2024/1689

12.7.2024

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/1689

z dnia 13 czerwca 2024 r.

w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)

(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]),

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 (zwanych dalej „systemami AI") w Unii, zgodnie z wartościami Unii, w celu promowania upowszechniania zorientowanej 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 (zwanej „Kartą"), w tym demokracji, praworządności i ochrony środowiska, ochrony przed szkodliwymi skutkami systemów AI w Unii, a także wspierania 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, praworządności oraz ochronę 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 w łatwy sposób być przedmiotem obrotu 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 rozwijają, importują lub wykorzystują systemy AI. Aby zatem AI stałą się godna zaufania, należy zapewnić spójny i wysoki poziom ochrony w całej Unii poprzez ustanowienie jednolitych obowiązków dla operatorów i zagwarantowanie jednolitej ochrony nadrzędnego interesu publicznego

([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. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 21 maja 2024 r.

i praw osób na całym rynku wewnętrznym na podstawie 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 ich zakresie oraz ich wdrażanie i rozpowszechnianie. W zakresie, w jakim niniejsze rozporządzenie zawiera przepisy szczególne 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 szczególnych powinien być art. 16 TFUE. W świetle tych przepisów szczególnych i skorzystania z art. 16 TFUE należy skonsultować się z Europejską Radą Ochrony Danych.

(4) AI to szybko rozwijająca się grupa technologii, która przyczynia 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 odtwarzania różnorodności biologicznej i ekosystemów oraz łagodzenia zmiany klimatu i przystosowywania się do niej.

(5) Jednocześnie AI może stwarzać zagrożenia i wyrządzać szkody dla interesu publicznego i praw podstawowych chronionych przepisami prawa 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), podstawowymi prawami i wolnościami zapisanymi w traktatach oraz, zgodnie z art. 6 TUE – w Karcie. Warunkiem wstępnym jest to, by AI była technologią zorientowaną 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 dotyczące systemów AI wysokiego ryzyka. Przepisy te powinny być zgodne z Kartą, niedyskryminacyjne i zgodne z międzynarodowymi zobowiązaniami handlowymi Unii. Przepisy te 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, aby chronić prawa podstawowe, sprzyjać nowym innowacyjnym rozwiązaniom, umożliwiać tworzenie europejskiego ekosystemu podmiotów publicznych i prywatnych tworzących 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 zorientowanego na człowieka podejścia do AI i znalezienie się przez Unię 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 wnioskiem 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]) (zwanymi dalej „nowymi ramami prawnymi"). Zharmonizowane przepisy ustanowione 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. 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 zgodne 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 poziomie Unii, w tym z prawa do strajku czy swobody prowadzenia 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. Niniejsze rozporządzenie nie powinno mieć wpływu na przepisy mające na celu poprawę warunków pracy świadczonej za pośrednictwem platform internetowych ustanowione w dyrektywie Parlamentu Europejskiego i Rady w sprawie poprawy warunków pracy za pośrednictwem platform internetowych. Ponadto niniejsze rozporządzenie ma na celu zwiększenie skuteczności takich istniejących praw i środków ochrony prawnej poprzez ustanowienie szczególnych 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 zgodnego z prawem Unii, skutkującego ograniczeniem wykorzystania określonych systemów AI, gdy prawo to nie wchodzi w zakres stosowania niniejszego rozporządzenia lub służy uzasadnionym celom interesu publicznego innym niż cele niniejszego rozporządzenia. Na przykład niniejsze rozporządzenie nie powinno mieć wpływu na krajowe prawo pracy i przepisy dotyczące ochrony małoletnich, tj. osób poniżej 18. roku życia, uwzględniające komentarz ogólny nr 25 z 2021 r. w sprawie praw dziecka w środowisku cyfrowym zamieszczony w Konwencji ONZ o prawach dziecka, w zakresie w jakim prawo to i te przepisy nie dotyczą konkretnie systemów AI i służą innym uzasadnionym celom interesu publicznego.

(10) Podstawowe prawo do ochrony danych osobowych jest gwarantowane w szczególności przez rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([11]) i (UE) 2018/1725 ([12]) oraz dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 ([13]). Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE ([14]) dodatkowo chroni życie prywatne i poufność komunikacji, w tym określając warunki dotyczące 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, w tym w przypadku gdy zbiory danych zawierają połączenie 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. W zakresie, w jakim projektowanie, rozwój lub wykorzystywanie systemów AI wiąże się z przetwarzaniem danych osobowych, niniejsze rozporządzenie nie wpływa też na wynikające z prawa Unii lub prawa krajowego obowiązki w dziedzinie ochrony danych osobowych

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji 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 (Dz.U. L 169 z 25.6.2019, s. 1).

([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 (Dz.U. L 210 z 7.8.1985, s. 29).

([11]) 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).

([12]) 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).

([13]) 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).

([14]) 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).

spoczywające na dostawcach i podmiotach 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 sprawach, w tym z profilowaniem. Ustanowione w niniejszym rozporządzeniu 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 powinno pozostawać bez uszczerbku dla przepisów dotyczących odpowiedzialności dostawców usług pośrednich, określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2065 ([15]).

(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 swobody 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 założeń programistycznych, 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 tworzenia modeli lub algorytmów na podstawie informacji wejściowych lub danych. Techniki, które umożliwiają wnioskowanie podczas tworzenia systemu AI, obejmują mechanizmy uczenia maszynowego, 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 w wyniku umożliwiania uczenia się, rozumowania lub modelowania. 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 AI 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 wykorzystywania. 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", o którym mowa w niniejszym rozporządzeniu, należy interpretować jako osobę fizyczną lub prawną, w tym organ publiczny, agencję lub inny podmiot, która wykorzystuje system AI, nad którym sprawuje kontrolę, oprócz przypadków gdy wykorzystywanie 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.

(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 zautomatyzowane 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.

([15]) 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).

(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 behawioralne bądź osobowości, język, religia, przynależność do mniejszości narodowej, orientacja seksualna lub poglądy polityczne. 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 pełnienia 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, aby pomóc mu w podjęciu decyzji 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” zbieranie 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 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 zebrane, a porównanie i identyfikacja następują ze znacznym opóźnieniem. Dotyczy to materiałów, takich jak zdjęcia lub materiały wideo generowane przez kamery telewizji przemysłowej lub urządzenia prywatne, które to materiały zostały wygenerowane, 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 ono stanów fizycznych, takich jak ból lub zmęczenie; w tym na przykład systemów stosowanych do wykrywania poziomu zmęczenia zawodowych pilotów lub kierowców w celu zapobiegania wypadkom. Nie obejmuje ono 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, lub cechy głosu danej osoby, takie jak podniesiony ton lub szept.

(19) Do celów niniejszego rozporządzenia pojęcie „przestrzeni publicznej” należy rozumieć jako odnoszące się do każdej przestrzeni fizycznej, która jest dostępna dla nieokreślonej liczby osób fizycznych, niezależnie od tego, czy dana przestrzeń jest własnością prywatną czy publiczną, a także niezależnie od rodzaju działalności, dla której się ją wykorzystuje, takiej jak działalność handlowa (na przykład sklepy, restauracje, kawiarnie), działalność usługowa (na przykład banki, działalność zawodowa, hotelarstwo), działalność sportowa (na przykład baseny, sale do ćwiczeń, stadiony), działalność transportowa (na przykład dworce autobusowe i kolejowe, stacje metra, lotniska, środki transportu), działalność rozrywkowa (na przykład kina, teatry, muzea, sale koncertowe i konferencyjne) lub przestrzenie służące wypoczynkowi lub innym celom (na przykład drogi publiczne i place, parki, lasy i place zabaw). Przestrzeń należy uznać za przestrzeń publiczną również wtedy, gdy niezależnie od potencjalnych ograniczeń w zakresie pojemności lub bezpieczeństwa, dostęp do niej 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. Danej przestrzeni nie należy natomiast uznawać za przestrzeń publiczną, jeśli dostęp do niej 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 taką przestrzenią. Faktyczna możliwość samego dostępu (taka jak niezamknięte drzwi, otwarta bramka w ogrodzeniu) nie oznacza, że dana przestrzeń 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 przestrzenie, które nie stanowią przestrzeni publicznej. Do przestrzeni publicznej nie zaliczają się więzienia ani strefy kontroli granicznej. Niektóre przestrzenie mogą zawierać zarówno przestrzenie publiczne, jak i niepubliczne, takie jak hol w prywatnym budynku mieszkalnym prowadzący do gabinetu lekarskiego lub lotnisko. Przestrzenie internetowe również nie są objęte tym pojęciem, 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 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 rozwoju 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 niniejszego 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 innowacyjną ścieżkę godnej zaufania AI w Unii. Europejska Rada ds. Sztucznej Inteligencji (zwana dalej „Radą 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 wykorzystaniem 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 rozwojem, działaniem 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 stosowania niniejszego rozporządzenia, nawet jeśli nie zostały wprowadzane do obrotu, oddane do użytku ani są 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 wprowadzony do obrotu lub oddany 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 lub miejsce zamieszkania w państwie trzecim, w zakresie, w jakim wyniki wytworzone przez te systemy 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, niniejszego rozporządzenia nie powinno się stosować do organów publicznych państwa trzeciego i organizacji międzynarodowych działających w ramach współpracy lub na mocy zawartych na poziomie Unii lub poziomie krajowym umów międzynarodowych o współpracy organów ścigania i wymiarów sprawiedliwości z Unią lub państwami członkowskimi, pod warunkiem zapewnienia przez to państwo trzecie lub organizację międzynarodową odpowiednich zabezpieczeń w odniesieniu do ochrony podstawowych praw i wolności osób fizycznych. 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 wymiaru sprawiedliwości na mocy niniejszego rozporządzenia powinny ocenić, czy te ramy współpracy lub umowy międzynarodowe zawierają odpowiednie

zabezpieczenia w odniesieniu do ochrony podstawowych praw i wolności osób fizycznych. Będące odbiorcami organy krajowe oraz 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 zawarcia nowych w przyszłości umawiające się strony powinny dołożyć wszelkich starań, by dostosować takie umowy do wymogów niniejszego rozporządzenia.

(23) Niniejsze rozporządzenie powinno być również stosowane 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 wykorzystuje się je 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 on podmiotem publicznym czy prywatnym. W przypadku celów wojskowych i obronnych, 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 przypadku 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 stosuje się do nich szczególne przepisy krajowe. Jeżeli jednak system AI rozwinięty, 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 system AI do celów inne niż cele wojskowe, obronne lub cele bezpieczeństwa narodowego powinien zapewnić zgodność systemu AI 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 niestanowiących podstawy wyłączenia, takich jak cele cywilne lub ściganie przestępstw, są objęte zakresem stosowania niniejszego rozporządzenia, a dostawcy tych systemów powinni zapewnić zgodność z niniejszym rozporządzeniem. W takich przypadkach fakt, że system AI może wchodzić w zakres stosowania 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 stosowania 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 stosowania 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 stosowania systemy i modele AI rozwinięte i oddane do użytku wyłącznie do celów badań naukowych i rozwojowych. Ponadto należy zapewnić, aby niniejsze rozporządzenie nie wpływało w żaden inny sposób na działalność badawczo-rozwojową dotyczącą systemów lub modeli AI przed wprowadzeniem tych systemów lub modeli do obrotu lub oddaniem ich do użytku. Przepisów niniejszego rozporządzenia nie powinno się również stosować do zorientowanej na produkty działalności badawczej, testowej i rozwojowej dotyczącej systemów lub modeli AI przed oddaniem tych systemów i modeli do użytku lub wprowadzaniem ich do obrotu. Wyłączenie to pozostaje to bez uszczerbku dla obowiązku zapewnienia zgodności z niniejszym rozporządzeniem, gdy system AI objęty zakresem stosowania niniejszego rozporządzenia jest wprowadzany do obrotu lub oddawany do użytku w wyniku takiej działalności badawczo-rozwojowej, oraz dla stosowania przepisów dotyczących piaskownic regulacyjnych w zakresie AI i testów w warunkach rzeczywistych. Ponadto bez uszczerbku dla wyłączenia systemów AI rozwiniętych i oddanych do użytku wyłącznie do celów badań naukowych i rozwojowych, 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 zbiór 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 w zakresie AI, ustanowienie wymogów dotyczących systemów AI wysokiego ryzyka i obowiązków spoczywających na odpowiednich operatorach oraz ustanowienie obowiązków w zakresie przejrzystości w odniesieniu do niektórych systemów AI.

(27) Chociaż podstawą proporcjonalnego i skutecznego zbioru 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; solidność techniczna 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, wytyczne te przyczyniają się do zaprojektowania spójnej, wiarygodnej i zorientowanej na człowieka AI, zgodnie z Kartą i wartościami, na których opiera się Unia. Zgodnie z wytycznymi grupy ekspertów wysokiego szczebla ds. AI przewodnia i nadzorcza rola człowieka oznacza, że systemy AI rozwija 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. Solidność techniczna i bezpieczeństwo oznaczają, że systemy AI rozwija się i wykorzystuje w taki sposób, by okazały się wytrzymałe w przypadku wystąpienia problemów oraz odporne na próby zmiany ich wykorzystania lub skuteczności działania, co pozwoli zapobiec bezprawnemu wykorzystaniu przez osoby trzecie i zminimalizować niezamierzone szkody. Ochrona prywatności i zarządzanie danymi oznaczają, że systemy AI rozwija 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 rozwija 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 o zdolnościach i ograniczeniach tego systemu AI, a osoby, na które AI ma wpływ, o przysługujących im prawach. Różnorodność, niedyskryminacja i sprawiedliwość oznaczają, że systemy AI rozwija 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 rozwija się i wykorzystuje w sposób zrównoważony, przyjazny dla środowiska i przynoszący korzyści wszystkim ludziom, jednocześnie monitorując i oceniając długoterminowy wpływ tych systemów na osoby fizyczne, 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 przedmiotowe zasady etyczne.

(28) Oprócz wielu korzystnych zastosowań AI może ona być również wykorzystywana niewłaściwie i może dostarczać nowych i potężnych narzędzi do praktyk manipulacji, wyzyskiwania i kontroli społecznej. Takie praktyki są szczególnie szkodliwe i stanowią nadużycie i powinny być zakazane, ponieważ są sprzeczne z unijnymi wartościami dotyczącymi 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 AI 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, których celem lub skutkiem jest znacząca zmiana 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. Takie systemy AI 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 nie są świadome takich technik lub nawet jeśli są ich świadome, mogą zostać 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, jakim bodźcom są poddawane osoby, do tego stopnia, że mogą one znacząco zmieniać 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 ([16]) 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 ich wykorzystanie. Takie systemy AI mogą być wprowadzane do obrotu, oddawane do użytku lub wykorzystywane w celu lub ze skutkiem znaczącej zmiany zachowania danej osoby, oraz w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić poważną szkodę 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

([16]) 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).

można zakładać, że zaistniał zamiar dokonania zmiany zachowania, jeżeli zmiana ta wynika z czynników, które mają charakter zewnętrzny w stosunku do systemu AI i które są poza kontrolą dostawcy lub podmiotu stosującego, 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 mieli zamiar wyrządzić poważną szkodę, istotny jest fakt, że szkoda wynika z praktyk manipulacyjnych opartych na AI lub ich wykorzystywania. Zakazy dotyczące takich praktyk w zakresie AI stanowią uzupełnienie przepisów zawartych w dyrektywie Parlamentu Europejskiego i Rady 2005/29/WE ([17]), 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 fizycznej 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 praktyki manipulacyjne oparte na AI.

(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 przez podmioty publiczne lub prywatne scoringu społecznego, mogą prowadzić do wyników stanowiących dyskryminację i do 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. Scoring społeczny uzyskany w rezultacie działania takich systemów AI może prowadzić do krzywdzącego lub niekorzystnego traktowania osób fizycznych lub całych grup osób fizycznych 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, które przynoszą takie krzywdzące lub niekorzystne wyniki. Zakaz ten nie powinien mieć wpływu na zgodne z prawem 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, do tego stopnia że może ono 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 zainteresowanych w związku z działaniami organów ścigania lub na które działania te miały wpływ.

