między odpowiednimi sektorowymi organami nadzoru rynku odpowiedzialnymi za egzekwowanie aktów prawnych wymienionych w załączniku I.***

4. Procedury, o których mowa w art. 79–83 niniejszego rozporządzenia, nie mają zastosowania do systemów AI związanych z produktami objętymi unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I sekcja A, w przypadku gdy w tych aktach prawnych przewidziano już procedury zapewniające równoważny poziom ochrony i mające taki sam cel. W takich przypadkach zastosowanie mają procedury sektorowe.

5. ***Bez uszczerbku dla uprawnień organów nadzoru rynku na podstawie art. 14 rozporządzenia (UE) 2019/1020 do celów zapewnienia skutecznego egzekwowania niniejszego rozporządzenia organy nadzoru rynku mogą w stosownych przypadkach wykonywać uprawnienia, o których mowa w art. 14 ust. 4 lit. d) i j) tego rozporządzenia, w sposób zdalny.***

6. W przypadku systemów AI ***wysokiego ryzyka*** wprowadzanych do obrotu, oddawanych do użytku lub wykorzystywanych przez instytucje finansowe podlegające unijnym przepisom dotyczącym usług finansowych organem nadzoru rynku do celów niniejszego rozporządzenia jest odpowiedni organ ***krajowy*** odpowiedzialny na mocy tego prawodawstwa za nadzór finansowy nad tymi instytucjami, w ***zakresie, w jakim wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie danego systemu AI jest bezpośrednio związane ze świadczeniem tych usług finansowych.***

7. ***W drodze odstępstwa od ust. 6, w odpowiednich okolicznościach i pod warunkiem zapewnienia koordynacji państwo członkowskie może do celów niniejszego rozporządzenia wyznaczyć inny odpowiedni organ jako organ nadzoru rynku.***

Krajowe organy nadzoru rynku nadzorujące instytucje kredytowe uregulowane na podstawie dyrektywy 2013/36/UE, które uczestniczą w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem nr 1024/2013, powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zidentyfikowane w trakcie prowadzonych przez siebie działań z zakresu nadzoru rynku, które potencjalnie mogą mieć znaczenie z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego.

8. W odniesieniu do wymienionych w załączniku III pkt 1 systemów AI ***wysokiego ryzyka*** w zakresie, w jakim systemy te są wykorzystywane do celów ścigania przestępstw, kontroli granicznej oraz w kontekście wymiaru sprawiedliwości i demokracji, ***oraz w odniesieniu do systemów AI wysokiego ryzyka wymienionych w*** załączniku III pkt 6, ***7 i 8*** niniejszego rozporządzenia, państwa członkowskie jako organy nadzoru rynku do celów niniejszego rozporządzenia wyznaczają albo właściwe organy nadzorcze ds. ochrony danych na podstawie ***rozporządzenia (UE) 2016/679*** lub dyrektywy (UE) 2016/680 ***lub którykolwiek z innych organów wyznaczonych zgodnie z tymi samymi warunkami ustanowionymi w*** art. 41–44 dyrektywy ***(UE) 2016/680***. ***Działania w zakresie nadzoru rynku nie mogą w żaden sposób wpływać na niezależność organów wymiaru sprawiedliwości, ani w żaden inny sposób zakłócać ich działań w ramach sprawowania przez nie wymiaru sprawiedliwości.***

9. W przypadku gdy zakresem stosowania niniejszego rozporządzenia objęte są instytucje, organy i jednostki organizacyjne Unii, rolę organu nadzoru rynku pełni w stosunku do nich Europejski Inspektor Ochrony Danych, ***z wyjątkiem przypadków sprawowania sprawiedliwości przez Trybunał Sprawiedliwości Unii Europejskiej***.

10. 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 I lub innych przepisów Unii, które mogą być istotne w kontekście systemów AI wysokiego ryzyka, o których mowa w załączniku III.

11. Organy nadzoru rynku i Komisja mogą proponować wspólne działania, w tym wspólne postępowania, prowadzone przez organy nadzoru rynku albo przez organy nadzoru rynku wspólnie z Komisją, mające na celu promowanie zgodności, wykrywanie przypadków niezgodności, podnoszenie świadomości lub zapewnianie wskazówek dotyczących niniejszego rozporządzenia w odniesieniu do szczególnych kategorii systemów AI wysokiego ryzyka, w przypadku których zgodnie z art. 9 rozporządzenia (UE) 2019/1020 stwierdzono, że stwarzają poważne ryzyko w co najmniej dwóch państwach członkowskich. Urząd ds. AI zapewnia wsparcie w zakresie koordynacji wspólnych postępowań.

12. Bez uszczerbku dla uprawnień przewidzianych na podstawie rozporządzenia (UE) 2019/1020 oraz w stosownych przypadkach i w zakresie ograniczonym do tego, co jest niezbędne do wykonywania ich zadań, dostawcy udzielają organom nadzoru rynku pełnego dostępu do dokumentacji, a także do zbiorów danych treningowych, walidacyjnych i testowych wykorzystywanych do opracowywania systemów AI wysokiego ryzyka, w tym, w stosownych przypadkach i z zastrzeżeniem gwarancji bezpieczeństwa, za pośrednictwem interfejsów programowania aplikacji („API") lub innych odpowiednich środków i narzędzi technicznych umożliwiających zdalny dostęp.

13. Organom nadzoru rynku udziela się dostępu do kodu źródłowego systemu AI wysokiego ryzyka na ich uzasadniony wniosek i wyłącznie wtedy, gdy spełnione są oba następujące warunki:

a) dostęp do kodu źródłowego jest niezbędny do oceny zgodności systemu AI wysokiego ryzyka z wymogami określonymi w rozdziale III sekcja 2; oraz

b) zostały wyczerpane lub okazały się niewystarczające procedury testowania lub audytu i weryfikacji w oparciu o dane i dokumentację dostarczone przez dostawcę.

14. Wszelkie informacje lub dokumenty uzyskane przez organy nadzoru rynku traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 78.

Artykuł 75

Wzajemna pomoc, nadzór rynku i kontrola systemów AI ogólnego przeznaczenia

1. W przypadku gdy system AI jest oparty na modelu AI ogólnego przeznaczenia i ten model i system są opracowywane przez tego samego dostawcę, Urząd ds. AI jest uprawniony do monitorowania i nadzorowania zgodności tego systemu AI z obowiązkami wynikającymi z niniejszego rozporządzenia. Do celów wykonywania zadania w zakresie monitorowania i nadzoru Urząd ds. AI ma uprawnienia organu nadzoru rynku w rozumieniu rozporządzenia (UE) 2019/1020.

2. W przypadku gdy odpowiednie organy nadzoru rynku mają wystarczający powód, by systemy AI ogólnego przeznaczenia, które przez podmioty stosujące AI mogą być wykorzystywane bezpośrednio do co najmniej jednego celu, który zgodnie z niniejszym rozporządzeniem został sklasyfikowany jako wysokiego ryzyka, uznać za niezgodne z wymogami ustanowionymi w niniejszym rozporządzeniu, organy te współpracują z Urzędem ds. AI w zakresie przeprowadzenia ocen zgodności i informują o tym odpowiednio Radę ds. AI i inne organy nadzoru rynku.

3. W przypadku gdy krajowy organ nadzoru rynku nie jest w stanie zakończyć postępowania dotyczącego systemu AI wysokiego ryzyka z uwagi na niemożność dostępu do niektórych informacji związanych z danym modelem AI pomimo podjęcia wszystkich stosownych wysiłków w zakresie uzyskania tych informacji, może zwrócić się z uzasadnionym wnioskiem do Urzędu ds. AI, który wyegzekwuje dostęp do takich informacji. W takim przypadku Urząd ds. AI udziela organowi wnioskującemu niezwłocznie, a w każdym razie w terminie 30 dni, wszelkich informacji, które Urząd ds. AI uznaje za istotne do celów ustalenia, czy dany system AI wysokiego ryzyka jest niezgodny z wymogami. Krajowe organy nadzoru rynku zapewniają poufność otrzymywanych informacji zgodnie z art. 78 niniejszego rozporządzenia. Odpowiednio stosuje się procedurę przewidzianą w rozdziale VI rozporządzenia (UE) 2019/1020.

Artykuł 76

Nadzór organów nadzoru rynku nad testami w warunkach rzeczywistych

1. *Organy nadzoru rynku mają kompetencje i uprawnienia do zapewnienia, by testy w warunkach rzeczywistych odbywały się zgodnie z niniejszym rozporządzeniem.*

2. *W przypadku testów w warunkach rzeczywistych prowadzonych na systemach AI nadzorowanych w ramach piaskownicy regulacyjnej w zakresie AI na podstawie art. 59 organy nadzoru rynku weryfikują zgodność z przepisami art. 60 w ramach swojej roli nadzorczej w odniesieniu do piaskownicy regulacyjnej w zakresie AI. Organy te mogą, w stosownych przypadkach, zezwolić na prowadzenie przez dostawcę lub potencjalnego dostawcę testów w warunkach rzeczywistych z zastosowaniem odstępstwa od warunków określonych w art. 60 ust. 4 lit. f) i g).*

3. *W przypadku gdy organ nadzoru rynku został przez potencjalnego dostawcę, dostawcę lub stronę trzecią poinformowany o poważnym incydencie lub ma podstawy sądzić, że nie są spełniane warunki określone w art. 60 i 61, może na swoim terytorium podjąć w stosownych przypadkach którąkolwiek z następujących decyzji:*

   a) zawiesić lub zakończyć testy w warunkach rzeczywistych;

b) zobowiązać dostawcę lub potencjalnego dostawcę i użytkowników do zmiany któregokolwiek aspektu testów w warunkach rzeczywistych.

4. W przypadku gdy organ nadzoru rynku podjął decyzję, o której mowa w ust. 3 niniejszego artykułu, lub zgłosił sprzeciw w rozumieniu art. 60 ust. 4 lit. b), w decyzji lub sprzeciwie podaje się ich uzasadnienie oraz warunki, na jakich dostawca lub potencjalny dostawca mogą zaskarżyć tę decyzję lub sprzeciw.

5. Tam, gdzie ma to zastosowanie, w przypadku gdy organ nadzoru rynku podjął decyzję, o której mowa w ust. 3, informuje o powodach takiej decyzji organy nadzoru rynku pozostałych państw członkowskich, w których dany system AI był testowany zgodnie z planem testów.

Artykuł 77

Uprawnienia organów ochrony praw podstawowych

1. Krajowe organy lub podmioty publiczne, które nadzorują lub egzekwują przestrzeganie obowiązków wynikających z prawa Unii służącego ochronie praw podstawowych, ***w tym prawa do niedyskryminacji***, w odniesieniu do stosowania systemów AI wysokiego ryzyka, o których mowa w załączniku III, są uprawnione do żądania wszelkiej dokumentacji sporządzonej lub prowadzonej na podstawie niniejszego rozporządzenia ***w przystępnym języku i formacie*** i uzyskania do niej dostępu, kiedy dostęp do tej dokumentacji jest im niezbędny do ***skutecznego wypełniania*** ich mandatów w granicach ich jurysdykcji. Odpowiedni organ lub podmiot publiczny informuje organ nadzoru rynku zainteresowanego państwa członkowskiego o każdym takim żądaniu.

2. Do dnia ... [***trzech*** miesięcy od wejścia w życie niniejszego rozporządzenia] każde państwo członkowskie wskaże organy lub podmioty publiczne, o których mowa w ust. 1, i poda ich wykaz do wiadomości publicznej ▌. Państwa członkowskie przekazują ten wykaz Komisji i pozostałym państwom członkowskim oraz na bieżąco go aktualizują.

3. W przypadku gdy dokumentacja, o której mowa w ust. 1, jest niewystarczająca do stwierdzenia, czy nastąpiło naruszenie obowiązków wynikających z unijnego prawa ochrony praw podstawowych, organ lub podmiot publiczny, o którym mowa w ust. 1, może wystąpić do organu nadzoru rynku z uzasadnionym wnioskiem o zorganizowanie testów systemu AI wysokiego ryzyka przy użyciu środków technicznych. Organ nadzoru rynku w rozsądnym terminie po otrzymaniu wniosku organizuje testy w ścisłej współpracy z organem lub podmiotem publicznym, które złożyły wniosek.

4. Wszelkie informacje lub dokumenty uzyskane zgodnie z niniejszym artykułem przez krajowe organy lub podmioty publiczne, o których mowa w ust. 1 niniejszego artykułu, traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 78.

Artykuł 78

Poufność

1. ***Komisja,*** organy ***nadzoru rynku*** i jednostki notyfikowane ***oraz wszelkie inne osoby fizyczne lub prawne*** zaangażowane w stosowanie niniejszego rozporządzenia zapewniają, ***zgodnie z prawem Unii i prawem krajowym***, poufność 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 Parlamentu Europejskiego i Rady(UE) 2016/943[60] w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem;

---

[60] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.U. L 157 z 15.6.2016, s. 1).

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

c) chronić interesy bezpieczeństwa publicznego i narodowego;

d) gwarantować uczciwy przebieg postępowań karnych i administracyjnych;

e) chronić informacje niejawne zgodnie z prawem Unii lub prawem krajowym.

2. Organy zaangażowane w stosowanie niniejszego rozporządzenia zgodnie z ust. 1 zwracają się wyłącznie o takie dane, które są im absolutnie niezbędne do oceny ryzyka stwarzanego przez systemy AI lub do wykonywania ich uprawnień zgodnie z niniejszym rozporządzeniem i rozporządzeniem (UE) 2019/1020. Wprowadzają odpowiednie i skuteczne środki w zakresie cyberbezpieczeństwa, aby chronić bezpieczeństwo i poufność uzyskanych informacji i danych oraz usuwają zgromadzone dane, gdy tylko przestaną one być potrzebne do celu, w jakim je uzyskano, zgodnie z mającym zastosowanie prawem unijnym lub krajowym.

3. Nie naruszając przepisów ust. 1 i ***2***, informacji wymienianych na zasadzie poufności między właściwymi organami krajowymi oraz między właściwymi organami krajowymi a Komisją nie można ujawniać bez uprzedniej konsultacji z właściwym organem krajowym, który je przekazał, oraz z ***podmiotem stosującym AI***, gdy z systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7, korzystają organy ścigania, ***organy kontroli granicznej***, organy imigracyjne lub organy azylowe, jeżeli takie ujawnienie mogłoby zagrozić interesom bezpieczeństwa publicznego i narodowego. ***Ta wymiana informacji nie obejmuje szczególnie chronionych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych.***

Jeżeli dostawcami systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 lub 7, są organy ścigania, organy imigracyjne lub organy azylowe, 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. 74 ust. 8 i 9, 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 posiadających poświadczenie bezpieczeństwa na odpowiednim poziomie.