(33) Wykorzystanie tych systemów w celu ścigania przestępstw powinno zatem być zabronione, z wyjątkiem wyczerpującej listy wąsko zdefiniowanych sytuacji, w których wykorzystanie to jest bezwzględnie 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 wymienionych w załączniku do niniejszego rozporządzenia, w przypadku gdy przestępstwa te podlegają w danym państwie członkowskim karze pozbawienia

([17]) 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).

wolności lub środkowi polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej cztery lata, zgodnie z ich definicją w prawie tego państwa członkowskiego. Taki próg kary pozbawienia wolności lub środka 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 wykaz przestępstw przedstawiony w załączniku do niniejszego rozporządzenia opiera się na 32 przestępstwach wymienionych w decyzji ramowej Rady 2002/584/WSiSW ([18]), 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 może być 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 ([19]), w przypadku gdy zakłócenie lub zniszczenie takiej infrastruktury krytycznej spowodowałoby bezpośrednie zagrożenie życia lub bezpieczeństwa fizycznego 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.

(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 wyczerpującej listy należy uwzględniać pewne elementy, w szczególności charakter sytuacji, która skutkowała złożeniem wniosku, wpływ wykorzystania takich systemów na prawa i wolności wszystkich zainteresowanych osób, a także zabezpieczenia i warunki przewidziane na potrzeby wykorzystania 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 odpowiedni organ ścigania przeprowadził ocenę skutków dla 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 wykorzystania w każdej z wyżej wymienionych sytuacji.

(35) Każde wykorzystanie systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw powinno wymagać wyraźnego i szczególnego zezwolenia wydanego przez organ wymiaru sprawiedliwości lub niezależny organ administracyjny państwa członkowskiego, którego decyzje są wiążące. Takie zezwolenie należy co do zasady uzyskać przed wykorzystaniem 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 wykorzystania 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 systemu AI powinno być ograniczone do bezwzględnie niezbędnego minimum i powinno podlegać odpowiednim zabezpieczeniom i warunkom określonym w prawie krajowym i sprecyzowanym przez sam organ ścigania w kontekście każdego przypadku nadzwyczajnego wykorzystania. Ponadto organ ścigania powinien w takich sytuacjach wystąpić 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

([18]) 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).

([19]) 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).

związane z tym zezwoleniem rezultaty i wyniki uzyskane podczas tego wykorzystania. Powyższe nie powinno mieć zastosowania do danych wejściowych uzyskanych legalnie zgodnie z innymi przepisami prawa Unii lub prawa krajowego. W każdym przypadku żadnej decyzji wywołującej niepożądane skutki prawne dla 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 ustanowionymi w niniejszym rozporządzeniu oraz w przepisach krajowych, należy powiadamiać je o każdym wykorzystaniu systemu identyfikacji biometrycznej w czasie rzeczywistym. 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. Komisja powinna zostać powiadomiona o takich przepisach krajowych w terminie 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 wykorzystywanie takich systemów i przetwarzanie takich 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 wyznaczonych przez te ramy. W tym kontekście niniejsze rozporządzenie nie ma na celu ustanowienia 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 szczególnymi 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 ani obowiązującym szczegółowym przepisom prawa krajowego, które mogą stanowić podstawę ubiegania się o takie zezwolenie.

(39) Wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane z wykorzystaniem 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 pozostawać zgodne z wymogami wynikającymi 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 zakazujących takiego wykorzystywania, 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 ustanowionymi w art. 5 ust. 1 akapit pierwszy lit. g) – 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 akapit pierwszy lit. d) – w takim zakresie, w jakim dotyczy on wykorzystania systemów AI objętych tym przepisem, w art. 5 ust. 1 akapit pierwszy lit. h), art. 5 ust. 2–6 i 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 stosowania 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 zapewnić zgodność z przepisami ustanowionymi 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 akapit pierwszy lit. g) – 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 akapit pierwszy lit. d) – w takim zakresie, w jakim dotyczy on wykorzystania systemów AI objętych tym przepisem, w art. 5 ust. 1 lit. h), art. 5 ust. 2–

6 i 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 uczestniczy w działalności przestępczej 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 prawdopodobieństwa 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 prawdopodobieństwa 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 nieukierunkowane pozyskiwanie (ang. untargeted scraping) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej, ponieważ praktyka ta zwiększa poczucie masowego nadzoru 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 wykrywania stanu emocjonalnego osób fizycznych 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 są zgodne z określonymi obowiązkowymi wymogami. Wymogi te powinny zapewniać, aby systemy AI wysokiego ryzyka dostępne w Unii lub takie, których wyniki są w inny sposób wykorzystywane w Unii, nie stwarzały niedopuszczalnego ryzyka dla istotnych interesów publicznych Unii uznanych w prawie Unii i przez to prawo chronionych. W oparciu o nowe ramy prawne, jak wyjaśniono w zawiadomieniu Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022” ([20]), ogólna zasada stanowi, że do jednego produktu można stosować więcej niż jeden akt prawny unijnego prawodawstwa harmonizacyjnego, taki jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 ([21]), rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 ([22]) lub dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady ([23]), ponieważ udostępnianie lub oddawanie do użytku może mieć miejsce tylko wtedy, gdy produkt jest zgodny z całością obowiązującego unijnego prawodawstwa harmonizacyjnego. Aby zapewnić spójność

([20]) Dz.U. C 247 z 29.6.2022, s. 1.

([21]) 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).

([22]) 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).

([23]) 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).

i uniknąć niepotrzebnych obciążeń administracyjnych lub kosztów, dostawcy produktu, który zawiera co najmniej jeden system AI wysokiego ryzyka, do którego stosuje się wymogi niniejszego rozporządzenia oraz unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku do niniejszego rozporządzenia, powinni mieć swobodę w zakresie decyzji operacyjnych dotyczących sposobu zapewnienia w optymalny sposób zgodności produktu zawierającego co najmniej jeden system AI 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.

(47) Systemy AI mogą mieć niepożądany wpływ na zdrowie i bezpieczeństwo osób, w szczególności w przypadku gdy takie systemy funkcjonują jako związane z bezpieczeństwem elementy produktów. Zgodnie z celami unijnego prawodawstwa harmonizacyjnego, polegającymi na ułatwieniu swobodnego przepływu produktów na rynku wewnętrznym oraz zapewnieniu, aby na rynek trafiały wyłącznie produkty bezpieczne i zgodne w pozostałym zakresie, istotne jest odpowiednie zapobieganie ryzyku 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 to, 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 prawo do niedyskryminacji, 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, a także prawo do dobrej administracji. Oprócz tych praw należy podkreślić, że dzieciom przysługują szczególne prawa zapisane w art. 24 Karty oraz w Konwencji ONZ o prawach dziecka, szerzej rozwinięte w komentarzu ogólnym nr 25 w sprawie praw dziecka w środowisku cyfrowym zamieszczony w Konwencji ONZ o prawach dziecka, 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 dotkliwości szkody, jaką może wyrządzić system AI, w tym w odniesieniu do zdrowia i bezpieczeństwa osób.

(49) W odniesieniu do systemów AI wysokiego ryzyka, które są związanymi z bezpieczeństwem elementami produktów lub systemów objętych zakresem stosowania rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 ([24]), rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 167/2013 ([25]), rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013 ([26]), dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE ([27]), dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/797 ([28]), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858 ([29]), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 ([30]) oraz

([24]) 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).

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) 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).

([30]) 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).

rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2144 ([31]) lub które same są takimi produktami lub systemami, wskazane jest dokonanie zmian tych aktów w celu zapewnienia, aby Komisja, przyjmując wszelkie stosowne akty delegowane lub wykonawcze na podstawie wspomnianych aktów, 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 ustanowione w niniejszym rozporządzeniu.

(50) W przypadku systemów AI, które są związanymi z bezpieczeństwem elementami produktów objętych zakresem stosowania niektórych przepisów unijnego prawodawstwa harmonizacyjnego wymienionych w załączniku do niemniejszego rozporządzenia lub które same są takimi produktami, 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, wyroby medyczne do diagnostyki *in vitro*, motoryzacja i lotnictwo.

(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 stosuje się do tego produktu. Dotyczy to w szczególności rozporządzeń (UE) 2017/745 i (UE) 2017/746, w przypadku gdy ocenę zgodności przeprowadza strona trzecia w odniesieniu do produktów średniego i wysokiego ryzyka.

(52) W odniesieniu do samodzielnych systemów AI, a mianowicie systemów 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 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 wskazanych w niniejszym rozporządzeniu nie prowadzą do znaczącego 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 na celu wykonywanie wąsko określonych zadań proceduralnych – jak np. 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 systemu AI w kontekście wymienionym w wykazie przypadków wykorzystania wysokiego ryzyka zamieszczonym w załączniku do niniejszego rozporządzenia. Drugim warunkiem powinno być to, aby

([31]) 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).

zadanie wykonywane przez system AI miało na celu poprawę wyników już zakończonego działania przeprowadzonego przez człowieka, które może być istotne w kontekście celów przypadków wykorzystania wysokiego ryzyka, wymienionych w załączniku do niniejszego rozporządzenia. 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 wcześniej 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 wykorzystuje 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 systemy AI wykorzystywane w przypadkach wykorzystania wysokiego ryzyka, wymienionych w załączniku do niniejszego rozporządzenia, należy uznać za stwarzające znaczące ryzyko szkody dla zdrowia, bezpieczeństwa lub praw podstawowych, 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 warunków, o których mowa powyżej, 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 przekazać tę dokumentację na wniosek właściwym organom krajowym. Taki dostawca powinien być zobowiązany do zarejestrowania systemu AI w bazie danych UE ustanowionej na mocy niniejszego rozporządzenia. By zapewnić dalsze wskazówki dotyczące praktycznego wdrażania warunków, na jakich systemy AI wymienione w załączniku do niniejszego rozporządzenia są, w drodze wyjątku, uznawane za niebędące systemami wysokiego ryzyka, Komisja powinna, po konsultacji z Radą ds. AI, przedstawić wytyczne w sprawie tego praktycznego wdrażania, uzupełnione wyczerpującym wykazem praktycznych przypadków wykorzystania systemów AI, które stanowią przypadki wykorzystania wysokiego ryzyka oraz które nie stanowią przypadków takiego wykorzystania.

(54) Ponieważ dane biometryczne stanowią szczególną kategorię danych osobowych, kilka krytycznych przypadków wykorzystania systemów biometrycznych należy zaklasyfikować jako obarczone wysokim ryzykiem, o ile ich wykorzystywanie jest dozwolone na mocy odpowiednich przepisów prawa Unii i prawa krajowego. Techniczne niedokładności systemów AI przeznaczonych do zdalnej identyfikacji biometrycznej osób fizycznych mogą prowadzić do nieobiektywnych wyników i wywoływać skutki w postaci dyskryminacji. Ryzyko wystąpienia takich nieobiektywnych 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 zaklasyfikować 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 tą 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 AI wysokiego ryzyka nie należy uznawać systemów biometrycznych, które są przeznaczone wyłącznie do tego, by umożliwić stosowanie środków na rzecz cyberbezpieczeństwa i ochrony danych osobowych.

(55) W odniesieniu do zarządzania infrastrukturą krytyczną i jej działania jako systemy wysokiego ryzyka należy klasyfikować systemy AI, które są przeznaczone do wykorzystania jako związane z bezpieczeństwem elementy procesów zarządzania i działania w przypadku krytycznej infrastruktury cyfrowej wymienionej w pkt 8 załącznika do dyrektywy (UE) 2022/2557, ruchu drogowego i zaopatrzenia w wodę, gaz, ciepło i energię elektryczną, ponieważ ich awaria lub nieprawidłowe działanie mogą stworzyć ryzyko dla 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 ryzyka dla fizycznej integralności infrastruktury krytycznej, a co za tym idzie, do ryzyka dla zdrowia i bezpieczeństwa osób i mienia. Elementów przeznaczonych wyłącznie do celów cyberbezpieczeństwa nie należy kwalifikować jako związanych z bezpieczeństwem elementów. Przykładami związanych z bezpieczeństwem elementów takiej infrastruktury krytycznej są systemy monitorowania ciśnienia wody lub systemy sterowania alarmem przeciwpożarowym w centrach przetwarzania danych w chmurze (ang. cloud computing centres).

(56) Wdrażanie 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 przydzielania osób do tych instytucji lub programów, do oceniania wyników nauki osób, do oceniania odpowiedniego poziomu wykształcenia i istotnego oddziaływania na poziom wykształcenia i szkolenia, jaki dana osoba fizyczna 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 mogą wpływać na jej zdolność do zapewnienia sobie źródła utrzymania. Takie systemy, jeżeli są niewłaściwie zaprojektowane i wykorzystywane, 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 lub charakter i do monitorowania lub oceny osób pozostających w umownych stosunkach pracy, należy również zaklasyfikować jako systemy wysokiego ryzyka, ponieważ systemy te mogą w znacznym stopniu wpływać na przyszłe perspektywy zawodowe, źródła utrzymania tych osób i prawa pracownicze. Odpowiednie 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 oceniania, awansowania 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 takich osób mogą również podważać ich prawa podstawowe w zakresie ochrony danych i prywatności.

(58) Innym obszarem, w którym wykorzystanie 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 zaklasyfikować 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 zgodnych i bezpiecznych systemów AI, pod warunkiem że systemy te nie stwarzają wysokiego ryzyka dla osób prawnych i fizycznych. Ponadto jako systemy wysokiego ryzyka należy zaklasyfikować systemy AI wykorzystywane do przeprowadzania scoringu kredytowego 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 przeprowadzania 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, rozwinięte i wykorzystywane, mogą naruszać ich prawa podstawowe i prowadzić do poważnych konsekwencji dla życia i zdrowia ludzi, w tym wykluczenia finansowego i dyskryminacji. Wreszcie systemy AI przeznaczone do przeprowadzania oceny i klasyfikowania 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, a także w ramach systemów oceny stanu zdrowia pacjentów w nagłych wypadkach, należy zaklasyfikować 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 rodzajami wykorzystania 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 innego niepożądanego wpływu na prawa podstawowe zagwarantowane w Karcie. W szczególności jeżeli system AI nie jest trenowany z wykorzystaniem danych wysokiej jakości, nie spełnia odpowiednich wymogów pod względem skuteczności jego działania, 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 wykorzystania w kontekście ścigania przestępstw, w którym dokładność, wiarygodność i przejrzystość są szczególnie ważne dla uniknięcia niepożądanego wpływu, 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 prawa Unii i prawa krajowego. Ze względu na charakter 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 w ramach wsparcia udzielanego organom ścigania w zakresie 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 zakazane na mocy niniejszego rozporządzenia, do oceny ryzyka popełnienia przestępstwa lub ponownego popełnienia przestępstwa przez osobę fizyczną niewyłącznie na podstawie profilowania osób fizycznych lub 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 wykorzystania w postępowaniach administracyjnych prowadzonych przez organy podatkowe i celne, jak również przez jednostki analityki finansowej wykonujące zadania administracyjne dotyczące analizy informacji na podstawie przepisów prawa Unii dotyczących przeciwdziałania praniu pieniędzy, nie należy zaklasyfikować jako systemów AI wysokiego ryzyka wykorzystywanych przez organy ścigania do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Wykorzystanie narzędzi sztucznej inteligencji przez organy ścigania i inne odpowiednie organy nie powinno stać się czynnikiem powodującym nierówności lub wykluczenie. Nie należy ignorować wpływu wykorzystania 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 osób, na które AI ma wpływ, w szczególności ich prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji. O ile wykorzystanie systemów AI jest dozwolone zgodnie z właściwymi przepisami prawa Unii i prawa krajowego, 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 rodzajów ryzyka 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 ([32]), dyrektywie

([32]) 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).

Parlamentu Europejskiego i Rady 2013/32/UE ([33]) i w innych właściwych przepisach prawa Unii. Wykorzystanie systemów AI w zarządzaniu migracją, azylem i kontrolą graniczną nie powinno w żadnym wypadku być wykorzystywane 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 one 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.

(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 zakwalifikować systemy AI przeznaczone do wykorzystania przez organy wymiaru sprawiedliwości lub w ich imieniu, aby pomóc tym organom w poszukiwaniu i interpretacji faktów i prawa oraz w stosowaniu przepisów prawa 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. Wykorzystanie narzędzi AI może wspierać uprawnienia decyzyjne sędziów lub niezależność sądownictwa, ale nie powinno ich zastępować; 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) 2024/900 ([34]) 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 zachowania wyborcze osób fizycznych podczas głosowania w wyborach lub referendach, należy zaklasyfikować 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 podstawie 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 niniejsze rozporządzenie nie stanowi wyraźnie inaczej.

(64) Aby ograniczyć ryzyko stwarzane przez systemy AI wysokiego ryzyka wprowadzone do obrotu lub oddawane do użytku oraz aby zapewnić wysoki poziom wiarygodności, należy stosować pewne obowiązkowe wymogi 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 zapewnienia zgodności z obowiązkowymi wymogami 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 do jednego produktu można stosować więcej niż jedne akt prawny unijnego prawodawstwa harmonizacyjnego, 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 obowiązujące unijne prawodawstwo harmonizacyjne, w związku z czym wymogi niniejszego rozporządzenia uzupełnią obowiązujące unijne prawodawstwo harmonizacyjne. Na przykład maszyny lub wyroby medyczne zawierające system AI mogą stwarzać ryzyko, które nie zostało uwzględnione w zasadniczych wymogach w zakresie zdrowia

([33]) 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).

([34]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/900 w sprawie przejrzystości i targetowania reklamy politycznej (Dz. U. L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

i bezpieczeństwa ustanowionych 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 stosuje się wymogi niniejszego rozporządzenia i unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych, wymienionego w załączniku do niniejszego rozporządzenia, powinni mieć swobodę w zakresie decyzji operacyjnych dotyczących sposobu zapewnienia w optymalny sposób zgodności produktu zawierającego co najmniej jeden system AI ze wszystkimi mającymi zastosowanie wymogami unijnego prawodawstwa harmonizacyjnego. Swoboda 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 i wymienionego w załączniku do niniejszego rozporządzenia. Nie powinno to w żaden sposób podważać spoczywającego na dostawcy obowiązku zapewnienia zgodności z wszystkimi mającymi zastosowanie wymogami.

(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 oraz uzasadnienie i dokumentację wszelkich istotnych decyzji i działań podjętych zgodnie z niniejszym rozporządzeniem. Proces ten powinien zapewniać, aby dostawca identyfikował ryzyko lub niepożądany wpływ 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 przypadki wykorzystania 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 takich przypadków wykorzystania 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 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 szczególnego dodatkowego szkolenia, by zaradzić temu dającemu się przewidzieć niewłaściwemu wykorzystaniu. 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) Do systemów AI wysokiego ryzyka należy stosować wymogi dotyczące zarządzania ryzykiem, jakości i istotności wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji podmiotom stosującym, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Wymogi te są konieczne, aby skutecznie ograniczyć ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych. Z uwagi na brak innych racjonalnie dostępnych środków, które powodowałyby mniejsze ograniczenia w handlu, wymogi te nie stanowią nieuzasadnionych ograniczeń w handlu.

(67) Wysokiej jakości dane i dostęp do wysokiej jakości danych odgrywają kluczową rolę w ustanawianiu struktury i zapewnianiu 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, powinny być adekwatne, wystarczająco reprezentatywne oraz w jak największym stopniu wolne od błędów i kompletne z punktu widzenia przeznaczenia systemu. Aby ułatwić zapewnienie zgodności z prawem Unii o ochronie danych, takim jak rozporządzenie (UE) 2016/679, praktyki w zakresie administrowania i zarządzania danymi powinny przewidywać, w przypadku danych osobowych, zapewnianie przejrzystości pierwotnego celu zbierania 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, ang. feedback loops). 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 należących do grup szczególnie wrażliwych, 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 wdrażania 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. Zgodność z wymogami związanymi z zarządzaniem danymi można zapewnić, 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 wdrażaniu 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 zakresie obszarów działalności tych podmiotów 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 prawie Unii 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 bezwzględnie konieczne 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 ustanowionych w niniejszym rozporządzeniu, w uzupełnieniu warunków ustanowionych 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 rozwinięto 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 cechy, 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 w spełnianiu ich obowiązków ustanowionych w niniejszym rozporządzeniu, 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 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. Obejmowałyby one informacje na temat ewentualnych znanych i dających się przewidzieć okoliczności związanych z wykorzystaniem systemu AI wysokiego ryzyka, w tym działań podmiotu stosującego, które mogą wpływać na zachowanie i skuteczność działania 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 systemu AI. Przejrzystość, w tym towarzyszące instrukcje obsługi, powinny pomóc podmiotom stosującym w korzystaniu z systemu i wspierać podejmowanie przez te podmioty świadomych decyzji. Podmioty stosujące powinny, między innymi, być lepiej przygotowane, aby dokonać właściwego wyboru systemu, z którego zamierzają korzystać w świetle mających do nich zastosowanie obowiązków, mieć wiedzę na temat zamierzonych i wykluczonych sposobów wykorzystania 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 sposobów wykorzystania 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 i prawdopodobnie posiadanej przez te podmioty wiedzy. Instrukcje obsługi powinny być udostępniane w języku łatwo zrozumiałym dla docelowych podmiotów stosujących, określonym przez zainteresowane państwo członkowskie.

(73) Systemy AI wysokiego ryzyka należy projektować i rozwijać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie, zapewniać, by ich wykorzystanie było zgodne z przeznaczeniem oraz zapewniać, aby skutki ich wykorzystania były uwzględniane 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 ryzyka lub zatrzymać system, jeżeli nie działa on zgodnie z przeznaczeniem. Zważywszy na istotne konsekwencje dla osób 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 nie mógł podejmować żadnych działań ani decyzji na podstawie identyfikacji wynikającej z systemu, dopóki nie została ona odrębnie zweryfikowana i potwierdzona 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, wymóg ten 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 odpowiednie organizacje i zainteresowane strony zachęca się, by należycie uwzględniały ograniczanie ryzyka i negatywnych skutków związanych z systemem AI. Oczekiwany poziom wskaźników skuteczności działania należy zadeklarować w załączonej instrukcji obsługi. Dostawców wzywa się, by przekazywali te informacje podmiotom stosującym 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 ([35]) i 2014/32/UE ([36]), 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.

([35]) 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).

([36]) 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 96 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 ze 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 rozwijanie 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 tym ryzykiem może mieć konsekwencje dla bezpieczeństwa lub negatywnie wpłynąć na prawa podstawowe, na przykład z powodu błędnych decyzji lub nieprawidłowych lub stronniczych wyników generowanych przez system AI.

(76) Cyberbezpieczeństwo odgrywa kluczową rolę w zapewnianiu odporności systemów AI na próby modyfikacji ich wykorzystania, 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 wnioskowania o członkostwie), 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 stosowania rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, zgodnie z tym rozporządzeniem mogą wykazać zgodność z wymogami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu w drodze spełnienia zasadniczych wymogów w zakresie cyberbezpieczeństwa ustanowionych w tym rozporządzeniu. W przypadku gdy systemy AI wysokiego ryzyka spełniają zasadnicze wymogi rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, należy uznać, że wykazują zgodność z wymogami w zakresie cyberbezpieczeństwa ustanowionymi w niniejszym rozporządzeniu w zakresie, w jakim spełnienie tych wymogów wykazano w deklaracji zgodności UE lub w jej częściach wydanych zgodnie z tym rozporządzeniem. W tym celu ocena ryzyka dotyczącego cyberbezpieczeństwa związanego z produktem z elementami cyfrowymi, które zaklasyfikowano jako system AI wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, przeprowadzana na podstawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, powinna uwzględniać ryzyko dla cyberodporności systemu AI w odniesieniu do podejmowanych przez nieupoważnione osoby trzecie prób zmiany jego wykorzystania, 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 praw podstawowych zgodnie z wymogami niniejszego rozporządzenia.

(78) Procedura oceny zgodności przewidziana w niniejszym rozporządzeniu powinna mieć zastosowanie do zasadniczych wymogów w zakresie cyberbezpieczeństwa produktu z elementami cyfrowymi objętego rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zaklasyfikowanego jako system AI wysokiego ryzyka na podstawie niniejszego rozporządzenia. Zasada ta nie powinna jednak powodować zmniejszenia niezbędnego poziomu ufności w odniesieniu do produktów krytycznych z elementami cyfrowymi objętych rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. 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 Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi 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 Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi 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 Parlamentu Europejskiego i Rady (UE) 2019/881 ([37]), Komisja powinna współpracować z ENISA w kwestiach związanych z cyberbezpieczeństwem systemów AI.

([37]) 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).

(79) Należy zapewnić, aby odpowiedzialność za wprowadzenie do obrotu lub oddanie do użytku systemu AI wysokiego ryzyka ponosiła konkretna osoba fizyczna lub prawna określona jako dostawca, niezależnie od tego, czy ta osoba fizyczna lub prawna jest osobą, która zaprojektowała lub rozwinęła 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 wykorzystanie 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 AI 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 ([38]) 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.

(81) Dostawca powinien ustanowić solidny 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 prawa Unii, powinni mieć możliwość włączenia elementów systemu zarządzania jakością przewidzianego w niniejszym rozporządzeniu do istniejącego systemu zarządzania jakością przewidzianego w innych sektorowych przepisach prawa Unii. Komplementarność między niniejszym rozporządzeniem a obowiązującymi sektorowymi przepisami prawa 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 poziomie 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 przepisów niniejszego rozporządzenia i stworzenia równych warunków działania dla operatorów, a także uwzględniając różne formy udostępniania produktów cyfrowych, należy zapewnić, aby w każdych okolicznościach osoba, która ma miejsce zamieszkania lub siedzibę w Unii, była w stanie przekazać organom wszystkie niezbędne informacje dotyczące zgodności danego systemu AI. W związku z tym dostawcy mający miejsce zamieszkania lub siedzibę w państwach trzecich przed udostępnieniem swoich systemów AI w Unii powinni ustanowić – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego miejsce zamieszkania lub 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 miejsca zamieszkania lub siedziby w Unii, oraz w pełnieniu funkcji ich osoby kontaktowej mającej miejsce zamieszkania lub 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 spełniać 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 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 odmienny podział obowiązków. Miałoby to miejsce również w przypadku, gdy 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 zmieni 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 należy stosować bez uszczerbku dla bardziej szczegółowych przepisów ustanowionych w unijnym prawodawstwie harmonizacyjnym opartym o nowe ramy prawne, wraz z którymi należy stosować niniejsze rozporządzenie. Na przykład do systemów

([38]) 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).

AI wysokiego ryzyka będących wyrobami medycznymi w rozumieniu rozporządzenia (UE) 2017/745, należy nadal stosować art. 16 ust. 2 tego rozporządzenia stanowiący, 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 odpowiedzialności w całym łańcuchu wartości AI, dostawcy takich systemów, niezależnie od tego, czy ich mogą być one wykorzystywane jako systemy AI wysokiego ryzyka przez innych dostawców czy jako elementy systemów AI wysokiego ryzyka, powinni ściśle współpracować – o ile niniejsze rozporządzenie nie stanowi inaczej – z dostawcami odpowiednich systemów AI wysokiego ryzyka, aby umożliwić im spełnianie odpowiednich obowiązków ustanowionych w niniejszym rozporządzeniu, 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 zostać zmieniony w system 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 spełnienia obowiązków ustanowionych 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 związanym z bezpieczeństwem elementem produktu, który wchodzi w zakres stosowania 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 tego prawodawstwa – powinien spełniać obowiązki dostawcy ustanowione w niniejszym rozporządzeniu, a w szczególności zapewnić zgodność systemu AI wbudowanego w produkt końcowy z wymogami niniejszego rozporządzenia.

(88) W całym łańcuchu 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, retrenowania 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 na podstawie pisemnej umowy niezbędne informacje, zdolności, dostęp techniczny i inną pomoc w oparciu o powszechnie uznany stan wiedzy technicznej, aby umożliwić dostawcy pełne spełnienie obowiązków ustanowionych 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 powinny być zobowiązane do zapewnienia zgodności z wymogami dotyczącymi odpowiedzialności w całym łańcuchu wartości AI, w szczególności wobec dostawcy, który je wykorzystał lub zintegrował, jeżeli te narzędzia, usługi, procesy lub elementy AI są udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania. Należy zachęcać twórców narzędzi, usług, procesów lub elementów AI, innych niż modele AI ogólnego przeznaczenia, które są udostępniane na bezpłatnej licencji otwartego oprogramowania, 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 wzorcowe 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 w całym łańcuchu wartości. Przy opracowywaniu dobrowolnych wzorcowych postanowień umownych, Komisja powinna też brać pod uwagę wymogi umowne, które mogą mieć zastosowanie w szczególnych 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. Podmioty stosujące 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 powinny zapewnić, aby osoby wyznaczone do stosowania instrukcji obsługi i sprawowania 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 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 prawa Unii o prawa krajowego oraz unijnej lub krajowej praktyki, w tym dyrektywy 2002/14/WE Parlamentu Europejskiego i Rady ([39]), 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.

(93) Ryzyko związane z systemami AI może wynikać ze sposobu zaprojektowania takich systemów, jak również ze sposobu ich wykorzystania. Podmioty stosujące systemy AI wysokiego ryzyka odgrywają zatem kluczową rolę w zapewnianiu ochrony praw podstawowych w uzupełnieniu obowiązków dostawcy podczas rozwoju systemu AI. Podmioty stosujące najlepiej rozumieją, jak konkretnie wykorzystywany będzie system AI wysokiego ryzyka, i mogą w związku z tym zidentyfikować potencjalne znaczące ryzyko, które nie zostało przewidziane na etapie rozwoju, dzięki bardziej precyzyjnej wiedzy na temat kontekstu wykorzystania, 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 jest w stosunku do nich wykorzystywany system AI wysokiego ryzyka. Taka informacja powinna obejmować przeznaczenie systemu i typ podejmowanych przez niego decyzji. Podmiot stosujący informuje również osoby fizyczne o przysługujących im prawie do uzyskania wyjaśnienia, które przewiduje niniejsze rozporządzenie. W odniesieniu do systemów AI wysokiego ryzyka wykorzystywanych do celów ścigania przestępstw obowiązek ten należy wykonywać 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 konieczne, z zastrzeżeniem odpowiednich zabezpieczeń w zakresie 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 powinno podlegać zabezpieczeniom. Systemy identyfikacji biometrycznej *post factum* powinny być zawsze wykorzystywane w sposób proporcjonalny, zgodny z prawem i jeżeli jest to bezwzględnie konieczne, a tym samym ukierunkowane na osoby fizyczne, 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 niezróżnicowanego nadzoru. 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 podmioty stosujące 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 dla praw podstawowych. Usługi o charakterze publicznym ważne dla osób fizycznych mogą być również świadczone przez podmioty prywatne. Podmioty prywatne świadczące takie usługi publiczne działają w powiązaniu z zadaniami świadczonymi w interesie publicznym, takimi jak edukacja, opieka zdrowotna, usługi społeczne, mieszkalnictwo, sprawowanie wymiaru sprawiedliwości. Celem oceny skutków dla praw podstawowych jest zidentyfikowanie przez podmiot stosujący konkretnych rodzajów ryzyka dla praw osób fizycznych lub grup osób fizycznych, na które AI może mieć wpływ, oraz określenie środków, które należy podjąć w przypadku

([39]) 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 (Dz.U. L 80 z 23.3.2002, s. 29).

urzeczywistnienia się tego ryzyka. Ocena skutków powinna być przeprowadzana przed wdrożeniem systemu AI wysokiego ryzyka i powinna być aktualizowana, gdy podmiot stosujący uzna, że którykolwiek z istotnych czynników uległ zmianie. W ocenie skutków należy określić odpowiednie procesy podmiotu stosującego, 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 wykorzystania, a także opis konkretnych kategorii osób fizycznych i grup, na które AI może mieć wpływ w tym konkretnym kontekście wykorzystania. Ocena powinna również obejmować określenie szczególnego ryzyka szkody, które może mieć wpływ na prawa podstawowe tych osób lub grup. Przeprowadzając tę ocenę, podmiot stosujący 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 powinny określić środki, które należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym na przykład rozwiązania dotyczące zarządzania w tym konkretnym kontekście wykorzystania, 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 wykorzystania. Po przeprowadzeniu tej oceny skutków podmiot stosujący powinien powiadomić odpowiedni 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 (zwany dalej „Urzędem ds. AI") powinien opracować wzór kwestionariusza, by ułatwić zapewnienie zgodności przez podmioty stosujące i zmniejszyć obciążenia administracyjne dla tych podmiotów.