4. Ust. 1***, 2*** i 3 pozostają bez uszczerbku dla praw i obowiązków Komisji, państw członkowskich i ***ich odpowiednich organów, a także*** jednostek notyfikowanych, w zakresie wymiany informacji i wydawania ostrzeżeń, ***w tym w kontekście współpracy transgranicznej***, nie wpływają one również na obowiązki zainteresowanych stron w zakresie udzielania informacji zgodnie z prawem karnym państw członkowskich.

5. Komisja i państwa członkowskie mogą, w razie potrzeby ***i zgodnie z odpowiednimi postanowieniami umów międzynarodowych i handlowych,*** wymieniać informacje poufne z organami regulacyjnymi państw trzecich, z którymi zawarły dwustronne lub wielostronne porozumienia o poufności gwarantujące odpowiedni stopień poufności.

Artykuł 79

Procedura postępowania na poziomie krajowym w przypadku systemów AI stwarzających ryzyko

1. Systemy AI stwarzające ryzyko uznaje się za produkt stwarzający ryzyko w rozumieniu art. 3 pkt 19 rozporządzenia (UE) 2019/1020 w zakresie, w jakim stwarzane przez nie ryzyko dotyczy zdrowia i bezpieczeństwa lub ▌ praw podstawowych obywateli.

2. W przypadku gdy organ nadzoru rynku państwa członkowskiego ma wystarczające powody, aby uznać, że system AI stwarza ryzyko, o którym mowa w ust. 1 niniejszego artykułu, organ ***ten*** przeprowadza ocenę danego systemu AI pod kątem jego zgodności ze wszystkimi wymogami i obowiązkami ustanowionymi w niniejszym rozporządzeniu. ***Szczególną uwagę należy zwrócić na systemy AI stwarzające ryzyko dla grup szczególnie wrażliwych, o których mowa w art. 5. W*** przypadku gdy zostanie ***stwierdzone*** ryzyko dla praw podstawowych pewnych osób, organ nadzoru rynku informuje o tym fakcie również odpowiednie krajowe organy lub podmioty publiczne, o których mowa w art. 77 ust. 1, ***i prowadzi z nimi pełną współpracę***. Operatorzy, których to dotyczy, współpracują odpowiednio z ***organem*** nadzoru rynku i innymi krajowymi organami lub podmiotami publicznymi, o których mowa w art. 77 ust. 1.

   W przypadku gdy w trakcie tej oceny organ nadzoru rynku lub, ***w stosownych przypadkach***, organ nadzoru rynku ***we współpracy z krajowym organem publicznym, o którym mowa w art. 77 ust. 1,*** stwierdzą, że system AI nie jest zgodny z wymogami i obowiązkami ustanowionymi w niniejszym rozporządzeniu, bez ***zbędnej*** zwłoki zobowiązuje danego operatora do podjęcia wszelkich odpowiednich działań naprawczych, aby zapewnić zgodność tego systemu AI z wymogami, wycofać ten system z rynku lub od użytkowników w wyznaczonym przez organ nadzoru rynku ***terminie, a w każdym razie w terminie krótszym niż 15 dni roboczych lub przewidzianym w odpowiednim unijnym prawodawstwie harmonizacyjnym.***

   Organ nadzoru rynku informuje o tym odpowiednią jednostkę notyfikowaną. Do środków, o których mowa w akapicie drugim niniejszego ustępu, zastosowanie ma art. 18 rozporządzenia (UE) nr 2019/1020.

3. W przypadku gdy organ nadzoru rynku uzna, że niezgodność nie ogranicza się do terytorium jego państwa, ***bez zbędnej zwłoki*** informuje Komisję i pozostałe 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 AI, które udostępnił na rynku w Unii.

5. W przypadku niepodjęcia przez operatora systemu AI 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 ***lub oddawania do użytku*** tego systemu AI na podległym mu rynku krajowym, lub w celu wycofania produktu ***lub samodzielnego systemu AI*** z tego rynku lub od użytkowników. Organ ten ***bez zbędnej zwłoki powiadamia*** ▌ o tych środkach Komisję i pozostałe państwa członkowskie.

6. W ***powiadomieniu***, o którym mowa w ust. 5, zawiera się wszelkie dostępne informacje szczegółowe, w szczególności takie jak informacje niezbędne do identyfikacji systemu AI niezgodnego z wymogami, pochodzenie systemu AI ***i informacje na temat jego łańcucha dostaw***, 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) nieprzestrzegania zakazu praktyk w zakresie AI, o których mowa w art. 5;

b) niespełnienia przez system AI ***wysokiego ryzyka*** wymogów określonych w rozdziale III sekcja 2;

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

d) nieprzestrzegania art. 50.

7. Organy nadzoru rynku państw członkowskich inne niż organ nadzoru rynku państwa członkowskiego, w którym wszczęto postępowanie, bez ***zbędnej*** zwłoki informują Komisję i pozostałe państwa członkowskie o wszelkich przyjętych środkach i o wszelkich posiadanych dodatkowych informacjach dotyczących niezgodności odnośnego systemu AI z przepisami, a w przypadku gdy nie zgadzają się ze zgłoszonym środkiem krajowym – o swoich zastrzeżeniach.

8. W przypadku gdy w terminie trzech miesięcy od dnia ***powiadomienia***, o którym mowa w ust. 5 niniejszego artykułu, ani ***organ nadzoru rynku jednego z*** państw członkowskich, ani Komisja nie zgłoszą sprzeciwu wobec środka tymczasowego przyjętego przez ***organ nadzoru rynku innego państwa członkowskiego***, środek ten uznaje się za uzasadniony. Pozostaje to bez uszczerbku dla praw proceduralnych danego operatora określonych w art. 18 rozporządzenia (UE) 2019/1020. ***Termin trzech miesięcy, o którym mowa w niniejszym ustępie, skraca się do 30 dni w przypadku nieprzestrzegania zakazu praktyk w zakresie AI, o których mowa w art. 5.***

9. Organy nadzoru rynku państw członkowskich zapewniają, by bez ***zbędnej*** zwłoki zostały wprowadzone odpowiednie środki ograniczające w odniesieniu do danego produktu ***lub systemu AI***, takie jak wycofanie produktu ***lub systemu AI*** z ich rynku.

Artykuł 80

Procedura postępowania w odniesieniu do systemów AI sklasyfikowanych przez dostawcę jako niebędące systemami wysokiego ryzyka w zastosowaniu załącznika III

1. *W przypadku gdy organ nadzoru rynku ma wystarczające powody, by sądzić, że system AI sklasyfikowany przez dostawcę zgodnie z art. 6 ust. 3 pkt I jako niebędący systemem wysokiego ryzyka jest w istocie systemem wysokiego ryzyka, organ ten przeprowadza ocenę danego systemu AI w zakresie jego klasyfikacji jako system AI wysokiego ryzyka na podstawie warunków określonych w art. 6 ust. 3 i wytycznych Komisji.*

2. *W przypadku gdy w trakcie tej oceny organ nadzoru rynku stwierdzi, że dany system AI jest systemem wysokiego ryzyka, bez zbędnej zwłoki nakłada na danego dostawcę obowiązek podjęcia wszystkich działań niezbędnych do osiągnięcia zgodności systemu AI z wymogami i obowiązkami ustanowionymi w niniejszym rozporządzeniu, jak również podjęcia odpowiednich działań naprawczych w terminie wyznaczonym przez organ nadzoru rynku.*

3. *W przypadku gdy organ nadzoru rynku uzna, że wykorzystywanie danego systemu AI nie ogranicza się do terytorium jego państwa, bez zbędnej zwłoki informuje Komisję i pozostałe państwa członkowskie o wynikach oceny i działaniach, do których podjęcia zobowiązał dostawcę.*

4. Dostawca zapewnia podjęcie wszystkich działań niezbędnych do zapewnienia zgodności danego systemu AI z wymogami i obowiązkami ustanowionymi w niniejszym rozporządzeniu. W przypadku gdy dostawca danego systemu AI nie zapewni zgodności tego systemu z tymi wymogami i obowiązkami w terminie, o którym mowa w ust. 2 niniejszego artykułu, dostawca ten podlega karom pieniężnym zgodnie z art. 99.

5. Dostawca zapewnia podjęcie wszelkich odpowiednich działań naprawczych w odniesieniu do wszystkich odnośnych systemów AI, które udostępnił na rynku w Unii.

6. W przypadku gdy dostawca danego systemu AI nie podejmie odpowiednich działań naprawczych w terminie, o którym mowa w ust. 2 niniejszego artykułu, zastosowanie ma art. 79 ust. 5–9.

7. W przypadku gdy w trakcie oceny zgodnie z ust. 1 niniejszego artykułu organ nadzoru rynku ustali, że dany system AI został przez dostawcę błędnie sklasyfikowany jako system niebędący systemem wysokiego ryzyka w celu obejścia stosowania wymogów zawartych w rozdziale III sekcja 2, dostawca ten podlega karom pieniężnym zgodnie z art. 99.

8. ***Wykonując swoje uprawnienia w zakresie monitorowania stosowania niniejszego artykułu oraz zgodnie z art. 11 rozporządzenia (UE) 2019/1020 organy nadzoru rynku mogą przeprowadzać odpowiednie kontrole, uwzględniając w szczególności informacje przechowywane w unijnej bazie danych, o której mowa w art. 71 niniejszego rozporządzenia.***

Artykuł 81

Unijna procedura ochronna

1. W przypadku gdy w terminie trzech miesięcy od dnia otrzymania powiadomienia, o którym mowa w art. 79 ust. 5, ***lub w terminie 30 dni w przypadku nieprzestrzegania zakazu praktyk w zakresie AI, o których mowa w art. 5***, ***organ nadzoru rynku jednego z państw członkowskich*** zgłosi sprzeciw wobec środka podjętego przez inny ***organ nadzoru rynku*** lub w przypadku gdy Komisja uzna taki środek za sprzeczny z prawem Unii, Komisja bez ***zbędnej*** zwłoki przystępuje do konsultacji z ***organem nadzoru rynku*** danego państwa członkowskiego i operatorem lub operatorami i dokonuje oceny takiego środka krajowego. Na podstawie wyników tej oceny Komisja w terminie ***sześciu*** miesięcy ***lub 60 dni – w przypadku nieprzestrzegania zakazu praktyk w zakresie AI, o których mowa w art. 5 – licząc*** od dnia otrzymania powiadomienia, o którym mowa w art. 79 ust. 5, rozstrzyga, czy środek krajowy jest uzasadniony, czy nie i powiadamia o swojej decyzji ***organ nadzoru rynku*** zainteresowanego państwa członkowskiego. ***Komisja powiadamia również wszystkie pozostałe krajowe organy nadzoru rynku o swojej decyzji.***

2. W przypadku gdy Komisja uzna, że ***środek podjęty przez dane państwo członkowskie*** jest uzasadniony, wszystkie państwa członkowskie ***zapewniają wprowadzenie bez zbędnej zwłoki odpowiednich*** środków ograniczających w ***odniesieniu do danego*** systemu AI, ***takich jak wymóg wycofania tego systemu AI*** z ich rynku, oraz informują o tym Komisję. W przypadku gdy Komisja uzna środek krajowy za nieuzasadniony, zainteresowane państwo członkowskie wycofuje dany środek ***oraz informuje odpowiednio Komisję***.

3. W przypadku uznania krajowego środka za uzasadniony i stwierdzenia, że niezgodność systemu AI 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 82

Zgodne z wymogami systemy AI stwarzające ryzyko

1. W przypadku gdy po przeprowadzeniu oceny zgodnie z art. 79, ***po konsultacji z odpowiednim krajowym organem publicznym, o którym mowa w art. 77 ust. 1***, organ nadzoru rynku państwa członkowskiego stwierdzi, że chociaż system AI ***wysokiego ryzyka*** jest zgodny z niniejszym rozporządzeniem, stwarza jednak ryzyko dla zdrowia lub bezpieczeństwa osób, ▌ dla praw podstawowych lub dla innych aspektów ochrony interesu publicznego, organ ten zobowiązuje właściwego operatora do podjęcia ***bez zbędnej zwłoki*** wszelkich odpowiednich środków w celu zapewnienia, aby odnośny system AI po wprowadzeniu do obrotu lub oddaniu do użytku nie stwarzał już takiego ryzyka, w ▌ wyznaczonym ▌ przez ten organ terminie.

2. Dostawca lub inny właściwy operator zapewniają podjęcie działań naprawczych w odniesieniu do wszystkich odnośnych systemów AI, które udostępnili na rynku w Unii, w terminie wyznaczonym przez organ nadzoru rynku państwa członkowskiego, o którym mowa w ust. 1.

3. Państwa ***członkowskie*** niezwłocznie powiadamiają Komisję i pozostałe państwa członkowskie o swoim ustaleniu zgodnie z ust. 1. W powiadomieniu tym zawiera się wszelkie dostępne szczegółowe informacje, w szczególności dane niezbędne do identyfikacji odnośnego systemu AI, pochodzenie systemu AI i informacje na temat jego łańcucha dostaw, charakter przedmiotowego ryzyka oraz charakter i okres obowiązywania zastosowanych środków krajowych.

4. Komisja bez ***zbędnej*** zwłoki przystępuje do konsultacji z państwem członkowskim lub państwami członkowskimi***, których to dotyczy,*** i właściwymi operatorami i ocenia zastosowane środki krajowe. Na podstawie wyników tej oceny Komisja podejmuje decyzję, czy środek krajowy jest uzasadniony, czy nie, i w razie potrzeby proponuje inne odpowiednie środki.

5. Komisja ***niezwłocznie przekazuje*** swoją decyzję do państw członkowskich ***i operatorów, których to dotyczy. Powiadamia również pozostałe państwa członkowskie.***

Artykuł 83

Niezgodność formalna

1. Organ nadzoru rynku państwa członkowskiego nakłada na właściwego dostawcę wymóg usunięcia niezgodności ***we wskazanym przez ten organ terminie***, w przypadku gdy ustali, że wystąpiło jedno z poniższych:

   a) umieszczenie oznakowania ***CE*** z naruszeniem art. 48;

   b) nieumieszczenie oznakowania ***CE***;

   c) nie sporządzono deklaracji zgodności UE;

   d) deklaracja zgodności UE została sporządzona nieprawidłowo;

   e) niedokonanie rejestracji w unijnej bazie danych;

   f) niewyznaczenie, w stosownych przypadkach, upoważnionego przedstawiciela;

   g) brak dokumentacji technicznej.