(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 zmieniane 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 szczególne dotyczące modeli AI ogólnego przeznaczenia oraz modeli AI ogólnego przeznaczenia, które stwarzają ryzyko systemowe, a przepisy te powinny być stosowane 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 ustanowione w niniejszym rozporządzeniu obowiązki dotyczące modeli powinny nadal mieć zastosowanie obok obowiązków dotyczących systemów AI. Obowiązki ustanowione 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 ustanowionym w niniejszym rozporządzeniu. 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 zapewnienia zgodności z niniejszym rozporządzeniem w przypadku wprowadzenia do obrotu danego modelu w następstwie takiej działalności.

(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 w całym łańcuchu wartości AI, ponieważ modele, które dostarczają, mogą stanowić podstawę szeregu systemów niższego szczebla, często dostarczanych 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 spełniać obowiązki ustanowione w niniejszym rozporządzeniu lub innych przepisach. 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 wykorzystania przez dostawców niższego szczebla. Dostawca modelu AI ogólnego przeznaczenia powinien przygotować i aktualizować dokumentację techniczną w celu udostępnienia jej na wniosek Urzędowi ds. AI i właściwym organom krajowym. Minimalny zbiór elementów do uwzględnienia w takiej dokumentacji należy określić w szczególnych 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, udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania, która umożliwia ich ogólne upowszechnianie i zezwala użytkownikom na swobodny dostęp do nich, ich wykorzystywanie, zmianę i ich redystrybucję lub ich zmienionych 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 licencji otwartego oprogramowania 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 licencję otwartego oprogramowania 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) Elementy AI na bezpłatnej licencji otwartego oprogramowania obejmują oprogramowanie i dane, w tym modele i modele AI ogólnego przeznaczenia, narzędzia, usługi lub procesy systemu AI. Elementy AI na bezpłatnej licencji otwartego oprogramowania mogą być dostarczane za pośrednictwem różnych kanałów, w tym rozwijane 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, w tym 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 licencji otwartego oprogramowania 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 fakt, że model jest przejrzysty i że towarzyszy mu licencja otwartego oprogramowania, nie powinien być uznawany za wystarczający powód zwolnienia ze spełnienia obowiązków ustanowionych w niniejszym rozporządzeniu. W każdym razie, biorąc pod uwagę, że udostępnianie modeli AI ogólnego przeznaczenia na podstawie bezpłatnej licencji otwartego oprogramowania niekoniecznie prowadzi do ujawnienia istotnych informacji na temat zbioru danych wykorzystywanego do trenowania lub dostrajania modelu oraz na temat sposobu zapewnienia tym samym zgodności z prawem autorskim, przewidziane w odniesieniu do modeli AI ogólnego przeznaczenia zwolnienie z obowiązku spełnienia wymogów związanych z przejrzystością nie powinno dotyczyć obowiązku sporządzenia streszczenia dotyczącego treści wykorzystywanych do trenowania modeli oraz obowiązku wprowadzenia polityki w celu zapewnienie zgodności 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 ([40]).

(105) Modele AI ogólnego przeznaczenia, w szczególności duże generatywne modele AI, 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. Rozwój 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

([40]) 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).

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, aby ustanowione w niniejszym rozporządzeniu odpowiednie obowiązki zostały spełnione. W tym celu dostawcy modeli AI ogólnego przeznaczenia powinni wprowadzić politykę w celu zapewnienia zgodności z prawem Unii dotyczącym prawa autorskiego i praw pokrewnych, w szczególności w celu identyfikacji i zastosowania się do zastrzeżenia praw wyrażonego 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 spełniać ten obowiązek, 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 Unii poprzez stosowanie niższych standardów praw autorskich niż normy przewidziane w Unii.

(107) W celu zwiększenia przejrzystości dotyczącej danych wykorzystywanych do pretrenowania 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 AI 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 uzasadniony interes, w tym posiadaczom praw autorskich, wykonywanie i egzekwowanie ich 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 zapewnić 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 spełnił obowiązki nałożone na dostawców modeli AI ogólnego przeznaczenia dotyczące wprowadzenia polityki w celu zapewnienia 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 zgodności z prawami autorskimi 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) Spełnianie obowiązków mających zastosowanie do dostawców modeli AI ogólnego przeznaczenia powinno być współmierne i proporcjonalne do rodzaju dostawcy modeli, z wyłączeniem konieczności ich spełnienia przez osoby, które rozwijają 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 spełnianie tych obowiązków powinno odbywać się przy należytym uwzględnieniu wielkości dostawcy i umożliwiać uproszczone sposoby spełnienia tych obowiązków przez MŚP, w tym przedsiębiorstwa typu start-up, które nie powinny wiązać się z nadmiernymi kosztami i zniechęcać do korzystania z takich modeli. W przypadku zmiany lub dostrajania modelu obowiązki dostawców modeli AI ogólnego przeznaczenia powinny być ograniczone do tej zmiany lub dostrajania modelu, na przykład poprzez uzupełnienie już istniejącej dokumentacji technicznej o informacje na temat zmiany, w tym nowych źródeł danych treningowych, w celu spełnienia 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 racjonalnie przewidywalne negatywne skutki poważnych awarii, zakłóceń w sektorach krytycznych oraz poważne konsekwencje dla zdrowia i bezpieczeństwa publicznego; wszelkie rzeczywiste lub racjonalnie przewidywalne 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, bezstronności i bezpieczeństwa modelu, poziomu jego autonomii, dostępu do narzędzi, stosowania nowatorskich lub połączonych metod, strategii udostępniania i dystrybucji, możliwości w zakresie usuwania zabezpieczeń i innych czynników. W szczególności podejścia międzynarodowe wskazywały jak dotąd na potrzebę zwrócenia uwagi na ryzyko wynikające z potencjalnego umyślnego niewłaściwego wykorzystania lub niezamierzonych problemów z kontrolą związanych z dostosowaniem się do zamiaru człowieka; ryzyko 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 osobom fizycznym, 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, na całą działalność w danym obszarze lub na 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 technicznych i metodologii, 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 wprowadzeniu do obrotu lub w momencie, w którym podmioty stosujące wchodzą 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 mierzona w operacjach zmiennoprzecinkowych. Łączna 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 pretrenowanie, generowanie danych syntetycznych i dostrajanie. W związku z tym należy określić próg minimalny operacjach zmiennoprzecinkowych, który, jeżeli zostanie spełniony przez model AI ogólnego przeznaczenia, stwarza domniemanie, 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 one uwzględniać sposób, w jaki model zostanie wprowadzony do obrotu lub liczbę użytkowników, na które model ten może mieć wpływ. Aby uzupełnić ten system, 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, na które wskazuje ustalony próg. Decyzję tę należy podjąć na podstawie ogólnej oceny kryteriów do celów uznawania modelu AI ogólnego przeznaczenia za model 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, poziom 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. W przypadku modelu AI ogólnego przeznaczenia, który osiąga mający zastosowanie próg dotyczący zdolności dużego oddziaływania, należy domniemywać, że jest on modelem 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 domniemania. Jest to szczególnie istotne w odniesieniu do progu dotyczącego operacji zmiennoprzecinkowych, 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 powiadomienia 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. Powiadomienia 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 spełnienia obowiązków ustanowionych w niniejszym rozporządzeniu może być trudniejsze po udostępnieniu modelu na zasadach otwartego oprogramowania.

(113) Jeżeli Komisja dowie się o tym, że model AI ogólnego przeznaczenia spełnia kryteria, by zostać zaklasyfikowany jako model AI o ogólnym przeznaczeniu z ryzykiem systemowym, czego wcześniej nie było wiadomo lub w przypadku gdy odpowiedni 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 system, 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 w całym łańcuchu wartości AI.

(115) Dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym powinni oceniać i ograniczać 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 przeciwdziałania temu ryzyku, w wyniku rozwoju lub wykorzystania 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 strategii 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 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 AI 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 właściwemu spełnianiu obowiązków przewidzianych w niniejszym rozporządzeniu w odniesieniu do dostawców modeli AI ogólnego przeznaczenia. Dostawcy powinni móc polegać na kodeksach praktyk w celu wykazania spełnienia tych obowiązków. 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, zgodność z europejską normą zharmonizowaną powinna 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 AI 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 uregulowanych rozporządzeniem (UE) 2022/2065. 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 ustanowione w niniejszym rozporządzeniu 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 nadużycia. Dostawcy ci są również zobowiązani podjąć odpowiednie środki ograniczające to ryzyko z poszanowaniem praw podstawowych.

(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 dostarczane 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 wygenerowane 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 faktycznych lub przewidywalnych negatywnych skutków dla procesów demokratycznych, dyskursu obywatelskiego i procesów wyborczych, 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 ([41]), które z założenia mają odzwierciedlać stan wiedzy technicznej, powinna stanowić dla dostawców sposób wykazania zgodności z wymogami niniejszego rozporządzenia. Przy opracowywaniu norm należy zatem zachęcać do zrównoważonej reprezentacji interesów 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. 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

([41]) 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).

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 zasadnym jest przyjęcie domniemania, 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 (UE) 2019/881 należy przyjąć domniemanie, 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*, są zgodne z wymogiem cyberbezpieczeństwa określonym 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.

(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 odpowiedniej procedury oceny zgodności w przypadku 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 te, które są 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 wskazujące na 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 te, które są powiązane z produktami objętymi zakresem stosowania odpowiedniego obowiązującego unijnego prawodawstwa harmonizacyjnego, a także dostawców, którzy uznają, że w związku z odstępstwem system AI wymieniony w wykazie przypadków wykorzystania stanowiących wysokie ryzyko zamieszczonym 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 bazie danych UE, która zostanie utworzona i będzie zarządzana przez Komisję. Przed wykorzystaniem systemu AI wymienionego w wykazie przypadków wykorzystania stanowiących wysokie ryzyko zamieszczonym w załączniku do niniejszego rozporządzenia będące publicznymi organami, agencjami lub jednostkami organizacyjnymi podmioty stosujące systemy AI wysokiego ryzyka powinny dokonać swojej rejestracji w tej bazie danych i wybrać system, który zamierzają wykorzystywać. Inne podmioty stosujące powinny być uprawnione do uczynienia tego dobrowolnie. Ta sekcja bazy danych UE powinna być publicznie dostępna, nieodpłatna, informacje powinny być łatwe do odnalezienia, zrozumiałe i nadające się do odczytu maszynowego. Ta baza danych UE 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 przedkładanych przy rejestracji systemów AI wysokiego ryzyka, oraz informacji na temat przypadków wykorzystywania systemów AI wysokiego ryzyka, określonych w załączniku do niniejszego rozporządzenia, któremu odpowiadają poszczególne systemy AI wysokiego ryzyka. W unijnej bazie danych UE 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 bazy danych UE. Systemy AI wysokiego ryzyka w obszarze infrastruktury krytycznej powinny być rejestrowane wyłącznie na poziomie krajowym. Komisja powinna być administratorem bazy danych UE zgodnie z rozporządzeniem (UE) 2018/1725. Aby zapewnić pełną funkcjonalność bazy danych UE po jej wdrożeniu, procedura ustanawiania bazy danych powinna obejmować rozwijanie przez Komisję specyfikacji funkcjonalnych oraz sprawozdanie z niezależnego audytu. Wykonując swoje zadania jako administrator danych bazy danych UE, Komisja powinna wziąć pod uwagę ryzyko dotyczące cyberbezpieczeństwa. Aby zmaksymalizować dostępność i wykorzystywanie bazy danych UE przez społeczeństwo, baza danych UE, 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 wprowadzania w błąd, niezależnie od tego, czy kwalifikują się jako systemy wysokiego ryzyka, czy też nie. W pewnych okolicznościach wykorzystanie 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 powiadamiane o tym, że wchodzą w 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 spełnianiu takiego obowiązku należy uwzględniać cechy osób fizycznych należących do grup 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 AI, 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 spełnianiu 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 AI lub na poziomie modelu AI, w tym modeli AI ogólnego przeznaczenia generujących treści, a tym samym ułatwiać spełnianie 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 danych wejściowych ani ich semantyki.

(134) Oprócz rozwiązań technicznych wykorzystywanych przez dostawców systemu AI, podmioty stosujące, które wykorzystują system AI do generowania obrazów, treści dźwiękowych lub wideo lub manipulowania nimi, tak by łudząco przypominały istniejące osoby, przedmioty. Miejsca, podmioty lub wydarzenia i które to treści mogą niesłusznie zostać uznane przez odbiorcę za autentyczne lub prawdziwe („deepfake"), powinny również jasno i wyraźnie ujawnić – poprzez odpowiednie oznakowanie wyniku AI i ujawnienie, że źródłem jest AI – że treści te zostały sztucznie wygenerowane lub zmanipulowane. Spełnienie obowiązku w zakresie przejrzystości nie powinno być interpretowane jako wskazujące na to, że wykorzystanie systemu AI 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 fikcyjny lub analogiczny, z zastrzeżeniem odpowiednich zabezpieczeń w zakresie praw 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 wygenerowanych lub zmanipulowanych treści w odpowiedni sposób, który nie utrudnia wyświetlania utworu lub korzystania z niego, 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 wygenerowanego przez AI lub zmanipulowanego przez AI w zakresie, w jakim jest on publikowany w celu informowania opinii publicznej o sprawach leżących w interesie publicznym, chyba że treści wygenerowane przez AI zostały poddane procesowi weryfikacji przez człowieka lub kontroli redakcyjnej, a osoba fizyczna lub prawna ponosi odpowiedzialność redakcyjną za publikację treści.

(135) 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 treści, które zostały sztucznie wygenerowane lub zmanipulowane, w tym aby wspierać praktyczne rozwiązania dotyczące udostępniania, stosownie do przypadku, mechanizmów wykrywania i ułatwiania współpracy z innymi podmiotami w całym łańcuchu wartości, które rozpowszechniają treści lub sprawdzają ich autentyczność i pochodzenie, aby umożliwić ogółowi społeczeństwa skuteczne rozróżnianie treści wygenerowanych 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 wygenerowane 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 faktycznych lub przewidywalnych negatywnych skutków dla procesów demokratycznych, dyskursu obywatelskiego i procesów wyborczych, w tym poprzez stosowanie dezinformacji. Wymóg oznakowania treści wygenerowanych 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) Spełnienie obowiązków w zakresie przejrzystości w odniesieniu do systemów AI objętych niniejszym rozporządzeniem nie powinno być interpretowane jako wskazanie, że wykorzystanie systemu AI 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 systemy AI.