2. W przypadku gdy niezgodność, o której mowa w ust. 1, utrzymuje się, ***krajowy organ nadzoru rynku*** zainteresowanego państwa członkowskiego wprowadza wszelkie ***odpowiednie i proporcjonalne*** środki w celu ograniczenia lub zakazania udostępniania na rynku takiego systemu AI wysokiego ryzyka lub zapewnienia, aby system ten ***niezwłocznie*** wycofano z użytku lub z rynku.

Artykuł 84

Unijne struktury wsparcia testowania AI

1. *Komisja wyznacza co najmniej jedną unijną strukturę wsparcia testowania AI do wykonywania w obszarze AI zadań wymienionych w art. 21 ust. 6 rozporządzenia (UE) 1020/2019.*

2. *Bez uszczerbku dla zadań, o których mowa w ust. 1, unijne struktury wsparcia testowania AI zapewniają również niezależne doradztwo techniczne lub naukowe na wniosek Rady ds. AI, Komisji lub organów nadzoru rynku.*

Sekcja 4

Środki ochrony prawnej

Artykuł 85

Prawo do wniesienia skargi do organu nadzoru rynku

Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej każda osoba fizyczna lub prawna mająca podstawy, by uznać, że zostały naruszone przepisy niniejszego rozporządzenia, może wnieść uzasadnioną skargę do odpowiedniego organu nadzoru rynku.

Zgodnie z rozporządzeniem (UE) 2019/1020 takie skargi uwzględnia się do celów prowadzenia działań w zakresie nadzoru rynku i rozpatruje zgodnie ze specjalnymi procedurami ustanowionymi w związku z tym przez organy nadzoru rynku.

Artykuł 86

Prawo do wyjaśnienia indywidualnego procesu podejmowania decyzji

1. *Każda osoba będąca przedmiotem decyzji podjętej przez podmiot stosujący AI na podstawie wyników działania systemu AI wysokiego ryzyka wymienionego w załączniku III, z wyjątkiem systemów wymienionych w pkt 2 tego załącznika, która to decyzja generuje skutki prawne lub w podobny sposób oddziałuje na tę osobę na tyle znacząco, że uważa ona, iż ma to niepożądany wpływ na jej zdrowie, bezpieczeństwo lub prawa podstawowe, ma prawo uzyskania od podmiotu stosującego AI merytorycznego wyjaśnienia roli tego systemu AI w procedurze podejmowania decyzji oraz głównych elementów podjętej decyzji.*

2. *Ust. 1 nie ma zastosowania do wykorzystywania systemów AI, w odniesieniu do których z prawa Unii lub zgodnego z prawem Unii prawa krajowego wynikają wyjątki od stosowania obowiązku na podstawie ust. 1 lub jego ograniczenia.*

3. *Niniejszy artykuł stosuje się jedynie w zakresie, w jakim prawo, o którym mowa w ust. 1, nie zostało inaczej przewidziane na podstawie prawa Unii.*

Artykuł 87

Zgłaszanie naruszeń i ochrona osób dokonujących zgłoszeń

W odniesieniu do przypadków zgłaszania naruszeń niniejszego rozporządzenia oraz w kwestiach ochrony osób zgłaszających takie naruszenia zastosowanie mają przepisy dyrektywy (UE) 2019/1937.

Sekcja 5

Nadzór, postępowania, egzekwowanie i monitorowanie w odniesieniu do dostawców modeli AI ogólnego przeznaczenia

Artykuł 88

Egzekwowanie obowiązków dostawców modeli AI ogólnego przeznaczenia

1. Komisja ma wyłączne uprawnienia do nadzorowania i egzekwowania przestrzegania przepisów rozdziału V, przy uwzględnieniu gwarancji proceduralnych na podstawie art. 94. Komisja powierza realizację tych zadań Urzędowi ds. AI, bez uszczerbku dla uprawnień organizacyjnych Komisji i podziału kompetencji między państwami członkowskimi a Unią na podstawie Traktatów.

2. Bez uszczerbku dla art. 75 ust. 3 organy nadzoru rynku mogą zwrócić się do Komisji o wykonanie uprawnień ustanowionych w niniejszej sekcji, w przypadku gdy będzie to konieczne i proporcjonalne w kontekście realizacji ich zadań na podstawie niniejszego rozporządzenia.

Artykuł 89

Działania monitorujące

1. *Do celów wykonywania zadań powierzonych w niniejszej sekcji Urząd ds. AI może podjąć działania niezbędne do monitorowania skutecznego wdrożenia i przestrzegania niniejszego rozporządzenia przez dostawców modeli AI ogólnego przeznaczenia, w tym przestrzegania przez nich zatwierdzonych kodeksów praktyk.*

2. *Dostawcy niższego szczebla mają prawo wniesienia skargi dotyczącej naruszenia niniejszego rozporządzenia. Skarga musi być należycie uzasadniona i zawierać co najmniej:*

   a) *dane kontaktowe danego dostawcy modelu AI ogólnego przeznaczenia;*

   b) *opis istotnych faktów, odnośne przepisy niniejszego rozporządzenia oraz powody, dla których dostawca niższego szczebla uważa, że dostawca systemu AI ogólnego przeznaczenia naruszył niniejsze rozporządzenie;*

   c) *wszelkie inne informacje uznane za istotne przez dostawcę niższego szczebla, który wysłał zgłoszenie, w tym, w stosownych przypadkach, informacje zebrane z własnej inicjatywy.*

Artykuł 90

Ostrzeżenia o ryzyku systemowym wydawane przez panel naukowy

1. *Panel naukowy może wydawać ostrzeżenia kwalifikowane skierowane do Urzędu ds. AI, w przypadku gdy ma powody podejrzewać, że:*

   a) *model AI ogólnego przeznaczenia stwarza konkretne możliwe do zidentyfikowania ryzyko na poziomie Unii; lub*

   b) *model AI ogólnego przeznaczenia spełnia wymogi, o których mowa w art. 51.*

2. *Po otrzymaniu takiego ostrzeżenia kwalifikowanego Komisja, za pośrednictwem Urzędu ds. AI i po poinformowaniu Rady ds. AI, może wykonać swoje uprawnienia ustanowione w niniejszym rozdziale do celów oceny przedmiotowej kwestii. Urząd ds. AI informuje Radę ds. AI o wszelkich środkach zgodnie z art. 91–94.*

3. *Ostrzeżenie kwalifikowane musi być należycie uzasadnione i zawierać co najmniej:*

   a) *dane kontaktowe danego dostawcy modelu AI ogólnego przeznaczenia z ryzykiem systemowym;*

b) opis stosownych faktów i uzasadnienie wydania ostrzeżenia przez panel naukowy;

c) wszelkie inne informacje, które panel naukowy uważa za istotne, w tym, w stosownych przypadkach, informacje zebrane z własnej inicjatywy.

Artykuł 91

Uprawnienie do zwracania się o dokumentację i informacje

1. Komisja może zwrócić się do danego dostawcy modelu AI ogólnego przeznaczenia o przedstawienie dokumentacji sporządzonej przez dostawcę zgodnie art. 53 i 55 lub o wszelkie dodatkowe informacje niezbędne do celów oceny zgodności danego dostawcy z niniejszym rozporządzeniem.

2. Przed wysłaniem wniosku o przedstawienie informacji Urząd ds. AI może rozpocząć zorganizowany dialog z dostawcą modelu AI ogólnego przeznaczenia.

3. Na należycie uzasadniony wniosek panelu naukowego Komisja może skierować do dostawcy modelu AI ogólnego przeznaczenia wniosek o udzielenie informacji, w przypadku gdy dostęp do informacji jest niezbędny i proporcjonalny w kontekście realizacji zadań panelu naukowego na podstawie art. 68 ust. 2.

4. We wniosku o udzielenie informacji określa się podstawę prawną i cel wniosku, podaje, jakie informacje są wymagane oraz określa się termin na dostarczenie tych informacji, a także wskazuje przewidziane w art. 101 kary pieniężne za podawanie informacji nieprawidłowych, niekompletnych lub wprowadzających w błąd.

5. Dostawca danego modelu AI ogólnego przeznaczenia lub jego przedstawiciel dostarczają żądane informacje. W przypadku osób prawnych, spółek lub firm lub w przypadku gdy dostawca nie ma osobowości prawnej, osoby upoważnione do ich reprezentowania z mocy prawa lub na podstawie aktu założycielskiego dostarczają żądane informacje w imieniu danego dostawcy modelu AI ogólnego przeznaczenia. Prawnicy należycie upoważnieni do działania mogą przekazać informacje w imieniu swoich klientów. Klienci pozostają jednak w pełni odpowiedzialni za informacje, jeśli przekazane informacje są nieprawidłowe, niekompletne lub wprowadzające w błąd.

Artykuł 92

Uprawnienia do przeprowadzania ocen

1. Urząd ds. AI po konsultacji z Radą ds. AI może przeprowadzać oceny danego modelu AI ogólnego przeznaczenia:

a) do celów oceny przestrzegania przez danego dostawcę obowiązków na podstawie niniejszego rozporządzenia, w przypadku gdy informacje zgromadzone zgodnie z art. 91 są niewystarczające; lub

b) do celów badania na poziomie Unii ryzyka systemowego modeli AI ogólnego przeznaczenia z ryzykiem systemowym, w szczególności w następstwie sprawozdania kwalifikowanego panelu naukowego zgodnie z art. 89 ust. 1 lit. a).

2. Komisja może podjąć decyzję o powołaniu niezależnych ekspertów do przeprowadzania ocen w jej imieniu, w tym z panelu naukowego ustanowionego zgodnie z art. 68. Niezależni eksperci powołani do tego zadania spełniają kryteria określone w art. 68 ust. 2.

3. Do celów ust. 1 Komisja może zwrócić się o dostęp do danego modelu AI ogólnego przeznaczenia za pośrednictwem API lub innych odpowiednich środków i narzędzi technicznych, w tym do kodu źródłowego.

4. We wniosku o udzielenie dostępu określa się podstawę prawną, cel i uzasadnienie wniosku oraz określa się termin na udzielenie tego dostępu, a także wskazuje przewidziane w art. 101 kary pieniężne za nieudzielenie dostępu.

5. Dostawcy modeli AI ogólnego przeznaczenia oraz, w przypadku osób prawnych, spółek lub firm nieposiadających osobowości prawnej, osoby upoważnione do ich reprezentowania z mocy prawa lub na podstawie aktu założycielskiego udzielają żądanego dostępu w imieniu danego dostawcy modelu AI ogólnego przeznaczenia.

6. Komisja przyjmuje akty wykonawcze określające szczegółowe ustalenia i warunki ocen, w tym szczegółowe ustalenia dotyczące udziału niezależnych ekspertów, oraz procedurę ich wyboru. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

7. Przed zwróceniem się o dostęp do danego modelu AI ogólnego przeznaczenia Urząd ds. AI może rozpocząć zorganizowany dialog z dostawcą danego modelu AI ogólnego przeznaczenia, aby zgromadzić więcej informacji na temat wewnętrznych testów modelu, wewnętrznych zabezpieczeń przed ryzykiem systemowym oraz innych wewnętrznych procedur i środków, jakie dostawca podjął w celu ograniczenia takiego ryzyka.

Artykuł 93

Uprawnienia do wymagania wprowadzenia środków

1. W miarę konieczności i w stosownych przypadkach Komisja może zwrócić się do dostawców o:

a) podjęcie odpowiednich środków w celu wypełnienia obowiązków określonych w art. 53;

b) wdrożenie środków zaradczych, w przypadku gdy z oceny przeprowadzonej zgodnie z art. 92 wynika poważna i uzasadniona obawa wystąpienia ryzyka systemowego na poziomie Unii;

c) ograniczenie udostępniania modelu na rynku, wycofanie modelu z obrotu lub od użytkowników.

2. Przed zwróceniem się z wnioskiem o wprowadzenie środka Urząd ds. AI może rozpocząć zorganizowany dialog z dostawcą modelu AI ogólnego przeznaczenia.

3. Jeśli w trakcie zorganizowanego dialogu, o którym mowa w ust. 2, dostawca modelu AI ogólnego przeznaczenia z ryzykiem systemowym zobowiąże się do wprowadzenia środków zaradczych w celu przeciwdziałania ryzyku systemowemu na poziomie Unii, Komisja może w drodze decyzji uczynić te zobowiązania wiążącymi i oświadczyć, że nie ma podstaw do dalszych działań.

Artykuł 94

Prawa proceduralne podmiotów gospodarczych zajmujących się modelami AI ogólnego przeznaczenia

Art. 18 rozporządzenia (UE) 2019/1020 stosuje się odpowiednio do dostawców modeli AI ogólnego przeznaczenia, bez uszczerbku dla bardziej szczegółowych praw proceduralnych przewidzianych w niniejszym rozporządzeniu.

ROZDZIAŁ X

KODEKSY POSTĘPOWANIA I WYTYCZNE

Artykuł 95

Kodeksy postępowania do celów dobrowolnego stosowania szczególnych wymogów

1. ***Urząd ds. AI*** i państwa członkowskie wspierają i ułatwiają opracowywanie kodeksów postępowania, ***w tym powiązanych mechanizmów zarządzania***, mających zachęcać do dobrowolnego stosowania w odniesieniu do systemów AI niebędących systemami wysokiego ryzyka ***niektórych lub wszystkich*** wymogów określonych w rozdziale III sekcja 2, ***przy uwzględnieniu dostępnych rozwiązań technicznych i najlepszych praktyk branżowych umożliwiających stosowanie takich wymogów***.