(138) AI jest szybko rozwijającą się grupą technologii, wymagającą nadzoru regulacyjnego oraz bezpiecznej i kontrolowanej przestrzeni do przeprowadzania doświadczeń, przy jednoczesnym zapewnieniu odpowiedzialnej innowacji oraz uwzględnieniu odpowiednich zabezpieczeń i środków ograniczających 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 poziomie 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 spełnić 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 w zakresie AI mogą być tworzone w formie fizycznej, cyfrowej lub hybrydowej i mogą obejmować zarówno produkty fizyczne, jak i cyfrowe. Organy ustanawiające piaskownice regulacyjne w zakresie AI 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 odpowiednimi przepisami prawa Unii i prawa krajowego. Ponadto piaskownice regulacyjne w zakresie AI powinny mieć na celu 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 w zakresie AI 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 i 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 rozwój, 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 znaczącego ryzyka na etapie rozwoju i testowania takich systemów AI powinno powodować konieczność właściwego ograniczenia tego ryzyka, a w przypadku niepowodzenia w tym zakresie – skutkować zawieszeniem procesu rozwoju 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 badawczo-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 w zakresie AI 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 ustanawianie innych piaskownic mających na celu zapewnienie zgodności z przepisami prawa innymi niż niniejsze rozporządzenie. W stosownych przypadkach odpowiednie właściwe organy odpowiedzialne za 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 rozwoju – 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 w zakresie AI 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 znaczącego ryzyka dla bezpieczeństwa, zdrowia i praw podstawowych, jakie może powstać w trakcie rozwoju produktów oraz prowadzenia działań testowych i doświadczalnych w ramach takiej piaskownicy regulacyjnej.

(141) Aby przyspieszyć proces rozwoju 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 osób fizycznych, należy zapewnić, by niniejsze rozporządzenie wprowadzało odpowiednie i wystarczające zabezpieczenia i warunki dotyczące dostawców lub potencjalnych dostawców. Takie zabezpieczenia 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 o ochronie 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 bazy danych UE (z pewnymi ograniczonymi wyjątkami), ustalenia ograniczeń co do okresu, w jakim można przeprowadzać testy, oraz wymagania dodatkowych zabezpieczeń w odniesieniu do osób należących do grup szczególnie wrażliwych, a także pisemnej umowy określającej role i obowiązki potencjalnych dostawców i podmiotów stosujących 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 systemu 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 prawa Unii 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 ([42]) i (UE) 2023/2854 ([43]).

(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 powinny zapewniać 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 powinny korzystać z istniejących kanałów komunikacji, a w stosownych przypadkach utworzyć nowy specjalny kanał komunikacji z MŚP, w tym przedsiębiorstwami typu start-up, podmiotami stosującymi, 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 wykonywania niniejszego rozporządzenia. W stosownych przypadkach kanały powinny ze sobą współpracować, by uzyskać synergię i zapewnić spójność wskazówek dla MŚP, w tym przedsiębiorstw typu start-up, i podmiotów stosujących. Dodatkowo państwa członkowskie powinny ułatwiać udział MŚP i innych odpowiednich zainteresowanych stron w procesie opracowywania norm. Ponadto przy ustalaniu przez jednostki notyfikowane

([42]) 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).

([43]) 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).

wysokości opłat z tytułu oceny zgodności należy uwzględnić szczególne interesy i potrzeby dostawców, którzy są MŚP, w tym przedsiębiorstwami typu start-up. Komisja powinna regularnie oceniać koszty certyfikacji i zapewnienia zgodności ponoszone przez MŚP, w tym przedsiębiorstwa typu start-up, w drodze przejrzystych konsultacji 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 prowadzonej przez odpowiednich dostawców oraz komunikacji z operatorami był język powszechnie rozumiany przez możliwie największą liczbę podmiotów stosujących w wymiarze transgranicznym. Aby zaspokoić szczególne potrzeby MŚP, w tym przedsiębiorstw typu start-up, Komisja powinna na wniosek Rady ds. AI zapewnić ujednolicone wzory w obszarach 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, 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. Średnie przedsiębiorstwa, które do niedawna kwalifikowały się jako małe przedsiębiorstwa w rozumieniu załącznika do zalecenia Komisji 2003/361/WE ([44]), 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 zapewnienia zgodności z niniejszym rozporządzeniem.

(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 poziomie Unii lub poziomie krajowym.

(145) Aby zminimalizować zagrożenia dla wdrożenia wynikające z braku wiedzy o rynku i jego znajomości, a także aby ułatwić dostawcom, w szczególności MŚP, w tym przedsiębiorstwom typu start-up, i jednostkom notyfikowanym spełnianie 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 poziomie Unii lub poziomie krajowym powinny przyczyniać się do wykonywania 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 spełnienie jednego z najbardziej kosztownych obowiązków, a mianowicie ustanowienia systemu zarządzania jakością, w sposób uproszczony, 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 poziomie krajowym, a także budowanie zdolności na poziomie Unii 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 poziomie Unii. Misją Urzędu ds. AI, który został ustanowiony decyzją Komisji ([45]), 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 w wykonywanie niniejszego rozporządzenia na poziomie Unii i poziomie krajowym. Rozwój unijnej wiedzy

([44]) 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).

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

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 poziomie Unii oraz synergię z powiązanymi inicjatywami na poziomie Unii, takimi jak Wspólne Przedsięwzięcie EuroHPC i ośrodki testowo-doświadczalne w dziedzinie AI w ramach programu „Cyfrowa Europa".

(149) Aby ułatwić sprawne, skuteczne i zharmonizowane wykonywanie 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 wykonywaniem 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 swobodę w zakresie wyznaczania 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 poziomie 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 przywołanego 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 przepisów prawa Unii dotyczących danych oraz produktów i usług cyfrowych.

(150) Aby zapewnić zaangażowanie zainteresowanych stron we wdrażanie i stosowanie niniejszego rozporządzenia, należy ustanowić forum doradcze, które ma 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, 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 w odniesieniu do systemów AI i wzmocnić zdolności państw członkowskich, należy ustanowić unijne struktury wsparcia 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 wykonywaniem 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 poziomie państw członkowskich i na poziomie Unii, 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 wykonywanie 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, które są organami ścigania. System ten ma również zasadnicze znaczenie dla zapewnienia skuteczniejszego i terminowego przeciwdziałania możliwym pojawiającym się ryzykom 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 wdrożenia systemu zgłaszania odpowiednim organom wszelkich poważnych incydentów zaistniałych w związku z wykorzystaniem 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 działaniu, naruszeń obowiązków ustanowionych w prawie Unii, których celem jest ochrona 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 wymogów i obowiązków ustanowione w niniejszym rozporządzeniu 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 podejmować 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 szczególną procedurę ochronną, 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 prawa 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 tymi aktami prawnymi i ich egzekwowania, w szczególności właściwe organy zdefiniowane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 575/2013 ([46]) oraz dyrektywach Parlamentu Europejskiego i Rady 2008/48/WE ([47]),

([46]) 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).

([47]) 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).

2009/138/WE ([48]), 2013/36/UE ([49]), 2014/17/UE ([50]) i (UE) 2016/97 ([51]), należy wyznaczyć w ramach ich odpowiednich kompetencji jako właściwe organy do celów nadzoru nad wykonywaniem niniejszego rozporządzenia, w tym do celów działań w zakresie nadzoru 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. Te właściwe organy powinny mieć wszystkie uprawnienia wynikające z niniejszego rozporządzenia i rozporządzenia (UE) 2019/1020 w celu egzekwowania wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, 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 przepisów prawa Unii dotyczących usług finansowych. Należy przewidzieć, że – działając w charakterze organów nadzoru rynku na podstawie niniejszego rozporządzenia –krajowe organy odpowiedzialne za nadzór nad instytucjami kredytowymi uregulowanymi w dyrektywie 2013/36/UE, które uczestniczą w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem Rady (UE) nr 1024/2013 ([52]), powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zidentyfikowane w trakcie prowadzonych przez siebie działań w zakresie nadzoru rynku, które potencjalnie mogą mieć znaczenie dla Europejskiego Banku Centralnego z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego. Aby dodatkowo zwiększyć spójność między niniejszym rozporządzeniem a przepisami mającymi zastosowanie do instytucji kredytowych uregulowanych w dyrektywie 2013/36/UE, niektóre obowiązki proceduralne dostawców związane z zarządzaniem ryzykiem, monitorowaniem po wprowadzeniu do obrotu oraz prowadzeniem dokumentacji 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 uregulowanych w dyrektywie 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 systemu zarządzania wewnętrznego, uzgodnień lub procedur ustanowionych zgodnie z odpowiednimi przepisami prawa Unii 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 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 odpowiedzialności i kompetencji na poziomie Unii i poziomie 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

([48]) 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).

([49]) 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).

([50]) 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).

([51]) 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).

([52]) 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).

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 do co najmniej jednego celu zaklasyfikowanego 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. Urząd ds. AI powinien mieć możliwość prowadzenia wszelkich niezbędnych działań w celu monitorowania skutecznego wykonywania 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 celu wsparcia skutecznego monitorowania Urząd ds. AI powinien ustanowić możliwość składania przez dostawców niższego szczebla skarg na dostawców modeli i systemów AI ogólnego przeznaczenia 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, aby wystąpiła do dostawcy z wnioskiem o przedstawienie dokumentacji lub informacji.

(164) Urząd ds. AI powinien mieć możliwość podejmowania niezbędnych działań w celu monitorowania skutecznego wdrażania i spełniania 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 przeprowadzania ocen w jego imieniu. Spełnienie 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 z użytku. 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 szczególnych praw proceduralnych przewidzianych w niniejszym rozporządzeniu.

(165) Rozwój systemów AI innych niż systemy AI wysokiego ryzyka zgodnie z wymogami 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, zarówno wysokiego ryzyka, jak i nie stanowiących wysokiego ryzyka, 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 rozwoju 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 rozwoju systemów AI oraz dotyczących różnorodności zespołów programistycznych, w tym pod względem równowagi płci. W celu zapewnienia skuteczności dobrowolnych kodeksów postępowania, powinny się one 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 powiązane z produktami, które nie są systemami wysokiego ryzyka w rozumieniu niniejszego rozporządzenia, a zatem nie muszą być zgodne z wymogami ustanowionymi w przypadku 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 ([53]) miałoby zastosowanie jako rozwiązanie zapasowe.

(167) W celu zapewnienia opartej na zaufaniu i konstruktywnej współpracy właściwych organów na poziomie Unii i poziomie krajowym wszystkie strony uczestniczące w stosowaniu niniejszego rozporządzenia powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań, zgodnie z prawem Unii lub prawem 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 wykonywanie niniejszego rozporządzenia, interesy bezpieczeństwa publicznego i narodowego, integralność postępowań karnych i administracyjnych oraz integralność informacji niejawnych.

(168) Zgodność z niniejszym rozporządzeniem powinna być możliwa do wyegzekwowania poprzez nakładanie kar i innych środków egzekwowania prawa. Państwa członkowskie powinny podjąć wszelkie niezbędne środki, aby zapewnić wdrożenie przepisów niniejszego rozporządzenia, w tym poprzez ustanowienie skutecznych, proporcjonalnych i odstraszających kar za ich naruszenie, oraz poszanowanie 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) Spełnienie obowiązków spoczywających na dostawcach modeli AI ogólnego przeznaczenia nałożonych na mocy niniejszego rozporządzenia powinna być możliwa do wyegzekwowania między innymi 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, w tym nieograniczonemu prawu orzekania zgodnie z art. 261 TFUE.

(170) W przepisach prawa Unii i prawa krajowego 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 uważać, że doszło do naruszenia niniejszego rozporządzenia, powinna być uprawniona do wniesienia skargi do odpowiedniego organu nadzoru rynku.

(171) Osoby, na które AI ma wpływ, powinny mieć prawo do uzyskania wyjaśnienia, jeżeli decyzja podmiotu stosującego opiera się głównie na wynikach określonych systemów AI wysokiego ryzyka objętych zakresem stosowania niniejszego rozporządzenia i jeżeli decyzja ta wywołuje skutki prawne lub podobnie znacząco oddziałuje na te

([53]) 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).

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, na które AI ma wpływ, podstawę do korzystania z ich praw. Prawo do uzyskania wyjaśnienia nie powinno mieć zastosowania do wykorzystania systemów AI, co do których na mocy przepisów praw Unii lub prawa krajowego obowiązują wyjątki lub ograniczenia, i powinno mieć zastosowanie wyłącznie w zakresie, w jakim prawo to nie jest jeszcze przewidziane w przepisach prawa 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 takich naruszeń powinno zatem stosować się dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937 ([54]).

(173) Aby zapewnić możliwość dostosowania w razie potrzeby ram regulacyjnych, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu zmiany warunków, na podstawie których systemu AI nie uznaje się 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 ([55]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach 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.

(174) Z uwagi na szybki rozwój technologiczny i wiedzę techniczną wymaganą do skutecznego stosowania niniejszego rozporządzenia, Komisja powinna dokonać oceny i przeglądu niniejszego rozporządzenia do dnia 2 sierpnia 2029 r., 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 do dnia 2 sierpnia 2028 r., a następnie co cztery lata, Komisja powinna ocenić, czy należy wprowadzić zmiany w wykazie nagłówków dotyczących obszarów wysokiego ryzyka zawartym w załączniku do niniejszego rozporządzenia, zmiany w zakresie 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 2 sierpnia 2028 r., a następnie co trzy lata, Komisja powinna oceniać wpływ i skuteczność dobrowolnych kodeksów postępowania pod względem wspierania stosowania wymogów przewidzianych w przypadku systemów AI wysokiego ryzyka do systemów AI innych niż systemy AI wysokiego ryzyka oraz ewentualnie innych dodatkowych wymogów dotyczących takich systemów AI.

(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 ([56]).

(176) Ponieważ cel niniejszego rozporządzenia, a mianowicie poprawa funkcjonowania rynku wewnętrznego i promowanie upowszechniania zorientowanej 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

([54]) 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).
([55]) Dz.U. L 123 z 12.5.2016, s. 1.
([56]) 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).

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 tego celu.

(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 należy stosować 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 dotyczące ich projektu 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 zgodnie z niniejszym rozporządzeniem. 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 do dnia 2 sierpnia 2030 r.

(178) Dostawców systemów AI wysokiego ryzyka zachęca się, by już w okresie przejściowym przystąpili do dobrowolnego spełniania odpowiednich obowiązków ustanowionych w niniejszym rozporządzeniu.

(179) Niniejsze rozporządzenie należy stosować od dnia 2 sierpnia 2026 r. Biorąc jednak pod uwagę niedopuszczalne ryzyko związane z niektórymi sposobami wykorzystania AI, zakazy oraz przepisy ogólne niniejszego rozporządzenia należy stosować już od dnia 2 lutego 2025 r. 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 przed dniem 2 sierpnia 2026 r., w związku z czym przepisy dotyczące jednostek notyfikowanych oraz struktury zarządzania należy stosować od dnia 2 sierpnia 2025 r. Biorąc pod uwagę szybkie tempo postępu technologicznego i przyjęcie modeli AI ogólnego przeznaczenia, obowiązki dostawców modeli AI ogólnego przeznaczenia należy stosować od dnia 2 sierpnia 2025 r. Kodeksy praktyk powinny być gotowe do dnia 2 maja 2025 r., 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 przepisy dotyczące kar, w tym administracyjnych kar pieniężnych i powiadomić o nich Komisję oraz zapewnić ich właściwe i skuteczne wdrożenie przed dniem rozpoczęcia stosowania niniejszego rozporządzenia. Przepisy dotyczące kar należy zatem stosować od dnia 2 sierpnia 2025 r.