2. ***Urząd ds. AI*** i ***państwa członkowskie*** umożliwiają ▌ opracowywanie kodeksów postępowania ***dotyczących*** dobrowolnego stosowania, ***również przez podmioty stosujące AI, szczególnych wymogów w odniesieniu do wszystkich*** systemów AI, ***na podstawie jasnych celów i kluczowych wskaźników skuteczności działania służących do pomiaru stopnia realizacji tych celów, z uwzględnieniem między innymi następujących elementów:***

a) mające zastosowanie elementy przewidziane w unijnych wytycznych etycznych dotyczących godnej zaufania AI;

b) ocena i minimalizacja wpływu systemów AI na zrównoważenie środowiskowe, w tym w odniesieniu do energooszczędnego programowania i technik wydajnego projektowania, trenowania i wykorzystywania AI;

c) promowanie kompetencji w zakresie AI, w szczególności w odniesieniu do osób mających związek z opracowywaniem, funkcjonowaniem i wykorzystywaniem AI;

d) sprzyjanie inkluzywności i różnorodności przy projektowaniu systemów AI, w tym poprzez tworzenie inkluzywnych i różnorodnych zespołów programistycznych oraz promowanie udziału zainteresowanych stron w tym procesie;

e) ocena i zapobieganie negatywnemu oddziaływaniu systemów AI na osoby szczególnie wrażliwe lub grupy osób szczególnie wrażliwych, w tym z punktu widzenia dostępności dla osób z niepełnosprawnościami, jak również na równość płci.

3. Kodeksy postępowania mogą być opracowywane przez poszczególnych dostawców systemów AI ***lub podmioty stosujące systemy AI*** lub przez reprezentujące ich organizacje lub też przez obie te grupy, w tym przy udziale ***podmiotów stosujących AI*** i wszelkich zainteresowanych stron oraz reprezentujących je organizacji, ***w tym organizacji społeczeństwa obywatelskiego i środowiska akademickiego***. Kodeksy postępowania mogą obejmować jeden lub większą liczbę systemów AI, przy uwzględnieniu podobieństw w przeznaczeniu danych systemów.

4. W ramach zachęcania do tworzenia kodeksów postępowania i ułatwiania ich tworzenia ***Urząd ds. AI*** i ***państwa członkowskie*** uwzględniają szczególne interesy i potrzeby ***MŚP, w tym*** przedsiębiorstw typu start-up.

Artykuł 96

Wytyczne Komisji w sprawie wdrożenia niniejszego rozporządzenia

1. Komisja opracowuje wytyczne dotyczące praktycznego wdrażania niniejszego rozporządzenia, a w szczególności:

a) stosowania wymogów i obowiązków, o których mowa w art. 8–15 i art. 25;

b) zakazanych praktyk, o których mowa w art. 5;

c) praktycznego wdrażania przepisów dotyczących istotnych zmian;

d) praktycznego wdrażania obowiązków w zakresie przejrzystości ustanowionych w art. 50;

e) podawania szczegółowych informacji na temat powiązań między niniejszym rozporządzeniem a unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I, jak również z innym odpowiednim prawem Unii, w tym w odniesieniu do spójności jego egzekwowania;

f) stosowania definicji systemu AI określonej w art. 3 ust. 1.

Przy wydawaniu takich wytycznych Komisja zwraca szczególną uwagę na potrzeby MŚP, w tym przedsiębiorstw typu start-up, lokalnych organów publicznych i sektorów, na które niniejsze rozporządzenie będzie miało największy wpływ.

Wytyczne, o których mowa w akapicie pierwszym, uwzględniają powszechnie uznany stan wiedzy technicznej w zakresie AI, jak również odpowiednie normy zharmonizowane i wspólne specyfikacje, o których mowa w art. 40 i 41, lub te normy zharmonizowane lub specyfikacje techniczne, które zostały określone zgodnie z unijnym prawodawstwem harmonizacyjnym.

2. Na wniosek państw członkowskich lub Urzędu ds. AI lub z własnej inicjatywy Komisja aktualizuje przyjęte już wytyczne, jeżeli zostanie to uznane za konieczne.

ROZDZIAŁ XI
PRZEKAZANIE UPRAWNIEŃ I PROCEDURA KOMITETOWA

Artykuł 97

Wykonywanie przekazanych uprawnień

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

2. ***Uprawnienia do przyjmowania aktów delegowanych***, o których mowa w art. 6 ust. 6, art. 7 ust. 1 i 3, art. 11 ust. 3, art. 43 ust. 5 i 6, art. 47 ust. 5, ***art. 51 ust. 3, art. 52 ust. 4 i art. 53 ust. 5 i 6*** powierza się Komisji na okres ***pięciu lat od dnia … [dzień wejścia*** w życie niniejszego rozporządzenia]. ***Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem tego okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.***

3. Przekazanie uprawnień, o którym mowa w art. 6 ust. 6, art. 7 ust. 1 i 3, art. 11 ust. 3, art. 43 ust. 5 i 6, art. 47 ust. 5, ***art. 51 ust. 3, art. 52 ust. 4 i art. 53 ust. 5 i 6***, 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 następnego dnia po jej opublikowaniu w ***Dzienniku Urzędowym Unii Europejskiej*** lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

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

6. Akt delegowany przyjęty na podstawie art. 6 ust. 6, art. 7 ust. 1 i 3, art. 11 ust. 3, art. 43 ust. 5 i 6, art. 47 ust. 5, ***art. 51 ust. 3, art. 52 ust. 4 i art. 53 ust. 5 i 6*** 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 98

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.

ROZDZIAŁ XII
KARY

Artykuł 99

Kary

1. Zgodnie z zasadami i warunkami ustanowionymi w niniejszym rozporządzeniu państwa członkowskie ustanawiają przepisy dotyczące kar ***i innych środków egzekwowania prawa, które mogą również obejmować ostrzeżenia i środki niepieniężne***, mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia ***przez operatorów*** i podejmują wszelkie działania niezbędne do zapewnienia ich właściwego i skutecznego wdrożenia, ***z uwzględnieniem wytycznych wydanych przez Komisję zgodnie z*** art. 96. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Uwzględniają one ▌ interesy ***MŚP, w tym przedsiębiorstw typu start-up***, oraz ich sytuację ekonomiczną.

2. Państwa członkowskie ***niezwłocznie, nie później jednak niż do dnia rozpoczęcia stosowania***, powiadamiają Komisję o przepisach dotyczących kar i innych środków egzekwowania prawa, o których mowa w ust. 1, jak również o ich wszelkich późniejszych zmianach.

3. ***Nieprzestrzeganie zakazu praktyk w zakresie AI, o których mowa w art. 5***, podlega administracyjnej karze pieniężnej w wysokości do ***35 000 000*** EUR lub – jeżeli naruszenia dokonuje ***przedsiębiorstwo*** – w wysokości do ***7*** % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

4. ▌ Niezgodność systemu AI z ***którymkolwiek z wymienionych poniżej przepisów dotyczących operatorów lub jednostek notyfikowanych***, poza przepisami ustanowionymi w art. 5 ▌, podlega administracyjnej karze pieniężnej w wysokości do ***15 000 000*** EUR lub – jeżeli naruszenia dokonuje przedsiębiorstwo – w wysokości do ***3*** % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa:

   a) obowiązki dostawców zgodnie z art. 16;

   b) obowiązki upoważnionych przedstawicieli zgodnie z art. 22;

   c) obowiązki importerów zgodnie z art. 23;

d) obowiązki dystrybutorów zgodnie z art. 24;

e) obowiązki podmiotów stosujących AI zgodnie z art. 26;

f) wymogi i obowiązki jednostek notyfikowanych zgodnie z art. 31, art. 33 ust. 1, art. 33 ust. 3, art. 33 ust. 4 lub art. 34;

g) obowiązki dostawców i użytkowników w zakresie przejrzystości zgodnie z art. 50.

5. Przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym lub właściwym organom krajowym w odpowiedzi na ich wezwanie podlega administracyjnej karze pieniężnej w wysokości do ***7 500 000*** EUR lub – jeżeli naruszenia dokonuje przedsiębiorstwo – w wysokości do ***1*** % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot jest wyższa.

6. W przypadku MŚP, w tym przedsiębiorstw typu start-up, każda kara pieniężna, o której mowa w niniejszym artykule, ma wysokość do wartości procentowej lub kwoty, o których mowa w ust. 3, 4 lub 5, w zależności od tego, która z tych wartości jest niższa.

7. Przy podejmowaniu decyzji, ***czy nałożyć administracyjną karę pieniężną, oraz przy ustalaniu*** jej wysokości, uwzględnia się wszystkie istotne okoliczności danej sytuacji w każdym indywidualnym przypadku i zwraca się ***w stosownych przypadkach*** uwagę na:

a) charakter, wagę i czas trwania naruszenia oraz jego konsekwencje, ***przy uwzględnieniu przeznaczenia systemu sztucznej inteligencji, a także, w stosownych przypadkach, liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody;***

b) czy inne organy nadzoru rynku ***w co najmniej jednym innym państwie członkowskim*** nałożyły już na tego samego operatora administracyjne kary pieniężne za to samo naruszenie;

c) czy inne organy nałożyły już administracyjne kary pieniężne na tego samego operatora za naruszenia innych przepisów prawa Unii lub prawa krajowego, w przypadku gdy takie naruszenia wynikają z tego samego działania lub zaniechania stanowiącego odnośne naruszenie niniejszego rozporządzenia;

d) wielkość operatora dopuszczającego się naruszenia, jego ***roczny obrót*** i udział w rynku;

e) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak bezpośrednio lub pośrednio powiązane z danym naruszeniem osiągnięte korzyści finansowe lub uniknięte straty;

f) stopień współpracy z właściwym organem krajowym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych niepożądanych skutków;

g) stopień odpowiedzialności operatora, z uwzględnieniem wdrożonych przez niego środków technicznych i organizacyjnych;

h) sposób, w jaki właściwe organy krajowe dowiedziały się o naruszeniu, w szczególności czy i w jakim zakresie operator zgłosił naruszenie;

i) umyślny lub wynikający z zaniedbania charakter naruszenia;

j) wszelkie działania podjęte przez operatora w celu złagodzenia szkody poniesionej przez poszkodowane osoby.

8. Każde państwo członkowskie ustanawia przepisy dotyczące określenia ▌, w jakim zakresie na organy i podmioty publiczne ustanowione w tym państwie członkowskim można nakładać administracyjne kary pieniężne.

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

10. Wykonywanie przez organ nadzoru rynku uprawnień powierzonych mu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom proceduralnym zgodnie z prawem Unii i prawem krajowym, obejmującym prawo do skutecznych środka zaskarżenia i rzetelnego postępowania sądowego.

11. Państwa członkowskie co roku składają Komisji sprawozdanie dotyczące administracyjnych kar pieniężnych, które nałożyły w danym roku zgodnie z niniejszym artykułem, oraz dotyczące wszelkich powiązanych sporów lub postępowań sądowych.

Artykuł 100

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 wysokości, uwzględnia się wszystkie istotne okoliczności danej sytuacji w każdym indywidualnym przypadku i zwraca się należytą uwagę na:

   a) charakter, wagę i czas trwania naruszenia oraz jego konsekwencji; ***przy uwzględnieniu przeznaczenia systemu AI, a także liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody, oraz wszelkich istotnych wcześniejszych naruszeń;***

b) stopień odpowiedzialności instytucji, organu lub jednostki organizacyjnej Unii, z uwzględnieniem wdrożonych przez nie środków technicznych i organizacyjnych;

c) wszelkie działania podjęte przez instytucję, organ lub jednostkę organizacyjną Unii w celu złagodzenia szkody poniesionej przez osoby poszkodowane;

d) ***stopień*** współpracy z Europejskim Inspektorem Ochrony Danych w celu usunięcia naruszenia i złagodzenia jego ewentualnych niepożądanych skutków, w tym zastosowanie się do wszelkich środków zarządzonych wcześniej przez Europejskiego Inspektora Ochrony Danych wobec danej instytucji, organu lub jednostki organizacyjnej Unii w odniesieniu do tej samej kwestii;

e) wszelkie podobne wcześniejsze naruszenia dokonane przez instytucję, organ, lub jednostkę organizacyjną Unii;

f) sposób, w jaki Europejski Inspektor Ochrony Danych dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie instytucja, organ lub jednostka organizacyjna Unii zgłosili naruszenie;

g) roczny budżet instytucji, organu lub jednostki organizacyjnej Unii.

2. ***Nieprzestrzeganie zakazu praktyk związanych z AI, o których mowa w art. 5***, podlega administracyjnym karom pieniężnym w wysokości do ***1 500 000 EUR***.

3. Niezgodność systemu AI z jakimikolwiek wymogami lub obowiązkami wynikającymi z niniejszego rozporządzenia, innymi niż te ustanowione w art. 5, podlega administracyjnej karze pieniężnej w wysokości do ***750 000*** 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 pieniężnych nałożonych na podstawie niniejszego artykułu ***zasilają budżet ogólny Unii***. ***Te kary pieniężne nie mogą mieć wpływu na skuteczne funkcjonowanie instytucji, organu lub jednostki organizacyjnej*** Unii, ***na które nałożono karę.***

7. Europejski Inspektor Ochrony Danych co roku powiadamia Komisję o administracyjnych karach pieniężnych, które nałożył zgodnie z niniejszym artykułem, oraz o wszelkich wszczętych przez siebie postępowaniach spornych lub sądowych.

Artykuł 101

Kary pieniężne dla dostawców modeli AI ogólnego przeznaczenia

1. Komisja może nakładać na dostawców modeli AI ogólnego przeznaczenia kary pieniężne nieprzekraczające 3 % ich całkowitego światowego obrotu w poprzednim roku obrotowym lub 15 mln EUR, w zależności od tego, która z tych kwot jest wyższa, jeśli stwierdzi, że dostawca celowo lub w wyniku zaniedbania:

a) naruszył odpowiednie przepisy niniejszego rozporządzenia;

b) nie zastosował się do wniosku o przedłożenie dokumentu lub informacji zgodnie z art. 91 lub przedłożył informacje nieprawidłowe, niekompletne lub wprowadzające w błąd;

c) nie zastosował się do środka wymaganego na podstawie art. 93;

d) nie udzielił Komisji dostępu – w celu przeprowadzenia oceny zgodnie z art. 92 – do modelu AI ogólnego przeznaczenia lub modelu AI ogólnego przeznaczenia z ryzykiem systemowym.

Przy ustalaniu kwoty kary pieniężnej lub okresowej kary pieniężnej bierze się pod uwagę charakter, wagę i czas trwania naruszenia z należytym uwzględnieniem zasad proporcjonalności i adekwatności. Komisja uwzględnia również zobowiązania podjęte zgodnie z art. 93 ust. 3 lub podjęte w odpowiednich kodeksach praktyki zgodnie z art. 56.

2. Przed przyjęciem decyzji zgodnie z ust. 1 Komisja przekazuje swoje wstępne ustalenia dostawcy modelu AI ogólnego przeznaczenia lub modelu AI ogólnego przeznaczenia z ryzykiem systemowym i daje mu możliwość przedstawienia swojego stanowiska.

3. Kary pieniężne nakładane zgodnie z niniejszym artykułem są skuteczne, proporcjonalne i odstraszające.

4. Informacje na temat kar pieniężnych nałożonych na podstawie niniejszego artykułu przekazuje się w stosownych przypadkach również Radzie ds. AI.

5. Trybunał Sprawiedliwości Unii Europejskiej ma nieograniczoną jurysdykcję w zakresie rozpatrywania odwołań od decyzji Komisji ustalających karę pieniężną na podstawie niniejszego artykułu. Może on uchylić, obniżyć lub podwyższyć nałożoną karę pieniężną.

6. Komisja przyjmuje akty wykonawcze zawierające szczegółowe ustalenia dotyczące postępowania w celu ewentualnego przyjęcia decyzji zgodnie z ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

ROZDZIAŁ XIII
PRZEPISY KOŃCOWE

Artykuł 102

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 dotyczącymi zatwierdzania i wykorzystywania sprzętu służącego do ochrony w odniesieniu do systemów AI w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/… [*+] uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 103

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) 2024/...[*+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 104

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) 2024/... [*+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 105

Zmiana dyrektywy 2014/90/UE

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

„5. W odniesieniu do systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/…[*+], 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 Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 106

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) 2024/…[*+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 107

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) 2024/…[*+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 108

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) 2024/…[*+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”;

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) 2024/...[++], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”;

[+] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

[++] Dz.U.: Proszę wstawić numer niniejszego rozporządzenia (2021/0106(COD)).

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) 2024/...[+], 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) 2024/...[+], 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) 2024/...[+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”;

[+] Dz.U.: Proszę wstawić numer niniejszego rozporządzenia (2021/0106(COD)).

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) 2024/...[+], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.”.

Artykuł 109

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) 2024/…[*++], uwzględnia się wymogi określone w tytule III rozdział 2 tego rozporządzenia.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …).”

[+] Dz.U.: Proszę wstawić numer niniejszego rozporządzenia (2021/0106(COD)).

[++] Dz.U.: Proszę wstawić w tekście numer niniejszego rozporządzenia (2021/0106 (COD)) oraz uzupełnić odpowiadający przypis.

Artykuł 110

Zmiana dyrektywy (UE) 2020/1828

W załączniku I do dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/1828*[61] *dodaje się punkt w brzmieniu:

„***(68)*** Rozporządzenie ***Parlamentu Europejskiego i Rady (UE) 2024/... z dnia … ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Dz.U. L ..., ELI: …)***”.

---

[61] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/1828 z dnia 25 listopada 2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz.U. L 409 z 4.12.2020, s. 1).

Artykuł 111

Systemy AI już wprowadzone do obrotu lub oddane do użytku

1. ***Bez uszczerbku dla stosowania art. 5, jak określono w art.*** 113 ust. 3 lit. a), ***do dnia 31 grudnia 2030 r. zapewnia się zgodność z niniejszym rozporządzeniem*** w odniesieniu do systemów AI, które stanowią elementy wielkoskalowych systemów informatycznych utworzonych na podstawie aktów prawnych wymienionych w załączniku X i które wprowadzono do obrotu lub oddano do użytku przed dniem ▌ ... [36 miesięcy od daty wejścia w życie niniejszego rozporządzenia].

   Wymogi ustanowione w niniejszym rozporządzeniu uwzględnia się ▌ w ocenach każdego z wielkoskalowego systemu informatycznego utworzonego na podstawie aktów prawnych wymienionych w załączniku X, które to oceny przeprowadza się zgodnie z tymi aktami ***oraz w przypadku gdy te akty prawne są zastępowane lub zmieniane***.

2. ***Bez uszczerbku dla stosowania art. 5, jak określono w art. 113 ust. 3 lit. a)*** niniejsze rozporządzenie ma zastosowanie do ***operatorów*** systemów AI wysokiego ryzyka innych niż systemy, o których mowa w ust. 1 niniejszego artykułu, które zostały wprowadzone do obrotu lub oddane do użytku przed dniem ... [24 miesiące od daty wejścia w życie niniejszego rozporządzenia] tylko wtedy, gdy po tej dacie w systemach tych wprowadzane będą istotne zmiany w ich ***projekcie***. ***W przypadku systemów AI wysokiego ryzyka, które*** mają być ***wykorzystywane przez organy publiczne, dostawcy i podmioty stosujące takie systemy podejmują niezbędne kroki w celu spełnienia wymogów niniejszego rozporządzenia do dnia ... [sześć lat od daty wejścia w życie niniejszego rozporządzenia].***

3. Dostawcy modeli AI ogólnego przeznaczenia, które zostały wprowadzone do obrotu przed dniem ... [12 miesięcy od daty wejścia w życie niniejszego rozporządzenia***] podejmują niezbędne kroki w celu wypełnienia obowiązków ustanowionych w niniejszym rozporządzeniu do dnia ... [36 miesięcy*** od daty wejścia w życie niniejszego rozporządzenia].

Artykuł 112

Ocena i przegląd

1. Komisja ocenia potrzebę wprowadzenia zmian w wykazie zawartym w załączniku III ***oraz w określonym w art. 5 wykazie zakazanych praktyk w zakresie AI*** raz w roku, począwszy od daty wejścia w życie niniejszego rozporządzenia ***do końca okresu przekazania uprawnień określonych w art. 97. Komisja przedstawia wyniki tej oceny Parlamentowi Europejskiemu i Radzie.***

2. Do dnia ... ***[cztery lata od daty wejścia w życie niniejszego rozporządzenia], a następnie co cztery lata Komisja przeprowadzi ocenę i przedłoży Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące:***

   a) konieczności zmian w postaci rozszerzenia istniejących nagłówków dotyczących obszarów lub dodania nowych nagłówków dotyczących obszarów w załączniku III;

   b) zmian wykazu systemów AI wymagających dodatkowych środków w zakresie przejrzystości określonych w art. 50;

   c) zmian w celu poprawy skuteczności systemu nadzoru i zarządzania.

3. Do dnia ... [cztery lata od daty wejścia w życie niniejszego rozporządzenia], a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia. ***Sprawozdanie zawiera ocenę struktury egzekwowania przepisów i ewentualnej konieczności usunięcia wszelkich stwierdzonych niedociągnięć przez agencję unijną. Na podstawie tych ustaleń do sprawozdania dołącza się, w stosownych przypadkach, wniosek dotyczący zmiany niniejszego rozporządzenia.*** Sprawozdania te są podawane do wiadomości publicznej.

4. W sprawozdaniach, o których mowa w ust. 2, szczególną uwagę zwraca się na następujące kwestie:

   a) stan zasobów finansowych, ***technicznych*** i zasobów ludzkich właściwych organów krajowych konieczny, 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. 99 ust. 1, nakładanych przez państwa członkowskie w przypadku naruszenia niniejszego rozporządzenia;

c) przyjęte normy zharmonizowane i wspólne specyfikacje opracowane w celu wsparcia niniejszego rozporządzenia;

d) liczbę przedsiębiorstw wchodzących na rynek po rozpoczęciu stosowania niniejszego rozporządzenia oraz jaką część z nich stanowią MŚP.

5. Do dnia ... [cztery lata od daty wejścia w życie niniejszego rozporządzenia] Komisja oceni funkcjonowanie Urzędu ds. AI, oceni, czy przyznano mu uprawnienia i kompetencje wystarczające do wykonywania jego zadań oraz czy dla właściwego wdrożenia i egzekwowania niniejszego rozporządzenia stosowne i potrzebne byłoby wzmocnienie Urzędu ds. AI i zwiększenie jego uprawnień w zakresie egzekwowania przepisów, a także zwiększenie jego zasobów. Komisja przedłoży sprawozdanie z oceny Parlamentowi Europejskiemu i Radzie.

6. Do dnia ... [cztery lata od daty wejścia w życie niniejszego rozporządzenia], a następnie co cztery lata, Komisja przedłoży sprawozdanie z przeglądu postępów w opracowywaniu dokumentów normalizacyjnych dotyczących wydajnego pod względem energii opracowywania modeli ogólnego przeznaczenia oraz oceni konieczność wprowadzenia dalszych środków lub działań, w tym wiążących środków lub działań. Sprawozdanie to jest przekazywane Parlamentowi Europejskiemu i Radzie i podawane do wiadomości publicznej.

7. Do dnia **...** [***cztery lata*** od daty wejścia w życie niniejszego rozporządzenia], a następnie co ***trzy*** lata Komisja oceni wpływ i skuteczność ***dobrowolnych*** kodeksów postępowania sprzyjających stosowaniu wymogów określonych w rozdziale II sekcja 2 ***w odniesieniu do systemów AI innych niż systemy AI wysokiego ryzyka*** oraz ewentualnie innych dodatkowych wymogów dotyczących systemów AI, w ***tym w zakresie zrównoważenia środowiskowego.***

8. Do celów ust. 1–7 Rada ds. AI, państwa członkowskie i właściwe organy krajowe przekazują Komisji informacje na jej wniosek ***i bez zbędnej zwłoki***.

9. Dokonując ocen i przeglądów, o których mowa w ust. 1–7, Komisja uwzględnia stanowiska i ustalenia Rady ds. AI, Parlamentu Europejskiego, Rady Unii Europejskiej oraz innych stosownych podmiotów lub źródeł.

10. W razie potrzeby Komisja przedkłada odpowiednie wnioski dotyczące zmiany niniejszego rozporządzenia, uwzględniając w szczególności rozwój technologii, ***wpływ systemów AI na zdrowie i bezpieczeństwo oraz na prawa podstawowe,*** oraz postępy dokonane w społeczeństwie informacyjnym.

11. W celu ukierunkowania ocen i przeglądów, o których mowa w ust. 1–7 niniejszego artykułu, Urząd ds. AI opracowuje obiektywną i partycypacyjną metodykę oceny poziomów ryzyka w oparciu o kryteria określone w odpowiednich artykułach i włączania nowych systemów do:

a) wykazu w załączniku III, łącznie z rozszerzeniem istniejących nagłówków dotyczących obszarów lub dodaniem nowych nagłówków dotyczących obszarów w tym załączniku;

b) zawartego w art. 5 wykazu zakazanych praktyk; oraz

c) wykazu systemów sztucznej inteligencji wymagających dodatkowych środków w zakresie przejrzystości zgodnie z art. 50.

12. Wszelkie zmiany w niniejszym rozporządzeniu zgodnie z ust. 10 lub odpowiednie akty delegowane i wykonawcze, które dotyczą unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja B, uwzględniają specyfikę regulacyjną każdego sektora oraz istniejące mechanizmy zarządzania, oceny zgodności i egzekwowania, jak również działalność organów ustanowionych dla danego sektora.

13. Do dnia ... [siedem lat od daty wejścia w życie niniejszego rozporządzenia] Komisja przeprowadzi ocenę wdrażania niniejszego rozporządzenia i przedłoży sprawozdanie z tej oceny Parlamentowi Europejskiemu, Radzie i Europejskiemu Komitetowi Ekonomiczno-Społecznemu, uwzględniając pierwsze lata stosowania niniejszego rozporządzenia. Na podstawie ustaleń do sprawozdania tego dołącza się, w stosownych przypadkach, wniosek dotyczący zmiany niniejszego rozporządzenia w odniesieniu do struktury egzekwowania przepisów i potrzeby usunięcia wszelkich stwierdzonych niedociągnięć przez agencję unijną.

Artykuł 113

Wejście w życie i rozpoczęcie stosowania

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia ... [24 miesiące od daty wejścia w życie niniejszego rozporządzenia] r.

Jednakże:

▌

a) rozdziały I i II stosuje się od dnia … [sześć miesięcy od daty wejścia w życie niniejszego rozporządzenia];

b) Rozdział III▌ sekcja 4, rozdział V, rozdział VII ***i rozdział XII*** stosuje się od dnia ... [***12*** miesięcy od daty wejścia w życie niniejszego rozporządzenia], ***z wyjątkiem art. 101***;

c) Art. ***6 ust. 1 i odpowiadające mu obowiązki ustanowione w niniejszym rozporządzeniu*** stosuje się od dnia … [***36*** miesięcy od daty wejścia w życie niniejszego rozporządzenia].

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w …

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący / Przewodnicząca*

ZAŁĄCZNIK I

Wykaz unijnego prawodawstwa harmonizacyjnego

Sekcja A. Wykaz unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych

1. dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE (Dz.U. L 157 z 9.6.2006, s. 24) [uchylona rozporządzeniem w sprawie maszyn];
2. dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz.U. L 170 z 30.6.2009, s. 1);
3. dyrektywa Parlamentu Europejskiego i Rady 2013/53/UE z dnia 20 listopada 2013 r. w sprawie rekreacyjnych jednostek pływających i skuterów wodnych i uchylająca dyrektywę 94/25/WE (Dz.U. L 354 z 28.12.2013, s. 90);
4. dyrektywa Parlamentu Europejskiego i Rady 2014/33/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących dźwigów i elementów bezpieczeństwa do dźwigów (Dz.U. L 96 z 29.3.2014, s. 251);
5. dyrektywa Parlamentu Europejskiego i Rady 2014/34/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do urządzeń i systemów ochronnych przeznaczonych do użytku w atmosferze potencjalnie wybuchowej (Dz.U. L 96 z 29.3.2014, s. 309);

6. dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62);

7. dyrektywa Parlamentu Europejskiego i Rady 2014/68/UE z dnia 15 maja 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku urządzeń ciśnieniowych (Dz.U. L 189 z 27.6.2014, s. 164);

8. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/424 z dnia 9 marca 2016 r. w sprawie urządzeń kolei linowych i uchylenia dyrektywy 2000/9/WE (Dz.U. L 81 z 31.3.2016, s. 1);

9. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/425 z dnia 9 marca 2016 r. w sprawie środków ochrony indywidualnej oraz uchylenia dyrektywy Rady 89/686/EWG (Dz.U. L 81 z 31.3.2016, s. 51);

10. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/426 z dnia 9 marca 2016 r. w sprawie urządzeń spalających paliwa gazowe oraz uchylenia dyrektywy 2009/142/WE (Dz.U. L 81 z 31.3.2016, s. 99);

11. 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);

12. 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).