(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 zorientowanej na człowieka i godnej zaufania sztucznej inteligencji (AI), przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie, w tym demokracji, praworządności i ochrony środowiska, przed szkodliwymi skutkami systemów AI w Unii oraz wspieraniu 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, nadzoru rynku, zarządzania i egzekwowania;

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

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie stosuje się 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 wytworzone przez system AI są wykorzystywane w Unii;

d) importerów i dystrybutorów systemów AI;

e) producentów produktu, którzy pod własną nazwą lub znakiem towarowym oraz wraz ze swoim produktem wprowadzają do obrotu lub oddają do użytku system AI;

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 związanych z produktami, które są objęte unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I sekcja B, stosuje się wyłącznie art. 6 ust. 1, art. 102–109 i art. 112. Art. 57 stosuje się wyłącznie w zakresie, w jakim wymogi dotyczące systemów AI wysokiego ryzyka ustanowione w niniejszym rozporządzeniu zostały włączone do tego unijnego prawodawstwa harmonizacyjnego.

3. Niniejszego rozporządzenia nie stosuje się do obszarów wykraczających poza zakres stosowania prawa Unii i w żadnym wypadku nie wpływa ono na kompetencje państw członkowskich w zakresie bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu, któremu państwa członkowskie powierzyły wykonywanie zadań związanych z tymi kompetencjami.

Niniejszego rozporządzenia nie stosuje się do systemów AI, jeżeli – i w zakresie, w jakim – wprowadzono je do obrotu, oddano do użytku lub są one wykorzystywane, ze zmianami lub bez zmian, wyłącznie do celów wojskowych, obronnych lub do celów bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu prowadzącego te działania.

Niniejszego rozporządzenia nie stosuje się do systemów AI, które nie zostały 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. Niniejszego rozporządzenia nie stosuje się 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 osób fizycznych.

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

6. Niniejszego rozporządzenia nie stosuje się do systemów AI lub modeli AI, w tym ich wyników, rozwiniętych i oddanych do użytku wyłącznie do celów badań naukowych i rozwojowych.

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

8. Niniejszego rozporządzenia nie stosuje się do żadnej działalności badawczej, testowej ani rozwojowej dotyczącej systemów AI lub modeli AI przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku. Działalność tego rodzaju prowadzona jest zgodnie z mającym zastosowanie prawem Unii. Niniejsze wyłączenie nie obejmuje testów w warunkach rzeczywistych.

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

10. Niniejsze rozporządzenie nie stosuje się do obowiązków podmiotów stosujących 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. Niniejszego rozporządzenia nie stosuje się do systemów AI udostępnianych na podstawie bezpłatnych licencji otwartego oprogramowania, chyba że systemy te są wprowadzane do obrotu lub oddawane do użytku jako systemy AI wysokiego ryzyka lub jako system AI objęty art. 5 lub 50.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „system AI” oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych 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 jej dotkliwości;

3) „dostawca” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które rozwijają system AI lub model AI ogólnego przeznaczenia lub zlecają rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz które – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadzają do obrotu lub oddają do użytku system AI;

4) „podmiot stosujący” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które wykorzystują system AI, nad którym sprawują 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 przyjęła pisemne pełnomocnictwo od dostawcy systemu AI lub modelu AI ogólnego przeznaczenia do, odpowiednio, spełnienia 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 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 Unii;

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

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

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

11) „oddanie do użytku" oznacza dostarczenie systemu AI do pierwszego użycia bezpośrednio podmiotowi stosującemu 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) „związany z bezpieczeństwem element" oznacza element produktu lub systemu AI, który spełnia funkcję bezpieczeństwa w przypadku tego produktu lub systemu AI 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 o, w szczególności, 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 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 znajdującego się w łańcuchu dostaw;

18) „skuteczność działania systemu AI" oznacza zdolność systemu AI do działania 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 ustanowione w rozdziale III 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 notyfikowano zgodnie z niniejszym rozporządzeniem i innym stosownym unijnym prawodawstwem harmonizacyjnym;

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 która ma wpływ na zgodność systemu AI z wymogami ustanowionymi w rozdziale III 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 ustanowione w rozdziale III sekcja 2 i innych mających zastosowanie unijnych przepisach harmonizacyjnych, 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 wykorzystania 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 zbiór specyfikacji technicznych zgodnie z definicją w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012, zapewniający środki umożliwiające zgodność z niektórymi wymogami ustanowionymi w niniejszym rozporządzeniu;

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

30) „dane walidacyjne” oznaczają dane wykorzystywane do oceny trenowanego systemu AI oraz do dostrajania 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;

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 zautomatyzowane rozpoznawanie fizycznych, fizjologicznych, behawioralnych lub psychologicznych cech ludzkich w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z danymi biometrycznymi osób fizycznych przechowywanymi w bazie danych;

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

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 postępowań przygotowawczych w ich sprawie lub ich ścigania, których ujawnienie mogłoby zagrozić integralności postępowania karnego;

39) „system rozpoznawania emocji” oznacza system AI służący do identyfikacji lub wywnioskowania emocji lub zamiarów osób fizycznych na podstawie danych biometrycznych tych osób;

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, zwykle na odległość, poprzez porównanie danych biometrycznych danej osoby fizycznej 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 który obejmuje nie tylko natychmiastową identyfikację, ale także ograniczone krótkie opóźnienia w celu uniknięcia obchodzenia przepisów;

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 miejsce fizyczne, będące własnością prywatną lub 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) organ publiczny właściwy w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; lub

b) 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 wykonywania kar, 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 wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

47) „Urząd ds. AI” oznacza zadanie Komisji polegające na przyczynianiu się do wdrażania, monitorowania i nadzorowania systemów AI i modeli AI ogólnego przeznaczenia oraz zarządzania AI, określone w decyzji Komisji z dnia 24 stycznia 2024 r.; zawarte w niniejszym rozporządzeniu odesłania do Urzędu ds. AI odczytuje się jako odesłania do Komisji;

48) „właściwy organ krajowy” oznacza organ notyfikujący lub organ nadzoru rynku; w odniesieniu do systemów AI oddanych do użytku lub wykorzystywanych przez instytucje, organy i jednostki organizacyjne Unii, zawarte w niniejszym rozporządzeniu odesłania do właściwych organów krajowych i organów nadzoru rynku odczytuje się jako odesłania do Europejskiego Inspektora Ochrony Danych;

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 działaniu;

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

d) poważnej szkody na mieniu lub poważnej 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;

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 rozwoju, 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 i osobom, na które AI ma wpływ – z uwzględnieniem ich odnośnych praw i obowiązków w kontekście niniejszego rozporządzenia – w przemyślany sposób wdrażać systemy sztucznej inteligencji oraz mieć świadomość, jakie możliwości i ryzyka 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 spełnienia przez system AI z wymogów niniejszego rozporządzenia i które nie są kwalifikowane jako 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 przez AI lub zmanipulowane przez AI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe;

61) „powszechne naruszenie” oznacza działanie lub zaniechanie sprzeczne z prawem Unii chroniącym interesy osób fizycznych, które:

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

(i) działanie 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, jeżeli naruszenie zostało popełnione przez ten podmiot;

b) wyrządziło, wyrządza lub może wyrządzić szkodę zbiorowym interesom osób fizycznych i ma cechy wspólne, w tym dotyczy tej samej bezprawnej praktyki lub naruszenia tego samego interesu, oraz ma miejsce jednocześnie w co najmniej trzech państwach członkowskich, a jego sprawcą jest ten sam operator;

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 ten 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 dające się racjonalnie przewidzieć 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 to system może służyć różnym celom, nadający się zarówno do bezpośredniego wykorzystania, jak i do integracji z innymi systemami AI;

67) „operacja zmiennoprzecinkowa” oznacza 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, rozwiniętego w drodze integracji modelu AI, niezależnie od tego, czy ten model AI 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 systemy AI podejmują środki w celu zapewnienia, w możliwie największym stopniu, odpowiedniego poziomu kompetencji w zakresie AI wśród swojego personelu i innych osób zajmujących się działaniem i wykorzystaniem systemów AI w ich imieniu, z uwzględnieniem ich wiedzy technicznej, doświadczenia, wykształcenia i wyszkolenia oraz kontekstu, w którym systemy AI mają być wykorzystywane, a także biorąc pod uwagę osoby lub grupy osób, wobec których systemy AI mają być wykorzystywane.

ROZDZIAŁ II

ZAKAZANE PRAKTYKI

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 dokonanie znaczącej zmiany zachowania danej osoby lub grupy osób poprzez znaczące ograniczenie ich zdolności do podejmowania świadomych decyzji, powodując tym samym podjęcie przez nie decyzji, której inaczej by nie podjęły, w sposób, który wyrządza lub może wyrządzić u niej, u innej osoby lub u grupy osób poważną szkodę;

b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu AI, który wykorzystuje słabości osoby fizycznej lub określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną, którego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub osoby należącej do tej grupy w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić 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, wywnioskowanych lub przewidywanych cech osobistych lub cech osobowości, kiedy to scoring społeczny prowadzi do jednego lub obu z następujących skutków:

   (i) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub grup osób w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zebrano 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 ryzyko 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 udziału danej osoby w działalności przestępczej, 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 nieukierunkowane pozyskiwanie (ang. untargeted 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 światopoglądowych, seksualności lub orientacji seksualnej; zakaz ten nie obejmuje przypadków etykietowania ani filtrowania pozyskanych zgodnie z prawem 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 bezwzględnie konieczne 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, istotnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub rzeczywistemu i aktualnemu lub rzeczywistemu i dającemu się przewidzieć zagrożeniu atakiem terrorystycznym;

(iii) lokalizowania lub identyfikowania osoby podejrzanej o popełnienie przestępstwa w celu prowadzenia postępowania przygotowawczego lub ścigania lub wykonania kar w odniesieniu do przestępstw, o których mowa w załączniku II, podlegających w danym państwie członkowskim karze pozbawienia wolności lub środkowi 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 do celów ścigania przestępstw w odniesieniu do któregokolwiek z celów, o których mowa w ust. 1 akapit pierwszy lit. h), mogą być wykorzystywane do celów określonych w tej literze, jedynie w celu potwierdzenia tożsamości konkretnej poszukiwanej osoby, z uwzględnieniem przy tym następujących elementów:

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

b) konsekwencje wykorzystania takiego 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 do celów ścigania przestępstw w odniesieniu do któregokolwiek z celów, o których mowa w ust. 1 akapit pierwszy 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 dla praw podstawowych zgodnie z art. 27 oraz zarejestrował system w bazie danych UE zgodnie z przepisami art. 49. W należycie uzasadnionych nadzwyczajnych przypadkach można jednak rozpocząć korzystanie z takich systemów bez rejestracji w bazie danych UE, pod warunkiem że taka rejestracja zostanie dokonana bez zbędnej zwłoki.

3. Na potrzeby ust. 1 akapit pierwszy lit. h) i ust. 2, każde wykorzystanie systemu zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw wymaga uzyskania uprzedniego zezwolenia udzielonego przez organ wymiaru sprawiedliwości 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 pilnych 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 wstrzymuje się ze skutkiem natychmiastowym, a wszystkie dane, a także rezultaty i wyniki uzyskane podczas tego wykorzystania musza zostać natychmiast odrzucone i usunięte.

Właściwy organ wymiaru sprawiedliwości 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 akapit pierwszy 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 można wydać 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 prawa krajowego, o których mowa w ust. 5. Powiadomienie zawiera co najmniej informacje określone w ust. 6 i nie może zawierać 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 do celów ścigania przestępstw w granicach i na warunkach wymienionych w ust. 1 akapit pierwszy lit. h) i w ust. 2 i 3. Zainteresowane państwa członkowskie ustanawiają w swoim prawie krajowym niezbędne szczegółowe przepisy dotyczące wniosku o udzielenie zezwoleń, o których mowa w ust. 3, wydawanie i wykonywanie tych zezwoleń oraz ich nadzorowanie składanie sprawozdań w ich sprawie. W przepisach tych określa się również, w odniesieniu do których celów wymienionych w ust. 1 akapit pierwszy lit. h) – w tym w odniesieniu do których przestępstw wymienionych w ust. 1 akapit pierwszy lit. h) ppkt (iii) – właściwe organy mogą uzyskać zezwolenie na wykorzystanie tych 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 wykorzystania 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 wymiaru sprawiedliwości 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 mogą zawierać wrażliwych danych operacyjnych dotyczących powiązanych działań w zakresie ścigania przestępstw.

8. Niniejszy artykuł nie ma wpływu na zakazy mające zastosowanie w przypadku, gdy praktyka w zakresie 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 wykorzystania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I lub sam system AI jest takim produktem;

b) produkt, którego związanym z bezpieczeństwem elementem jest zgodnie z lit. a) system AI, lub sam system AI 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 oddaniem 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, o którym mowa w załączniku III, nie uznaje się za system wysokiego ryzyka, w przypadku gdy nie stwarza on znaczącego ryzyka szkody dla zdrowia, bezpieczeństwa lub praw podstawowych osób fizycznych, w tym poprzez brak znaczącego wpływu na wynik procesu decyzyjnego.

Akapit pierwszy stosuje się w przypadku, gdy spełniony jest którykolwiek z następujących warunków:

a) system AI jest przeznaczony do wykonywania wąsko określonego 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 zakończoną 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 wykorzystania 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 wniosek właściwych organów krajowych dostawca przedstawia dokumentację tej oceny.

5. Po konsultacji z Europejską Radą ds. Sztucznej Inteligencji (zwaną dalej „Radą ds. AI"), Komisja przedstawi nie później niż w dniu 2 lutego 2026 r. wytyczne określające praktyczne wdrożenie niniejszego artykułu zgodnie z art. 96 wraz z kompleksowym wykazem praktycznych przykładów przypadków wykorzystania systemów AI, które stanowią przypadki wykorzystania wysokiego ryzyka oraz które nie stanowią przypadków takiego wykorzystania.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 97 w celu zmiany akapitu drugiego ust. 3 niniejszego artykułu poprzez dodanie nowych warunków do warunków ustanowionych w tym przepisie lub ich zmianę, 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.

7. Komisja przyjmuje zgodnie z art 97 akty delegowane w celu zmiany akapitu drugiego ust. 3 niniejszego artykułu poprzez usunięcie któregokolwiek z warunków ustanowionych w tym przepisie, w przypadku gdy istnieją konkretne i wiarygodne dowody na to, że jest to konieczne w celu utrzymania poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych przewidzianego w niniejszym rozporządzeniu.

8. Zmiana warunków ustanowionych w ust. 3 akapit drugi, przyjęta zgodnie z ust. 6 i 7 niniejszego artykułu, nie może prowadzić do obniżenia ogólnego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych przewidzianego w niniejszym rozporządzeniu i musi zapewniać spójność z aktami delegowanymi przyjętymi zgodnie z art. 7 ust. 1 oraz uwzględniać rozwój rynku i technologii.

Artykuł 7

Zmiany w załączniku III

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 97 w celu zmiany załącznika III poprzez dodanie systemów AI wysokiego ryzyka lub zmianę przypadków ich wykorzystania, w przypadku gdy spełnione są oba poniższe warunki:

a) systemy AI są przeznaczone do wykorzystania 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 już wyrządziło szkodę dla zdrowia i bezpieczeństwa lub miało niepożądany wpływ na prawa podstawowe lub wzbudziło istotne obawy co do prawdopodobieństwa wystąpienia takiej szkody lub niepożądanego wpływu, czego potwierdzeniem są np. zgłoszenia lub poparte dokumentami twierdzenia przedstawione 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) rozmiary i prawdopodobieństwo korzyści płynących z wdrożenia 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 ochrony prawnej w związku z ryzykiem stwarzanym przez system AI, z wyłączeniem roszczeń o odszkodowanie;

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

3. Komisja jest uprawniona do przyjmowania zgodnie z art. 97 aktów delegowanych 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 żadnego znaczącego ryzyka dla praw podstawowych, zdrowia lub bezpieczeństwa, biorąc pod uwagę kryteria wymienione w ust. 2;

b) usunięcie 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 być zgodne z wymogami ustanowionymi w niniejszej sekcji, przy uwzględnieniu ich przeznaczenia oraz powszechnie uznanego stanu wiedzy technicznej w dziedzinie AI oraz technologii powiązanych z AI. 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 na podstawie mającego zastosowanie unijnego prawodawstwa harmonizacyjnego. Przy zapewnianiu zgodności systemów AI wysokiego ryzyka, o których mowa w ust. 1, z wymogami ustanowionymi 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 zapewniają 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 obsługuje system zarządzania ryzykiem w odniesieniu do systemów AI wysokiego ryzyka.