Sekcja B. Wykaz innego unijnego prawodawstwa harmonizacyjnego

13. 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);

14. 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);

15. 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);

16. 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);

17. 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);

18. 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);

19. 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);

20. 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) w zakresie projektowania, produkcji i wprowadzania do obrotu statków powietrznych, o których mowa w art. 2 ust. 1 lit. a) i b), w odniesieniu do bezzałogowych statków powietrznych oraz ich silników, śmigieł, części i wyposażenia do zdalnego sterowania statkami powietrznymi.

ZAŁĄCZNIK II

Wykaz przestępstw, o których mowa w art. 5 ust. 1 lit. e) ppkt (iii)

Przestępstwa, o których mowa w art. 5 ust. 1 lit. e) ppkt (iii):

- ***terroryzm,***
- ***handel ludźmi,***
- ***wykorzystywanie seksualne dzieci i pornografia dziecięca,***
- ***nielegalny obrót środkami odurzającymi lub substancjami psychotropowymi,***
- ***nielegalny handel bronią, amunicją lub materiałami wybuchowymi,***
- ***zabójstwo, ciężkie uszkodzenie ciała,***
- ***nielegalny obrót organami lub tkankami ludzkimi,***
- ***nielegalny handel materiałami jądrowymi lub promieniotwórczymi,***
- ***uprowadzenie, bezprawne przetrzymywanie lub wzięcie zakładników,***

– *przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego,*

– *bezprawne zawładnięcie statkiem powietrznym lub statkiem,*

– *zgwałcenie,*

– *przestępstwo przeciw środowisku,*

– *rozbój w formie zorganizowanej lub rozbój przy użyciu broni,*

– *sabotaż,*

– *udział w organizacji przestępczej uczestniczącej w co najmniej jednym z wyżej wymienionych przestępstw.*

ZAŁĄCZNIK III

Systemy AI wysokiego ryzyka, o których mowa w art. 6 ust. 2

Systemy AI wysokiego ryzyka zgodnie z art. 6 ust. 2 to systemy AI wymienione w którymkolwiek z poniższych obszarów:

1. ***Biometria, w zakresie, w jakim jej stosowanie jest dozwolone na podstawie odpowiednich przepisów unijnych lub krajowych:***

   a) ***systemy zdalnej identyfikacji biometrycznej.***

   Nie obejmuje to systemów AI przeznaczonych do stosowania przy ***weryfikacji biometrycznej, której jedynym celem jest potwierdzenie, że określona osoba*** fizyczna ***jest osobą, za którą się podaje;***

   b) systemy AI przeznaczone do stosowania przy kategoryzacji biometrycznej, według wrażliwych lub chronionych atrybutów lub cech lub na podstawie wywnioskowania tych atrybutów lub cech;

   c) systemy AI przeznaczone do stosowania przy rozpoznawaniu emocji.

2. ▌Infrastruktura krytyczna:

   a) systemy AI przeznaczone do stosowania jako związane z bezpieczeństwem elementy procesów zarządzania ***krytyczną infrastrukturą cyfrową***, ruchem drogowym i procesów ich obsługi lub zaopatrzenia w wodę, gaz, ciepło lub energię elektryczną.

3. Kształcenie i szkolenie zawodowe:

   a) systemy AI przeznaczone do stosowania ***do celów podejmowania decyzji o dostępie lub przyjęciu*** do instytucji edukacyjnych i instytucji szkolenia zawodowego ***lub*** nadawania osobom ***przydziału*** do tych instytucji ***na wszystkich poziomach***;

   b) systemy AI przeznaczone do stosowania ***do celów oceny efektów uczenia się, także w przypadku gdy efekty te są wykorzystywane do kierowania procesem uczenia się osób fizycznych w instytucjach edukacyjnych i instytucjach szkolenia zawodowego na wszystkich poziomach;***

   c) systemy AI przeznaczone do stosowania do celów oceny odpowiedniego poziomu wykształcenia, jaki dana osoba otrzyma lub do jakiego będzie mogła mieć dostęp w kontekście lub w ramach instytucji edukacyjnych i instytucji szkolenia zawodowego;

   d) systemy AI przeznaczone do stosowania do celów monitorowania i wykrywania niedozwolonego zachowania uczniów podczas testów w kontekście lub w ramach instytucji edukacyjnych i instytucji szkolenia zawodowego.

4. Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia:

   a) systemy AI przeznaczone do stosowania do celów rekrutacji lub wyboru osób fizycznych, w szczególności ***do celów umieszczania ukierunkowanych ogłoszeń o pracę, analizowania i filtrowania podań o pracę oraz do oceny kandydatów;***

   b) systemy AI przeznaczone do stosowania do celów ***podejmowania*** decyzji ***wpływających na warunki stosunków pracy***, decyzji o awansie i rozwiązaniu stosunku pracy, ***przydzielania zadań w oparciu o indywidualne zachowanie lub cechy osobowości lub charakter oraz do monitorowania lub*** oceny wydajności i zachowania osób pozostających w takich stosunkach.

5. Dostęp do podstawowych usług prywatnych oraz ***podstawowych*** usług i świadczeń publicznych, a także korzystanie z nich:

   a) systemy AI przeznaczone do wykorzystywania przez organy publiczne lub w imieniu organów publicznych w celu oceny kwalifikowalności osób fizycznych do ***podstawowych*** świadczeń i usług publicznych, w ***tym opieki zdrowotnej***, jak również w celu przyznawania, ograniczania, unieważniania lub żądania zwrotu takich świadczeń i usług;

   b) systemy AI przeznaczone do stosowania do celów oceny zdolności kredytowej osób fizycznych lub ustalenia ich punktowej oceny kredytowej, z wyjątkiem systemów AI ***wykorzystywanych w celu wykrywania oszustw finansowych;***

c) ***systemy AI przeznaczone do stosowania przy ocenie ryzyka i ustalaniu cen w odniesieniu do osób fizycznych w przypadku ubezpieczenia na życie i ubezpieczenia zdrowotnego;***

d) systemy AI przeznaczone do ***oceny i klasyfikacji zgłoszeń alarmowych dokonywanych przez osoby fizyczne lub do*** wykorzystywania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb pierwszej pomocy , w tym ***policji***, straży pożarnej i pomocy medycznej, a ***także w ramach systemów oceny stanu zdrowia pacjentów w nagłych wypadkach***;

6. Ściganie przestępstw***, w zakresie, w jakim stosowanie przedmiotowych systemów jest dozwolone na podstawie odpowiednich przepisów unijnych lub krajowych:***

a) systemy AI przeznaczone do wykorzystywania przez organy ścigania ***lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii wspierające organy ścigania lub w ich imieniu*** do oceny ryzyka, że osoba fizyczna ***stanie się ofiarą*** przestępstwa;

b) systemy AI przeznaczone do wykorzystywania ***jako wariografy lub podobne narzędzia*** przez organy ścigania ***lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii wspierające organy ścigania;***

c) systemy AI przeznaczone do wykorzystywania przez organy ścigania ***lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii wspierające organy ścigania do oceny*** wiarygodności dowodów w toku ścigania przestępstw lub prowadzenia postępowań przygotowawczych w ich sprawie;

d) systemy AI przeznaczone do wykorzystywania przez organy ścigania ***lub w ich imieniu lub przez instytucje, organy i jednostki organizacyjne Unii wspierające organy ścigania do oceny prawdopodobieństwa, że osoba fizyczna popełni lub ponownie popełni przestępstwo, niewyłącznie*** na podstawie profilowania osób fizycznych, o którym mowa w art. 3 pkt 4 dyrektywy (UE) 2016/680, lub do ***oceny*** cech osobowości i charakteru lub uprzedniego zachowania przestępczego osób fizycznych lub grup;

e) systemy AI przeznaczone do wykorzystywania ***przez organy ścigania lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii wspierające organy ścigania*** do profilowania osób fizycznych, o którym mowa w art. 3 pkt 4 dyrektywy (UE) 2016/680, w toku wykrywania i ścigania przestępstw lub prowadzenia postępowań przygotowawczych w ich sprawie.

7. Zarządzanie migracją, azylem i kontrolą graniczną***, w zakresie, w jakim stosowanie przedmiotowych systemów jest dozwolone na podstawie odpowiednich przepisów unijnych lub krajowych:***

a) systemy AI przeznaczone do wykorzystywania przez właściwe organy publiczne jako wariografy i podobne narzędzia;

b) systemy AI przeznaczone do wykorzystywania przez właściwe organy publiczne ***lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii*** do celów oceny ryzyka, w tym ryzyka dla bezpieczeństwa, ryzyka ***migracji*** nieuregulowanej lub ryzyka dla zdrowia, stwarzanych przez osobę fizyczną, która zamierza wjechać lub wjechała na terytorium państwa członkowskiego;

c) systemy AI przeznaczone do ***wykorzystywania przez właściwe organy publiczne lub w ich imieniu, lub przez instytucje, organy i jednostki organizacyjne Unii do celów*** wspierania właściwych organów publicznych przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu, ***w tym przy powiązanej ocenie wiarygodności dowodów;***

d) systemy AI przeznaczone do stosowania przez właściwe organy publiczne lub w ich imieniu, w tym instytucje, organy i jednostki organizacyjne Unii w kontekście zarządzania migracją, azylem i kontrolą graniczną, do celów wykrywania, rozpoznawania lub identyfikacji osób fizycznych, z wyjątkiem weryfikacji dokumentów podróży.

8. Sprawowanie wymiaru sprawiedliwości i procesy demokratyczne:

a) systemy AI przeznaczone do ***wykorzystywania przez organ sądowy lub w jego imieniu*** w celu wspomagania organu sądowego w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego ***lub do wykorzystywania w podobny sposób w alternatywnych metodach rozwiązywania sporów;***

b) ***Systemy AI przeznaczone do stosowania w celu wywierania wpływu na wynik wyborów lub referendum lub na zachowanie osób fizycznych podczas głosowania w wyborach lub referendach. Nie obejmuje to systemów AI, na których wyniki osoby fizyczne nie są bezpośrednio narażone, takich jak narzędzia wykorzystywane do organizowania, optymalizacji lub strukturyzowania kampanii politycznych z administracyjnego lub logistycznego punktu widzenia.***

ZAŁĄCZNIK IV

Dokumentacja techniczna, o której mowa w art. 11 ust. 1

Dokumentacja techniczna, o której mowa w art. 11 ust. 1, zawiera, stosownie do przypadku, co najmniej następujące informacje właściwe dla danego systemu AI:

1. Ogólny opis systemu AI, w tym:

   a) jego przeznaczenie, ***nazwę dostawcy*** i wersję systemu, ***odzwierciedlające jego związek z poprzednimi wersjami;***

   b) sposób, w jaki system AI, w stosownych przypadkach, współdziała lub może być wykorzystany do współdziałania ze sprzętem lub oprogramowaniem, ***w tym z innymi systemami AI, które*** nie są częścią samego systemu AI;

   c) wersje odpowiedniego oprogramowania lub oprogramowania układowego oraz wszelkie wymogi związane z aktualizacjami wersji;

   d) opis wszystkich form, w jakich system AI wprowadza się do obrotu lub oddaje do użytku, ***takie jak pakiety oprogramowania wbudowane w urządzenie, oprogramowanie do pobrania lub API***;

e) opis sprzętu, na którym system AI ma być eksploatowany;

f) w przypadku gdy system AI jest elementem produktów – zdjęcia lub ilustracje przedstawiające cechy zewnętrzne, oznakowanie i układ wewnętrzny tych produktów;

g) podstawowy opis interfejsu użytkownika, który dostarczono podmiotowi stosującemu AI;

h) instrukcja obsługi dla ***podmiotu stosującego AI oraz, w*** stosownych przypadkach***, podstawowy opis interfejsu użytkownika, który dostarczono podmiotowi stosującemu AI*** ▌;

2. Szczegółowy opis elementów systemu AI oraz procesu jego opracowywania, w tym:

a) metody i działania zastosowane w celu opracowania systemu AI, w tym, w stosownych przypadkach, skorzystanie z już wytrenowanych systemów lub narzędzi dostarczonych przez osoby trzecie oraz wskazanie, w jaki sposób dostawca wykorzystał, zintegrował lub zmodyfikował te systemy lub narzędzia;

b) specyfikacje projektowe systemu, a mianowicie ogólna logika systemu AI i algorytmów; kluczowe decyzje projektowe wraz z uzasadnieniem i przyjętymi założeniami, w tym w odniesieniu do osób lub grup osób, wobec których system ma być wykorzystywany; główne wybory klasyfikacyjne; wskazanie, pod kątem czego system ma być optymalizowany, i znaczenie poszczególnych parametrów; ***opis oczekiwanego wyniku działania systemu oraz jakości tego wyniku***; decyzje dotyczące wszelkich możliwych kompromisów w zakresie rozwiązań technicznych przyjętych w celu spełnienia wymogów określonych w rozdziale III sekcja 2;

c) opis architektury systemu wyjaśniający, w jaki sposób elementy oprogramowania współgrają ze sobą lub wzajemnie się uzupełniają oraz włączają się w ogólne przetwarzanie; zasoby obliczeniowe wykorzystywane do opracowania, trenowania, testowania i walidacji systemu AI;

d) w stosownych przypadkach wymogi dotyczące danych w zakresie arkuszy danych opisujących metodyki i techniki trenowania systemu oraz wykorzystywane zbiory danych treningowych, w tym ***ogólny opis tych*** zbiorów danych, ***informacje o ich pochodzeniu***, ich zakresie i głównych cechach; sposób uzyskania i wyboru danych; procedury etykietowania (np. w przypadku uczenia nadzorowanego), metody oczyszczania danych (np. wykrywanie wartości oddalonych);

e) ocenę środków nadzoru ze strony człowieka wymaganych na podstawie art. 14, w tym ocenę środków technicznych potrzebnych do ułatwienia ***podmiotom stosującym AI*** interpretacji wyników działania systemów AI, zgodnie z art. 13 ust. 3 lit. d);

f) w stosownych przypadkach szczegółowy opis z góry zaplanowanych zmian w systemie AI i jego skuteczności działania wraz ze wszystkimi istotnymi informacjami dotyczącymi rozwiązań technicznych przyjętych w celu zapewnienia ciągłej zgodności systemu AI z odpowiednimi wymogami określonymi w rozdziale III sekcja 2;

g) zastosowane procedury walidacji i testowania, w tym informacje o wykorzystywanych danych walidacyjnych i danych testowych oraz ich głównych cechach; wskaźniki stosowane do pomiaru dokładności, solidności ▌ i zgodności z innymi stosownymi wymogami określonymi w rozdziale III sekcja 2, jak również skutków potencjalnie dyskryminujących; rejestry zdarzeń generowane podczas testów i wszystkie sprawozdania z testów opatrzone datą i podpisane przez osoby odpowiedzialne, w tym w odniesieniu do z góry zaplanowanych zmian, o których mowa w lit. f);

h) wdrożone środki w zakresie cyberbezpieczeństwa;

3. Szczegółowe informacje dotyczące monitorowania, funkcjonowania i kontroli systemu AI, w szczególności w odniesieniu do: jego możliwości i ograniczeń w zakresie skuteczności działania, w tym stopnie dokładności w przypadku określonych osób lub grup osób, wobec których system ma być wykorzystywany, oraz ogólny spodziewany poziom dokładności w stosunku do jego przeznaczenia; możliwych do przewidzenia niezamierzonych wyników działania i źródeł zagrożeń zdrowia i bezpieczeństwa, praw podstawowych i zagrożeń powodujących dyskryminację w świetle przeznaczenia systemu AI; środków nadzoru ze strony człowieka wymaganych na podstawie art. 14, w tym środków technicznych wprowadzonych w celu ułatwienia ***podmiotom stosującym AI*** interpretacji wyników działania systemów AI; w stosownych przypadkach specyfikacji dotyczących danych wejściowych;

4. opis adekwatności wskaźników wydajności w odniesieniu do konkretnego systemu AI;

5. Szczegółowy opis systemu zarządzania ryzykiem zgodnie z art. 9;

6. Opis ***odpowiednich zmian dokonanych przez dostawcę*** w systemie w czasie trwania cyklu życia tego systemu;

7. Wykaz norm zharmonizowanych stosowanych w całości lub w części, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*; w przypadku gdy nie zastosowano takich norm zharmonizowanych, szczegółowy opis rozwiązań przyjętych w celu spełnienia wymogów określonych w rozdziale III sekcja 2, w tym wykaz innych odpowiednich zastosowanych norm i specyfikacji technicznych;

8. Kopię deklaracji zgodności UE;

9. Szczegółowy opis systemu stosowanego do oceny skuteczności działania systemu AI po wprowadzeniu do obrotu zgodnie z art. 72, w tym plan monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 72 ust. 3.

ZAŁĄCZNIK V

Deklaracja zgodności UE

Deklaracja zgodności UE, o której mowa w art. 47, zawiera wszystkie następujące informacje:

1. nazwę i rodzaj systemu AI oraz wszelkie dodatkowe jednoznaczne odniesienia umożliwiające identyfikację i identyfikowalność systemu AI;
2. nazwę/imię i nazwisko i adres dostawcy lub, w stosownych przypadkach, jego upoważnionego przedstawiciela;
3. oświadczenie, że deklarację zgodności UE wydano na wyłączną odpowiedzialność dostawcy;
4. oświadczenie, że system AI jest zgodny z niniejszym rozporządzeniem oraz, w stosownych przypadkach, z wszelkimi innymi odpowiednimi przepisami Unii, w których przewidziano wydanie deklaracji zgodności UE;
5. ***W przypadku gdy system AI wiąże się z przetwarzaniem danych osobowych, oświadczenie, że system AI jest zgodny z rozporządzeniami (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywą (UE) 2016/680;***
6. odniesienia do wszelkich zastosowanych odpowiednich norm zharmonizowanych lub wszelkich innych wspólnych specyfikacji, z którymi deklaruje się zgodność;
7. w stosownych przypadkach nazwę i numer identyfikacyjny jednostki notyfikowanej, opis przeprowadzonej procedury oceny zgodności oraz dane identyfikacyjne wydanego certyfikatu;
8. miejsce i datę wystawienia deklaracji, imię i nazwisko oraz stanowisko osoby, która złożyła podpis pod dokumentem, oraz wskazanie, z czyjego upoważnienia lub w czyim imieniu ta osoba podpisała dokument, oraz podpis.

ZAŁĄCZNIK VI

Procedura oceny zgodności opierająca się na kontroli wewnętrznej

1. Procedura oceny zgodności opierająca się na kontroli wewnętrznej jest procedurą oceny zgodności przeprowadzaną na podstawie pkt 2–4.

2. Dostawca sprawdza, czy ustanowiony system zarządzania jakością spełnia wymogi art. 17.

3. Dostawca analizuje informacje zawarte w dokumentacji technicznej, aby ocenić zgodność systemu AI z odpowiednimi zasadniczymi wymogami określonymi w rozdziale III sekcja 2.

4. Dostawca sprawdza również, czy proces projektowania i opracowywania systemu AI oraz proces jego monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 72, są zgodne z dokumentacją techniczną.

ZAŁĄCZNIK VII

Zgodność opierająca się na ocenie systemu zarządzania jakością i ocenie dokumentacji technicznej

1. Wprowadzenie

Zgodność opierająca się na ocenie systemu zarządzania jakością i ocenie dokumentacji technicznej jest procedurą oceny zgodności przeprowadzaną na podstawie pkt 2–5.

2. Informacje ogólne

Zatwierdzony system zarządzania jakością w zakresie projektowania, opracowywania i testowania systemów AI zgodnie z art. 17 ocenia się zgodnie z pkt 3 i poddaje nadzorowi zgodnie z pkt 5. Dokumentację techniczną systemu AI ocenia się zgodnie z pkt 4.

3. System zarządzania jakością

3.1. Wniosek dostawcy zawiera:

a) nazwę/imię i nazwisko i adres dostawcy oraz, jeśli wniosek jest składany przez upoważnionego przedstawiciela, również jego nazwę/imię i nazwisko i adres;

b) wykaz systemów AI objętych tym samym systemem zarządzania jakością;

c) dokumentację techniczną każdego systemu AI objętego tym samym systemem zarządzania jakością;

d) dokumentację dotyczącą systemu zarządzania jakością, która obejmuje wszystkie aspekty wymienione w art. 17;

e) opis procedur zapewniających stałą adekwatność i skuteczność systemu zarządzania jakością;

f) pisemne oświadczenie, że tego samego wniosku nie złożono w innej jednostce notyfikowanej.

3.2. System zarządzania jakością jest oceniany przez jednostkę notyfikowaną, która ustala, czy spełnia on wymogi, o których mowa w art. 17.

O decyzji powiadamia się dostawcę lub jego upoważnionego przedstawiciela.

Powiadomienie to zawiera wnioski z oceny systemu zarządzania jakością oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

3.3. System zarządzania jakością w jego zatwierdzonej formie jest dalej wdrażany i utrzymywany przez dostawcę, tak aby mógł zachować adekwatność i skuteczność.

3.4. Dostawca powiadamia jednostkę notyfikowaną o wszelkich zamierzonych zmianach w zatwierdzonym systemie zarządzania jakością lub w wykazie systemów AI objętych tym systemem.

Proponowane zmiany podlegają weryfikacji przeprowadzanej przez jednostkę notyfikowaną, która stwierdza, czy zmieniony system zarządzania jakością nadal spełnia wymogi, o których mowa w pkt 3.2, czy też konieczna jest jego ponowna ocena.

Jednostka notyfikowana powiadamia dostawcę o swojej decyzji. Takie powiadomienie zawiera wnioski z weryfikacji zmian oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

4. Kontrola dokumentacji technicznej

4.1. Oprócz wniosku, o którym mowa w pkt 3, dostawca składa wniosek do wybranej przez siebie jednostki notyfikowanej o ocenę dokumentacji technicznej dotyczącej systemu AI, który dostawca zamierza wprowadzić do obrotu lub oddać do użytku i który jest objęty systemem zarządzania jakością, o którym mowa w pkt 3.

4.2. Wniosek zawiera:

a) nazwę/imię i nazwisko i adres dostawcy;

b) pisemne oświadczenie, że tego samego wniosku nie złożono w innej jednostce notyfikowanej;

c) dokumentację techniczną, o której mowa w załączniku IV.

4.3. Ocenę dokumentacji technicznej przeprowadza jednostka notyfikowana. ***W stosownych przypadkach i w zakresie ograniczonym do tego, co jest niezbędne do wykonywania jej zadań***, jednostka notyfikowana otrzymuje pełny dostęp do wykorzystywanych zbiorów danych treningowych, ***walidacyjnych*** i testowych, ***w tym, w stosownych przypadkach i z zastrzeżeniem gwarancji bezpieczeństwa,*** za pośrednictwem API lub innych ***odpowiednich*** środków i narzędzi ***technicznych*** umożliwiających zdalny dostęp.

4.4. Analizując dokumentację techniczną, jednostka notyfikowana może zażądać od dostawcy przedstawienia dalszych dowodów lub przeprowadzenia dalszych testów w celu umożliwienia właściwej oceny zgodności systemu AI z wymogami określonymi w rozdziale III sekcja 2. W przypadku gdy jednostka notyfikowana nie jest usatysfakcjonowana testami przeprowadzonymi przez dostawcę, jednostka notyfikowana sama przeprowadza bezpośrednio, stosownie do okoliczności, odpowiednie testy.

4.5. W przypadku gdy jest to konieczne do oceny zgodności systemu AI wysokiego ryzyka z wymogami określonymi w rozdziale III sekcja 2, ***po wyczerpaniu wszystkich innych racjonalnych sposobów weryfikacji zgodności, które okazały się niewystarczające***, jednostka notyfikowana uzyskuje – na uzasadniony wniosek – również dostęp do ***modeli treningowych i trenowanych*** systemu AI, ***w tym do odpowiednich jego parametrów***. ***Taki dostęp podlega obowiązującym przepisom unijnym dotyczącym własności intelektualnej i tajemnic przedsiębiorstwa.***

4.6. O decyzji jednostki notyfikowanej powiadamia się dostawcę lub jego upoważnionego przedstawiciela. Powiadomienie to zawiera wnioski z oceny dokumentacji produktu oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

W przypadku gdy system AI spełnia wymogi określone w rozdziale III sekcja 2, jednostka notyfikowana wydaje unijny certyfikat oceny dokumentacji technicznej. Certyfikat zawiera nazwę/imię i nazwisko oraz adres dostawcy, wnioski z oceny, ewentualne warunki jego ważności oraz dane niezbędne do identyfikacji systemu AI.

Certyfikat wraz z załącznikami musi zawierać wszystkie istotne informacje umożliwiające ocenę zgodności systemu AI oraz, w stosownych przypadkach, kontrolę systemu AI podczas jego użytkowania.

W przypadku gdy system AI nie spełnia wymogów określonych w rozdziale III sekcja 2, jednostka notyfikowana odmawia wydania unijnego certyfikatu oceny dokumentacji technicznej i informuje o tym wnioskodawcę, podając szczegółowe uzasadnienie odmowy.

W przypadku gdy system AI nie spełnia wymogu dotyczącego danych wykorzystywanych do jego trenowania, przed złożeniem wniosku o nową ocenę zgodności system AI należy poddać ponownemu treningowi. W takim przypadku uzasadniona decyzja jednostki notyfikowanej o odmowie wydania unijnego certyfikatu oceny dokumentacji technicznej zawiera szczegółowe uwagi na temat jakości danych wykorzystanych do treningu systemu AI, w szczególności na temat przyczyn niezgodności.

4.7. Wszelkie zmiany w systemie AI, które mogłyby wpłynąć na zgodność systemu AI z wymogami lub jego przeznaczeniem, podlegają ocenie przez jednostkę notyfikowaną, która wydała unijny certyfikat oceny dokumentacji technicznej. Dostawca informuje taką jednostkę notyfikowaną, jeżeli zamierza wprowadzić wyżej wymienione zmiany lub jeżeli w inny sposób dowiedział się o ich zaistnieniu. Zamierzone zmiany ocenia jednostka notyfikowana, która decyduje, czy zmiany te wymagają przeprowadzenia nowej oceny zgodności zgodnie z art. 43 ust. 4, czy też można je uwzględnić w formie suplementu do unijnego certyfikatu oceny dokumentacji technicznej. W tym ostatnim przypadku jednostka notyfikowana ocenia zmiany, powiadamia dostawcę o swojej decyzji i, w przypadku zatwierdzenia zmian, wydaje dostawcy suplement do unijnego certyfikatu oceny dokumentacji technicznej.

5. Nadzór nad zatwierdzonym systemem zarządzania jakością

5.1. Celem nadzoru sprawowanego przez jednostkę notyfikowaną, o której mowa w pkt 3, jest zapewnienie, aby dostawca należycie wywiązywał się z warunków, jakimi obwarowano zatwierdzony system zarządzania jakością.

5.2. Do celów oceny dostawca umożliwia jednostce notyfikowanej dostęp do pomieszczeń, w których odbywa się projektowanie, opracowywanie i testowanie systemów AI. Dostawca udostępnia ponadto jednostce notyfikowanej wszystkie niezbędne informacje.

5.3. Jednostka notyfikowana przeprowadza okresowe audyty, aby upewnić się, że dostawca utrzymuje i stosuje system zarządzania jakością, oraz przedstawia dostawcy sprawozdanie z audytu. W ramach tych audytów jednostka notyfikowana może przeprowadzać dodatkowe testy systemów AI, w odniesieniu do których wydano unijny certyfikat oceny dokumentacji technicznej.

ZAŁĄCZNIK VIII

Informacje, które należy przedłożyć przy rejestracji systemów AI wysokiego ryzyka zgodnie z art. 49

Sekcja A – Informacje przekazywane przez dostawców systemów AI wysokiego ryzyka zgodnie z art. 49 ust. 1

W odniesieniu do systemów AI wysokiego ryzyka, które podlegają rejestracji zgodnie z art. 49 ***ust. 1***, przekazuje się, a następnie aktualizuje następujące informacje:

1. nazwa/imię i nazwisko, adres i dane kontaktowe dostawcy;
2. w przypadku gdy w imieniu dostawcy informacje przekazuje inna osoba, nazwa/imię i nazwisko, adres i dane kontaktowe tej osoby;
3. w stosownych przypadkach nazwa/imię i nazwisko, adres i dane kontaktowe upoważnionego przedstawiciela;
4. nazwa handlowa systemu AI oraz wszelkie dodatkowe jednoznaczne odniesienia umożliwiające identyfikację i identyfikowalność systemu AI;
5. opis przeznaczenia systemu AI ***oraz elementów i funkcji wspieranych przez ten system AI;***
6. ***podstawowy i zwięzły opis informacji wykorzystywanych przez ten system (dane, dane wejściowe) oraz logika jego działania;***

7. status systemu AI (dostępny na rynku lub użytkowany; niedostępny już na rynku / już nieużytkowany, wycofany od użytkowników);

8. rodzaj, numer i datę ważności certyfikatu wydanego przez jednostkę notyfikowaną oraz w stosownych przypadkach nazwę lub numer identyfikacyjny tej jednostki notyfikowanej;

9. w stosownych przypadkach skan certyfikatu, o którym mowa w pkt 8;

10. wszystkie państwa członkowskie, w których system AI był dostępny na rynku, został oddany do użytku lub był udostępniany w Unii;

11. kopia deklaracji zgodności UE, o której mowa w art. 47;

12. elektroniczna instrukcja obsługi; informacji tych nie podaje się w przypadku systemów AI wysokiego ryzyka w obszarach ścigania przestępstw oraz zarządzania migracją, azylem lub kontrolą graniczną, o których mowa w załączniku III pkt 1, 6 i 7;

13. adres URL odsyłający do dodatkowych informacji (opcjonalnie).