2. Przez system zarządzania ryzykiem rozumie się 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 podczas jego stosowania zgodnie z przeznaczeniem;

b) oszacowanie i ocenę ryzyka, jakie może wystąpić podczas wykorzystywania systemu AI wysokiego ryzyka zgodnie z 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. Ryzyko, o którym mowa w niniejszym artykule, oznacza tylko takie rodzaje ryzyka, które można stosownie ograniczyć lub wyeliminować poprzez rozwój 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 ustanowionych w niniejszej sekcji, w celu skuteczniejszego minimalizowania ryzyka przy jednoczesnym osiągnięciu odpowiedniej równowagi we wdrażaniu środków służących spełnieniu tych wymogów.

5. Środki zarządzania ryzykiem, o których mowa w ust. 2 lit. d), muszą być takie, aby odpowiednie 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 i rozwój systemu AI wysokiego ryzyka;

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.

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, 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 ustanowionymi 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 rozwoju 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 ze względu na przeznaczenie systemu AI wysokiego ryzyka.

9. Przy wdrażaniu systemu zarządzania ryzykiem przewidzianego w ust. 1–7 dostawcy zwracają uwagę na to, czy dany system AI wysokiego ryzyka w świetle swojego przeznaczenia może mieć niekorzystny wpływ na osoby poniżej 18 roku życia oraz, w stosownych przypadkach, na inne grupy szczególnie wrażliwe.

10. W odniesieniu do dostawców systemów AI wysokiego ryzyka, którzy podlegają wymogom dotyczącym wewnętrznych procesów zarządzania ryzykiem na podstawie innych odpowiednich przepisów 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 AI z wykorzystaniem danych, rozwija się na podstawie zbiorów danych treningowych, walidacyjnych i testowych spełniających kryteria jakości, o których mowa w ust. 2–5, w każdym przypadku gdy 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 zbierania danych i pochodzenia danych oraz, w przypadku danych osobowych, pierwotnego celu zbierania 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 zgodność z niniejszym rozporządzeniem, 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 wykorzystywany system AI wysokiego ryzyka.

5. W zakresie, w jakim jest to bezwzględnie konieczne 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 w zakresie podstawowych praw i wolności osób fizycznych. Oprócz przepisów określonych w rozporządzeniach (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywie (UE) 2016/680, aby takie przetwarzanie mogło się odbyć, przetwarzanie takie musi spełniać 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, zobowiązane do spełnienia odpowiednich obowiązków dotyczących poufności;

d) szczególne kategorie danych osobowych nie są przesyłane, przekazywane ani w inny sposób udostępniane innym podmiotom;

e) szczególne kategorie danych osobowych usuwa się po skorygowaniu stronniczości lub po upływie okresu przechowywania danych osobowych, w zależności od tego, co nastąpi 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 bezwzględnie konieczne do wykrycia i skorygowania stronniczości oraz dlaczego cel ten nie mógł zostać osiągnięty w wyniku przetwarzania innych danych.

6. W przypadkach rozwoju 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 jest zgodny z wymogami ustanowionymi 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 wzór uproszczonej 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 wzoru, o którym mowa w niniejszym ustępie. Jednostki notyfikowane akceptują ten wzór do celów oceny zgodności.

2. W przypadku wprowadzania do obrotu lub oddawania do użytku systemu AI wysokiego ryzyka związanego z produktem, który jest objęty zakresem stosowania unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A, sporządza się jeden zestaw dokumentacji technicznych zawierający wszystkie informacje określone w ust. 1, jak również informacje wymagane na podstawie tych aktów prawnych.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 97 w celu zmiany, w razie potrzeby, załącznika IV, aby zagwarantować, by w świetle postępu technicznego dokumentacja techniczna zawierała wszystkie informacje niezbędne do oceny zgodności systemu z wymogami ustanowionymi w niniejszej sekcji.

Artykuł 12

Rejestrowanie zdarzeń

1. Systemy AI wysokiego ryzyka muszą dysponować technicznymi możliwościami automatycznego rejestrowania zdarzeń (zwanymi dalej „rejestrami zdarzeń") w całym cyklu życia danego systemu.

2. W celu zapewnienia, by poziom identyfikowalności funkcjonowania systemu AI wysokiego ryzyka był stosowny ze względu na przeznaczenie tego systemu, funkcja rejestracji zdarzeń musi umożliwiać rejestrowanie zdarzeń istotnych dla:

a) identyfikowania sytuacji, które mogą skutkować tym, że system AI wysokiego ryzyka będzie stwarzał ryzyko w rozumieniu art. 79 ust. 1, lub które mogą prowadzić do 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. 5.

3. W przypadku systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 1 lit. a), funkcja rejestracji zdarzeń musi zapewniać rejestrowanie 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 uczestniczących w weryfikacji wyników, o których mowa w art. 14 ust. 5.

Artykuł 13

Przejrzystość i udostępnianie informacji podmiotom stosującym

1. Systemy AI wysokiego ryzyka projektuje się i rozwija w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą podmiotom stosującym interpretację wyników systemu i ich właściwe wykorzystanie. Zapewnia się odpowiedni rodzaj i stopień przejrzystości w celu osiągnięcia spełnienia przez dostawcę i podmiot stosujący odpowiednich obowiązków określonych 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.

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 jego 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 udostępniania informacji istotnych dla wyjaśnienia jego wyników;

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

(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 interpretację wyników systemu AI wysokiego ryzyka i odpowiednie wykorzystanie tych wyników;

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

d) środki nadzoru ze strony człowieka, o których mowa w art. 14, w tym środki techniczne wprowadzone w celu ułatwienia podmiotom stosującym interpretacji wyników 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 prawidłowe zbieranie, przechowywanie i interpretowanie rejestrów zdarzeń, zgodnie z art. 12.

Artykuł 14

Nadzór ze strony człowieka

1. Systemy AI wysokiego ryzyka projektuje się i rozwija w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie ich wykorzystywania systemu AI mogły być skutecznie nadzorowane przez 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 ustanowionych w niniejszej sekcji.

3. Środki nadzoru muszą być współmierne do ryzyka, poziomu autonomii i kontekstu wykorzystywania 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.

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

a) należyte zrozumienie odpowiednich możliwości i ograniczeń systemu AI wysokiego ryzyka oraz należyte monitorowanie jego działania, w tym w celu wykrywania anomalii, nieprawidłowego funkcjonowania i nieoczekiwanych wyników działania oraz zaradzeniu im w przypadku ich wystąpienia;

b) pozostawanie świadomym potencjalnej tendencji do automatycznego polegania lub nadmiernego polegania na wyniku wytworzonym przez system 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 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 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 nie podejmował żadnego działania ani decyzji na podstawie identyfikacji będącej wynikiem działania systemu, jeżeli identyfikacji tej nie zweryfikowały ani nie potwierdziły 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 rozwija 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 określonych w ust. 1 oraz wszelkich innych istotnych wskaźników skuteczności działania, Komisja we współpracy z odpowiednimi zainteresowanymi stronami i organizacjami, takimi jak organy metrologiczne i organy ds. analizy porównawczej, zachęca w stosownych przypadkach do opracowywania poziomów odniesienia 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 zakresie 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, rozwija się w taki sposób, aby w możliwie największym stopniu wyeliminować lub ograniczyć ryzyko potencjalnie stronniczych wyników wpływających na dane wejściowe wykorzystywane na potrzeby przyszłych operacji (sprzężenie zwrotne) oraz aby zapewnić, by wszelkie tego typu sprzężenie zwrotne zostało odpowiednio uwzględnione przy pomocy odpowiednich środków ograniczających ryzyko.

5. Systemy AI wysokiego ryzyka muszą być odporne na próby nieupoważnionych osób trzecich mające na celu zmianę ich wykorzystania, 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 elementami stosowanymi przy trenowaniu, które zostały poddane pretrenowaniu (zatruwanie modelu), wprowadzaniu danych wejściowych, 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 ich kontrolowania.

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 dołączonej do niego dokumentacji, 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, 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 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 dołączonej do niego dokumentacji, na potwierdzenie zgodności z niniejszym rozporządzeniem;

i) spełniają 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 uzasadniony wniosek właściwego organu krajowego, zgodność systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2;

l) zapewniają, by system AI wysokiego ryzyka był zgodny z wymogami 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 rozwoju, kontroli jakości i zapewniania jakości systemu AI wysokiego ryzyka;

d) procedury badania, testowania i walidacji, które należy przeprowadzić przed przystąpieniem do rozwoju systemu AI wysokiego ryzyka, w trakcie tego rozwoju 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 ustanowionych 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, zbierania 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 obsługa systemu monitorowania po wprowadzeniu do obrotu, zgodnie z art. 72;

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

j) porozumiewanie się 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 rejestrowania wszelkiej istotnej dokumentacji i wszelkich istotnych informacji;

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

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

2. Wdrożenie aspektów, o których mowa w ust. 1, musi być proporcjonalne do wielkości organizacji dostawcy. W każdym przypadku dostawcy przestrzegają stopnia rygoryzmu i poziomu ochrony wymaganych 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 sektorowych przepisów prawa Unii, mogą uwzględnić aspekty wymienione w ust. 1 jako część systemów zarządzania jakością zgodnie z tymi przepisami.

4. W odniesieniu do dostawców będących instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie przepisów prawa Unii 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 przepisami prawa Unii 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 miejsce zamieszkania lub 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 przepisów prawa Unii dotyczących usług finansowych, prowadzą dokumentację techniczną jako część dokumentacji prowadzonej na podstawie odpowiednich przepisów prawa Unii dotyczących usług finansowych.

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 stosowny ze względu na przeznaczenie systemu AI wysokiego ryzyka, wynoszący co najmniej 6 miesięcy, o ile mające zastosowanie prawo Unii lub prawo krajowym, w szczególności prawo Unii dotyczące ochrony danych osobowych, nie stanowi inaczej.

2. Dostawcy będący instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie przepisów prawa Unii dotyczących usług finansowych, prowadzą 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 uważają lub mają powody, by uważać, że system AI wysokiego ryzyka, który wprowadzili do obrotu lub oddali do użytku, nie jest zgodny z niniejszym rozporządzeniem, natychmiast podejmują niezbędne działania naprawcze w celu, stosownie do przypadku, zapewnienia zgodności tego systemu, wycofania go z rynku, wyłączenia go lub wycofania go z użytku. Informują oni o tym dystrybutorów danego systemu AI wysokiego ryzyka oraz, w stosownych przypadkach, odpowiednio podmioty stosujące, upoważnionego przedstawiciela i importerów.

2. W przypadku gdy system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1 i dostawca danego systemu dowie się o tym ryzyku, dostawca ten natychmiast wyjaśnia przyczyny tego ryzyka, w stosownych przypadkach we współpracy ze zgłaszającym podmiotem stosującym, oraz informuje organy nadzoru rynku właściwe w zakresie przedmiotowych systemów AI wysokiego ryzyka, 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 uzasadniony wniosek 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 uzasadniony wniosek właściwego organu dostawcy zapewniają również występującemu z wnioskiem właściwemu organowi, 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 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 miejsce zamieszkania lub siedzibę w państwach trzecich ustanawiają – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego miejsce zamieszkania lub 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. Upoważniony przedstawiciel przekazuje organom nadzoru rynku, na wniosek, kopię pełnomocnictwa w jednym z oficjalnych języków instytucji Unii wskazanym przez właściwy organ. Do celów niniejszego rozporządzenia pełnomocnictwo uprawnia upoważnionego przedstawiciela do wykonywania następujących zadań:

a) sprawdzenie, czy zostały sporządzone deklaracja zgodności UE, o której mowa w art. 47, 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 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 ustanowił upoważnionego przedstawiciela, kopii deklaracji zgodności UE, o której mowa w art. 47, dokumentacji technicznej oraz, w stosownych przypadkach, certyfikatu wydanego przez jednostkę notyfikowaną;

c) przekazywanie właściwemu organowi, na uzasadniony wniosek, wszelkich informacji i dokumentów, w tym tych, o których mowa 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 ograniczyć ryzyko, jakie stwarza ten system AI wysokiego ryzyka;

e) w stosownych przypadkach spełnianie obowiązków rejestracyjnych, o których mowa w art. 49 ust. 1, lub, jeżeli rejestracji dokonuje sam dostawca, zapewnienie, by informacje, o których mowa w załączniku VIII sekcja A pkt 3, 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 uważa lub ma powody uważać, że dostawca działa w sposób sprzeczny ze swoimi obowiązkami wynikającymi z niniejszego rozporządzenia. W takim przypadku upoważniony przedstawiciel natychmiast informuje o wypowiedzeniu pełnomocnictwa i jego przyczynach odpowiedni organ nadzoru rynku, a także, w stosownych przypadkach, odpowiednią jednostkę notyfikowaną.

Artykuł 23

Obowiązki importerów

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

a) dostawca 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, o której mowa w art. 47, oraz instrukcję obsługi;

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

2. W przypadku gdy importer ma wystarczające powody, aby uważać, że system AI wysokiego ryzyka jest niezgodny z niniejszym rozporządzeniem lub został sfałszowany lub sfałszowana została dołączona do niego dokumentacja, nie wprowadza tego systemu do obrotu, dopóki nie zostanie zapewniona jego zgodność z niniejszym rozporządzeniem. 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 w systemie AI wysokiego ryzyka, na opakowaniu tego systemu lub, w stosownych przypadkach, w dołączonej do niego dokumentacji swoją nazwę, zarejestrowaną nazwę handlową lub zarejestrowany znak towarowy i adres, pod którym można się z nimi skontaktować.

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 ustanowionymi w sekcji 2.

5. Przez okres 10 lat od wprowadzenia systemu AI wysokiego ryzyka do obrotu lub oddania go do użytku, importerzy przechowują kopię certyfikatu wydanego przez jednostkę notyfikowaną, w stosownych przypadkach, kopię instrukcji obsługi oraz deklaracji zgodności UE, o której mowa w art. 47.

6. Na uzasadniony wniosek odpowiednich właściwych organów importerzy przekazują im wszelkie niezbędne informacje i dokumentację, w tym te, o których mowa w ust. 5, w celu wykazania zgodności systemu AI wysokiego ryzyka z wymogami ustanowionymi w sekcji 2, w języku łatwo zrozumiałym dla tych organów. W tym celu importerzy zapewniają również możliwość udostępnienia tym organom dokumentacji technicznej.

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

Artykuł 24

Obowiązki dystrybutorów

1. Przed udostępnieniem na rynku systemu AI wysokiego ryzyka dystrybutorzy sprawdzają, czy został on opatrzony wymaganym oznakowaniem zgodności CE, czy dołączono do niego kopię deklaracji zgodności UE, o której mowa w art. 47, i instrukcję obsługi oraz czy dostawca oraz – w stosownych przypadkach – importer tego systemu spełnili swoje obowiązki ustanowione 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 z tymi wymogami, do wycofania go z rynku lub wycofania go z użytku lub zapewnia podjęcie takich działań naprawczych przez, stosownie do przypadku, dostawcę, importera lub odpowiedniego operatora. W przypadku gdy system AI wysokiego ryzyka stwarza ryzyko w rozumieniu art. 79 ust. 1, dystrybutor natychmiast informuje o tym dostawcę lub importera systemu oraz organy właściwe w zakresie przedmiotowego system AI wysokiego ryzyka, przekazując szczegółowe informacje w szczególności na temat niezgodności systemu z wymogami i wszelkich podjętych działań naprawczych.