Sekcja B – Informacje przekazywane przez dostawców systemów AI wysokiego ryzyka zgodnie z art. 49 ust. 2

W odniesieniu do systemów AI, które podlegają rejestracji zgodnie z art. 49 ust. 2, przekazuje się, a następnie aktualizuje następujące informacje:

1. ***nazwa/imię i nazwisko, adres i dane kontaktowe dostawcy;***
2. ***w przypadku gdy w imieniu dostawcy informacje przekazuje inna osoba, nazwa/imię i nazwisko, adres i dane kontaktowe tej osoby;***
3. ***w stosownych przypadkach nazwa/imię i nazwisko, adres i dane kontaktowe upoważnionego przedstawiciela;***
4. ***nazwa handlowa systemu AI oraz wszelkie dodatkowe jednoznaczne odniesienia umożliwiające identyfikację i identyfikowalność systemu AI;***
5. ***opis przeznaczenia systemu AI;***
6. ***warunek lub warunki określone w art. 6 ust. 3, na podstawie których system AI jest uznawany za niebędący systemem wysokiego ryzyka;***
7. ***krótkie streszczenie uzasadnienia, dlaczego system AI jest uznawany za niebędący systemem wysokiego ryzyka w wyniku zastosowania procedury na podstawie art. 6 ust. 3;***
8. ***status systemu AI (dostępny na rynku lub użytkowany; niedostępny już na rynku / już nieużytkowany, wycofany od użytkowników);***
9. ***wszystkie państwa członkowskie, w których system AI wprowadzono do obrotu, oddano do użytku lub udostępniono w Unii.***

Sekcja C – Informacje przekazywane zgodnie z art. 49 ust. 3 przez podmioty stosujące systemy AI wysokiego ryzyka

W odniesieniu do systemów AI wysokiego ryzyka, które podlegają rejestracji zgodnie z art. 49, przekazuje się, a następnie aktualizuje następujące informacje:

1. ***nazwa/imię i nazwisko, adres i dane kontaktowe podmiotu stosującego AI;***
2. ***imię i nazwisko, adres i dane kontaktowe osoby przesyłającej informacje w imieniu podmiotu stosującego AI;***
3. ***streszczenie ustaleń oceny skutków w zakresie praw podstawowych przeprowadzonej zgodnie z art. 27;***
4. ***adres URL wpisu systemu AI do unijnej bazy danych dokonanego przez jego dostawcę;***
5. ***w stosownych przypadkach streszczenie oceny skutków dla ochrony danych przeprowadzonej zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680, jak określono w*** art. 26 ust. 8 ***niniejszego rozporządzenia.***

ZAŁĄCZNIK IX

Informacje, które należy przedłożyć przy rejestracji systemów AI wysokiego ryzyka wymienionych w załączniku III w odniesieniu do testów w warunkach rzeczywistych zgodnie z art. 60

W odniesieniu do testów w warunkach rzeczywistych, które podlegają rejestracji zgodnie z art. 60, przekazuje się, a następnie aktualizuje następujące informacje:

1. ***ogólnounijny niepowtarzalny numer identyfikacyjny testów w warunkach rzeczywistych;***
2. ***nazwę/imię i nazwisko oraz dane kontaktowe dostawcy lub potencjalnego dostawcy i podmiotów stosujących AI uczestniczących w testach w warunkach rzeczywistych;***
3. ***krótki opis systemu AI, jego przeznaczenie oraz inne informacje niezbędne do identyfikacji systemu;***
4. ***streszczenie głównych założeń planu testów w warunkach rzeczywistych;***
5. ***informacje o zawieszeniu lub zakończeniu testów w warunkach rzeczywistych.***

ZAŁĄCZNIK X

Unijne akty prawne dotyczące wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości

1. System Informacyjny Schengen:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz.U. L 312 z 7.12.2018, s. 1);

   b) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006 (Dz.U. L 312 z 7.12.2018, s. 14);

   c) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz.U. L 312 z 7.12.2018, s. 56).

2. Wizowy system informacyjny:

a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1133 z dnia 7 lipca 2021 r. w sprawie zmiany rozporządzeń (UE) nr 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 i (UE) 2019/818 w odniesieniu do ustanowienia warunków dostępu do innych systemów informacyjnych UE do celów Wizowego Systemu Informacyjnego (Dz.U. L 248 z 13.7.2021, s. 1).

b) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1134 z dnia 7 lipca 2021 r. w sprawie zmiany rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 767/2008, (WE) nr 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 i (UE) 2019/1896 oraz uchylenia decyzji Rady 2004/512/WE i (WE) nr 2008/633/WSiSW w celu zreformowania Wizowego Systemu Informacyjnego (Dz.U. L 248 z 13.7.2021, s. 11).

3. Eurodac:

a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/… w sprawie ustanowienia systemu Eurodac do porównywania danych biometrycznych w celu skutecznego stosowania rozporządzenia (UE) .../... [rozporządzenie w sprawie zarządzania azylem i migracją] i rozporządzenia (UE) .../... [rozporządzenie w sprawie przesiedleń] oraz dyrektywy 2001/55/WE [dyrektywa w sprawie tymczasowej ochrony] na potrzeby identyfikowania nielegalnie przebywających obywateli państw trzecich lub bezpaństwowców oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego oraz zmieniającego rozporządzenia (UE) 2018/1240 i (UE) 2019/818[+].

[+] Dz.U.: proszę wstawić w tekście numer rozporządzenia zawartego w dokumencie PE-CONS 15/24 (2016/0132(COD)) oraz, w przypisie, numer, datę, tytuł i odniesienie do publikacji tego rozporządzenia w Dz.U.

4. System wjazdu/wyjazdu:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz.U. L 327 z 9.12.2017, s. 20).

5. Europejski system informacji o podróży oraz zezwoleń na podróż:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz.U. L 236 z 19.9.2018, s. 1);

   b) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1241 z dnia 12 września 2018 r. zmieniające rozporządzenie (UE) 2016/794 w celu ustanowienia europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) (Dz.U. L 236 z 19.9.2018, s. 72).

6. Europejski system przekazywania informacji z rejestrów karnych dotyczących obywateli państw trzecich i bezpaństwowców:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.U. L 135 z 22.5.2019, s. 1).

7. Interoperacyjność:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze granic i polityki wizowej (Dz.U. L 135 z 22.5.2019, s. 27);

   b) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/818 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze współpracy policyjnej i sądowej, azylu i migracji (Dz.U. L 135 z 22.5.2019, s. 85).

ZAŁĄCZNIK XI

Dokumentacja techniczna, o której mowa w art. 53 ust. 1 lit. a) **– *dokumentacja techniczna dla dostawców modeli AI ogólnego przeznaczenia***

Sekcja 1

Informacje przekazywane przez wszystkich dostawców modeli AI ogólnego przeznaczenia

Dokumentacja techniczna, o której mowa w art. 53 ust. 1 lit. a), ***zawiera co najmniej następujące informacje stosownie do rozmiaru danego systemu AI oraz jego profilu ryzyka:***

1. ***Ogólny opis modelu AI ogólnego przeznaczenia, w tym:***

   a) ***zadania, który dany model ma wykonywać, oraz rodzaj i charakter systemów AI, z którymi może zostać zintegrowany;***

   b) ***mające zastosowanie dopuszczalne zasady wykorzystania;***

   c) ***data wydania i metody dystrybucji;***

   d) ***architektura i liczba parametrów;***

   e) ***forma (np. tekst, obraz) oraz format danych wejściowych i wyjściowych;***

   f) ***licencja.***

2. ***Szczegółowy opis elementów modelu, o których mowa w pkt 1, oraz stosowne informacje na temat procesu opracowywania, z uwzględnieniem następujących elementów:***

   a) ***środki techniczne (np. instrukcja obsługi, infrastruktura, narzędzia) wymagane do integracji danego modelu AI ogólnego przeznaczenia z systemami AI;***

   b) ***specyfikacje projektu danego modelu i proces szkolenia, w tym metody i techniki treningowe, kluczowe wybory projektowe wraz z uzasadnieniem i przyjętymi założeniami; wskazanie, pod kątem czego model ma być optymalizowany, i znaczenie poszczególnych parametrów, w stosownych przypadkach;***

   c) ***informacje na temat danych wykorzystywanych do trenowania, testowania i walidacji, w stosownych przypadkach, w tym rodzaju i pochodzenia danych oraz metody porządkowania (np. czyszczenie, filtrowanie, itp.), liczby punktów danych, ich zakresu i głównych właściwości; w jaki sposób dane zostały uzyskane i wyselekcjonowane, a także wszystkie inne środki służące wykryciu nieodpowiednich źródeł danych i metod wykrywania możliwej do zidentyfikowania stronniczości, w stosownych przypadkach;***

d) zasoby obliczeniowe wykorzystywane do trenowania danego modelu (np. liczba operacji zmiennoprzecinkowych – FLOP), czas trenowania oraz inne istotne informacje dotyczące trenowania;

e) znane lub szacowane zużycie energii dla danego modelu.

W odniesieniu do lit. e), w przypadku gdy nie jest znane zużycie energii dla danego modelu, zużycie energii może opierać się na informacjach dotyczących wykorzystanych zasobów obliczeniowych.

Sekcja 2

Dodatkowe informacje przekazywane przez dostawców modeli AI ogólnego przeznaczenia z ryzykiem systemowym

1. Szczegółowy opis strategii ewaluacji, w tym jej wyników, na podstawie dostępnych publicznych protokołów i narzędzi ewaluacji lub na podstawie innych metod oceny. Strategie ewaluacji obejmują kryteria, wskaźniki i metodykę identyfikacji ograniczeń.

2. W stosownych przypadkach szczegółowy opis środków wprowadzonych w celu przeprowadzenia wewnętrznych lub zewnętrznych testów kontradyktoryjnych (np. red teaming), dostosowań modelu, w tym dopasowania i dostrojenia.

3. W stosownych przypadkach, szczegółowy opis architektury systemu wyjaśniający, w jaki sposób elementy oprogramowania współgrają ze sobą lub wzajemnie się uzupełniają oraz włączają się w ogólne przetwarzanie.

ZAŁĄCZNIK XII

Informacje dotyczące przejrzystości, o których mowa w art. 53 ust. 1 lit. b) – dokumentacja techniczna dostawców modeli AI ogólnego przeznaczenia przekazywana dostawcom niższego szczebla, którzy integrują dany model ze swoim systemem AI

Informacje, o których mowa w art. 53 ust. 1 lit. b), zawierają przynajmniej następujące elementy:

1. Ogólny opis systemu AI ogólnego przeznaczenia, w tym:

a) zadania, który dany model ma wykonywać, oraz rodzaj i charakter systemów AI, z którymi może zostać zintegrowany;

b) mające zastosowanie dopuszczalne zasady wykorzystania;

c) data wydania i metody dystrybucji;

d) sposób, w jaki model, w stosownych przypadkach, współdziała lub może być wykorzystywany do współdziałania ze sprzętem lub oprogramowaniem, które nie są częścią samego modelu;

e) w stosownych przypadkach, wersje odpowiedniego oprogramowania związanego z wykorzystaniem modelu AI ogólnego przeznaczenia;

f) architektura i liczba parametrów;

g) formę (np. tekst, obraz) oraz format danych wejściowych i wyjściowych;

h) licencja dla danego modelu.

2. Opis elementów modelu oraz procesu jego opracowywania, w tym:

a) środki techniczne (np. instrukcja obsługi, infrastruktura, narzędzia) wymagane do integracji danego modelu AI ogólnego przeznaczenia z systemami AI;

b) forma (np. tekst, obraz) oraz format danych wejściowych i wyjściowych, a także ich maksymalny rozmiar (np. rozmiar okna kontekstowego, itp.);

c) informacje na temat danych wykorzystywanych do trenowania, testowania i walidacji, w stosownych przypadkach, w tym rodzaju i pochodzenia danych oraz metody porządkowania.

ZAŁĄCZNIK XIII

Kryteria identyfikowania modeli AI ogólnego przeznaczenia z ryzykiem systemowym, o których mowa w art. 51

Do celów stwierdzenia, czy model AI ogólnego przeznaczenia ma zdolności lub skutki równoważne z tymi, które określono w art. 51 ust. 1 lit. a) i b), Komisja uwzględnia następujące kryteria:

a) liczbę parametrów modelu;

b) jakość lub rozmiar zbioru danych, na przykład mierzone za pomocą tokenów;

c) ilość zasobów obliczeniowych wykorzystanych do trenowania modelu, mierzoną we FLOP lub wskazaną przez połączenie innych zmiennych, takich jak szacunkowy koszt trenowania, szacowany czas potrzebny na trenowanie lub szacowane zużycie energii na potrzeby trenowania;

d) format danych wejściowych i wyjściowych danego modelu, takie jak tekst–tekst (duże modele językowe), tekst–obraz, multimodalne, a także najnowocześniejsze progi dla określania zdolności dużego oddziaływania dla każdego formatu, jak również szczególne rodzaje danych wejściowych i wyjściowych (np. sekwencje biologiczne);

e) poziomy odniesienia i oceny zdolności modelu, w tym analiza liczby zadań bez dodatkowego trenowania, zdolności adaptacji do uczenia się nowych, odrębnych zadań, stopień jego autonomii i skalowalności, narzędzia, do których ma dostęp;

f) czy ze względu na swój zasięg ma duży wpływ na rynek wewnętrzny, co należy zakładać, jeśli został udostępniony co najmniej 10 000 zarejestrowanych użytkowników biznesowych mających siedzibę w Unii;

g) liczbę zarejestrowanych użytkowników końcowych.