5. Na uzasadniony wniosek odpowiedniego organu 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 odpowiednimi organami krajowymi w zakresie wszelkich działań, które organy te podejmują w odniesieniu do systemu AI wysokiego ryzyka udostępnionego na rynku przez dystrybutorów, w szczególności aby zmniejszyć lub ograniczyć 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 ustanowionymi w art. 16 każdego dystrybutora, importera, podmiot stosujący lub inną stronę trzecią, jeżeli zachodzi którakolwiek z następujących okoliczności:

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

2. W przypadku zaistnienia okoliczności, o których mowa w ust. 1, dostawcy, który pierwotnie wprowadził do obrotu lub oddał do użytku ten system AI, 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 spełnienia obowiązków określonych w niniejszym rozporządzeniu, w szczególności w odniesieniu do zgodności z kryteriami oceny zgodności systemów AI wysokiego ryzyka. Niniejszego ustępu nie stosuje się w przypadkach, gdy pierwotny dostawca wyraźnie określił, że jego system AI nie może zostać zmieniony 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 produktów uznaje się za dostawcę systemu AI wysokiego ryzyka i podlega on obowiązkom ustanowionym w art. 16, jeżeli zachodzi którakolwiek z następujących okoliczności:

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, wskazują, 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 spełnienie obowiązków ustanowionych w niniejszym rozporządzeniu. Niniejszego ustępu nie stosuje się do osób trzecich udostępniających publicznie na podstawie bezpłatnej licencji otwartego oprogramowania narzędzia, usługi, procesy lub komponenty inne niż modele AI ogólnego przeznaczenia.

Urząd ds. AI może opracować i zalecić dobrowolne wzorcowe postanowienia umowne 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 dobrowolnych wzorcowych postanowień umownych, Urząd ds. AI bierze również pod uwagę ewentualne wymogi umowne mające zastosowanie w określonych sektorach lub przypadkach biznesowych. Dobrowolne wzorcowe postanowienia umowne 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 w celu zapewnienia, aby systemy takie były wykorzystywane zgodnie z dołączoną do nich instrukcją obsługi.

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

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

4. Bez uszczerbku dla ust. 1 i 2 podmiot stosujący zapewnia, w zakresie, w jakim sprawuje on kontrolę nad danymi wejściowymi, adekwatność i wystarczającą reprezentatywność danych wejściowych w odniesieniu do przeznaczenia systemu AI wysokiego ryzyka.

5. Podmioty stosujące 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 mają powody uważać, że wykorzystanie systemu AI wysokiego ryzyka zgodnie z instrukcją obsługi może powodować, że ten system AI będzie stwarzał ryzyko w rozumieniu art. 79 ust. 1, bez zbędnej zwłoki informują o tym dostawcę lub dystrybutora oraz odpowiedni organ nadzoru rynku i zawieszają wykorzystywanie systemu. W przypadku gdy podmioty stosujące stwierdziły wystąpienie poważnego incydentu, natychmiast informują o tym incydencie najpierw dostawcę, a następnie importera lub dystrybutora oraz odpowiednie organy nadzoru rynku. Jeżeli podmiot stosujący nie jest w stanie skontaktować się z dostawcą, art. 73 stosuje się odpowiednio. Obowiązek ten nie obejmuje wrażliwych danych operacyjnych podmiotów stosujących systemy AI będących organami ścigania.

W odniesieniu do podmiotów stosujących będących instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie przepisów prawa Unii dotyczących usług finansowych, obowiązek w zakresie monitorowania, 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 pod ich kontrolą – przez stosowny ze względu na przeznaczenie danego systemu AI wysokiego ryzyka okres, wynoszący co najmniej sześć miesięcy, o ile mające zastosowanie prawo Unii lub prawo krajowe, w szczególności prawo Unii dotyczące ochrony danych osobowych, nie stanowi inaczej.

Podmioty stosujące będące instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie przepisów prawa Unii 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 będące pracodawcami informują przedstawicieli pracowników i pracowników, których to dotyczy, że będzie w stosunku do nich wykorzystywany system AI wysokiego ryzyka. Informacje te przekazuje się, w stosownych przypadkach, zgodnie z zasadami i procedurami ustanowionymi w prawie Unii i prawie krajowym oraz praktyką w zakresie informowania pracowników i ich przedstawicieli.

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

9. W stosownych przypadkach, podmioty stosujące systemy AI wysokiego ryzyka korzystają z informacji przekazanych na podstawie art. 13 niniejszego rozporządzenia, aby spełnić spoczywając na nich obowiązki 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 dotyczącego 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 wymiaru sprawiedliwości lub organu administracyjnego, którego decyzja jest wiążąca i podlega kontroli sądowej, z wnioskiem o zezwolenie na wykorzystanie 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 wykorzystanie takiego systemu musi być ograniczone do tego, co jest bezwzględnie konieczne do prowadzenia postępowań przygotowawczych w sprawie konkretnego przestępstwa.

W przypadku gdy wniosek o zezwolenie, o którym mowa w akapicie pierwszym, zostanie odrzucony, korzystanie 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 przypadku 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 rzeczywistym i dającym się przewidzieć zagrożeniem popełnieniem przestępstwa lub poszukiwaniem konkretnej osoby zaginionej. Zapewnia się, aby organy ścigania mogły wydać żadnej decyzji wywołującej niepożądane skutki prawne dla danej osoby 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 każde wykorzystanie takich systemów AI wysokiego ryzyka musi zostać udokumentowane w odpowiednich aktach policyjnych i udostępnione na wniosek właściwego organu nadzoru rynku i krajowemu organowi ochrony danych, z wyłączeniem ujawniania wrażliwych danych operacyjnych związanych ze ściganiem przestępstw. Niniejszy akapit pozostaje bez uszczerbku dla uprawnień powierzonych organom nadzorczym dyrektywą (UE) 2016/680.

Podmioty stosujące przedkładają właściwym organom nadzoru rynku i krajowym organom ochrony danych roczne sprawozdania dotyczące wykorzystania przez nie systemów zdalnej identyfikacji biometrycznej *post factum*, z wyłączeniem ujawniania wrażliwych 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 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 stosunku do nich wykorzystywany system AI wysokiego ryzyka. W przypadku systemów AI wysokiego ryzyka wykorzystywanych do celów ścigania przestępstw stosuje się art. 13 dyrektywy (UE) 2016/680.

12. Podmioty stosujące współpracują z odpowiednimi właściwymi organami przy wszelkich działaniach, które organy te podejmują w odniesieniu do systemu AI wysokiego ryzyka, w celu wykonywania niniejszego rozporządzenia.

Artykuł 27

Ocena skutków systemów AI wysokiego ryzyka dla praw podstawowych

1. Przed wdrożeniem 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 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 skutków w zakresie praw podstawowych, jakie może wywołać wykorzystanie takiego systemu. W tym celu podmioty stosujące przeprowadzają ocenę obejmującą:

a) opis procesów podmiotu stosującego, 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 tego wykorzystywania;

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

d) szczególne ryzyko szkody, które może mieć wpływ na kategorie osób fizycznych 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 urzeczywistnienia 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 może polegać na wcześniej przeprowadzonych ocenach skutków dla praw podstawowych lub na istniejących ocenach skutków przeprowadzonych przez dostawcę. Jeżeli w trakcie wykorzystania systemu AI wysokiego ryzyka podmiot stosujący 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 powiadamia organ nadzoru rynku o jej wynikach, przedkładając jako element tego powiadomienia wypełniony wzór, o którym mowa w ust. 5 niniejszego artykułu. W przypadku, o którym mowa w art. 46 ust. 1, podmioty stosujące mogą zostać zwolnione z obowiązku dokonania powiadomienia.

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 w zakresie praw podstawowych, o której mowa w ust. 1 niniejszego artykułu, stanowi uzupełnieniem tej oceny skutków dla ochrony danych.

5. Urząd ds. AI opracowuje wzór kwestionariusza, w tym za pomocą zautomatyzowanego narzędzia, aby ułatwić podmiotom stosującym spełnianie 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 przygotowywane 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 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 przeprowadzały 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 muszą posiadać, w odpowiednich przypadkach, wiedzę fachową niezbędną do pełnienia ich funkcji 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 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 spełnienia przez tę jednostkę wymogów ustanowionych w art. 31.

4. W odniesieniu do jednostek notyfikowanych wyznaczonych na podstawie 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, w każdym przypadku gdy wystąpią istotne zmiany, aby umożliwić organowi odpowiedzialnemu za jednostki notyfikowane monitorowanie i weryfikowanie, czy zapewniona jest ciągła zgodność 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 Komisji i pozostałym państwom członkowskim 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 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 pozostałym państwom członkowskim dowody w postaci dokumentów potwierdzające kompetencje jednostki oceniającej zgodność oraz wdrożone rozwiązania zapewniające regularne monitorowanie tej jednostki i nieustanne spełnianie przez nią wymagań ustanowionych w art. 31.

4. Dana jednostka oceniająca zgodność może wykonywać czynności jednostki notyfikowanej tylko wówczas, gdy Komisja lub pozostałe państwa członkowskie nie zgłosiły sprzeciwu 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 sprzeciwu Komisja niezwłocznie przystępuje do konsultacji z odpowiednimi państwami członkowskimi i jednostką oceniającą zgodność. Na podstawie tych konsultacji 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. Jednostkę notyfikowaną ustanawia się zgodnie z prawem krajowym danego państwa członkowskiego i ma ona 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 zapewniają, 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 będących przedmiotem oceny 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, rozwój, 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 czynnościami z zakresu 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 czynności. Jednostki notyfikowane dokumentują i wdrażają strukturę i procedury służące zagwarantowaniu ich bezstronności oraz propagowaniu i stosowaniu zasad bezstronności we wszystkich podejmowanych przez nie czynnościach organizacyjnych i kadrowych oraz we wszystkich ich czynnościach 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 podejmują czynności.

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 dysponuje stałą dostępnością 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 zapewniają, 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*, domniemuje 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 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 dnia zakończenia podwykonawstwa.

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, w którym prowadzi on działalność, jego strukturę oraz stopień złożoności danego systemu AI wysokiego ryzyka, w szczególności w celu zminimalizowania obciążeń administracyjnych i kosztów zapewnienia zgodności dla mikroprzedsiębiorstw i małych przedsiębiorstw w rozumieniu zalecenia 2003/361/WE. Jednostka notyfikowana przestrzega jednak rygoryzmu i poziomu ochrony wymaganych do zapewnienia zgodności danego systemu AI wysokiego ryzyka z wymogami niniejszego rozporządzenia.

3. Na wniosek organu notyfikującego, o którym mowa w art. 28, jednostki notyfikowane udostępniają i przekazują temu organowi wszystkie stosowne dokumenty, uwzględniając dokumentację dostawców, aby umożliwić temu organowi przeprowadzenie 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 stosuje się do rozszerzenia zakresu notyfikacji.

W przypadku zmian w notyfikacji innych niż rozszerzenie jej zakresu stosuje się procedury ustanowione w ust. 3-9.

3. W przypadku gdy jednostka notyfikowana podejmie decyzję o zaprzestaniu prowadzenia czynności z zakresu oceny zgodności, jak najszybciej informuje o tym organ notyfikujący i zainteresowanych dostawców, a w przypadku planowanego zaprzestania działalności – na co najmniej rok przed zaprzestaniem działalności. Certyfikaty wydane przez jednostkę notyfikowaną mogą pozostać ważne 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 ta inna jednostka notyfikowana przeprowadza pełną ocenę odnośnych systemów AI wysokiego ryzyka, zanim wyda nowe certyfikaty dla tych systemów. W przypadku gdy jednostka notyfikowana zaprzestała działalności, organ notyfikujący cofa jej wyznaczenie.

4. W przypadku gdy organ notyfikujący ma wystarczające powody, by uważać, że jednostka notyfikowana przestała spełniać wymogi określone w art. 31 lub nie spełnia 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 zgłoszonym sprzeciwu i zapewnia jej możliwość ustosunkowania się do tego sprzeciwu. Jeżeli organ notyfikujący dojdzie do wniosku, że jednostka notyfikowana przestała spełniać wymogi ustanowione w art. 31 lub nie spełnia swoich obowiązków, organ ten, stosownie do przypadku, ogranicza, zawiesza lub cofa wyznaczenie, w zależności od powagi niespełnienia tych wymogów lub tych obowiązków. Informuje on o tym natychmiast Komisję i pozostałe państwa członkowskie.

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

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 ona 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 skutki dla certyfikatów wydanych przez daną jednostkę notyfikowaną;

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

c) zwraca się do jednostki notyfikowanej z żądaniem, by w celu zapewnienia ciągłości zgodności systemów AI wysokiego ryzyka 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, których zawieszenia lub cofnięcia zażądał; organy te podejmują w stosownych przypadkach odpowiednie środki w celu uniknięcia potencjalnego ryzyka dla zdrowia, bezpieczeństwa lub praw podstawowych.

8. Z wyjątkiem certyfikatów nienależnie wydanych, w przypadkach, w których wyznaczenie zostało zawieszone lub ograniczone, certyfikaty pozostają ważne, jeżeli zachodzi którakolwiek z następujących okoliczności:

a) organ notyfikujący potwierdził, w terminie jednego miesiąca od zawieszenia lub ograniczenia, że w odniesieniu do certyfikatów, których dotyczy zawieszenie lub ograniczenie, nie występuje ryzyko dla zdrowia, bezpieczeństwa lub praw podstawowych i określił czas działań służących temu, by znieść zawieszenie lub ograniczenie; 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.

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 wysokiego ryzyka objętego certyfikatem ma zarejestrowane miejsce prowadzenia działalności, potwierdził, że nie występuje ryzyko dla 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 te systemy 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 o dodatkowe trzymiesięczne okresy, które łącznie nie mogą przekraczać dwunastu miesięcy.

Właściwy organ krajowy lub jednostka notyfikowana przejmująca funkcje jednostki notyfikowanej, której dotyczy zmiana wyznaczenia, natychmiast powiadamiają o tym Komisję, pozostałe państwa członkowskie i pozostałe jednostki notyfikowane.

Artykuł 37

Kwestionowanie kompetencji jednostek notyfikowanych

1. W razie konieczności Komisja przeprowadza postępowanie wyjaśniające dotyczące wszystkich przypadków, w których ma podstawy, by 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 wniosek, 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 notyfikujące państwo członkowskie i zwraca się do niego o podjęcie koniecznych środków naprawczych, włącznie z zawieszeniem lub cofnięciem notyfikacji, jeżeli zachodzi taka potrzeba. W przypadku niepodjęcia 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 w formie sektorowej grupy jednostek notyfikowanych jednostek notyfikowanych prowadzących działalność w zakresie procedur oceny zgodności zgodnie z niniejszym rozporządzeniem.

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.

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 wykonywania czynności jednostek notyfikowanych zgodnie z niniejszym rozporządzeniem, pod warunkiem, że spełniają wymogi ustanowione w art. 31 lub zapewniają równoważny poziom zgodności.

SEKCJA 5

Normy, ocena zgodności, certyfikaty, rejestracja

Artykuł 40

Normy zharmonizowane i dokumenty normalizacyjne

1. W przypadku systemów AI wysokiego ryzyka oraz systemów AI ogólnego przeznaczenia spełniających normy zharmonizowane lub części tych norm, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej* zgodnie z rozporządzeniem (UE) nr 1025/2012, domniemuje się, że spełniają one wymogi ustanowione w sekcji 2 niniejszego rozdziału lub, w stosownych przypadkach, obowiązki ustanowione w rozdziale V sekcja 2 i 3 niniejszego rozporządzenia, w zakresie, w jakim normy te obejmują te wymogi lub obowiązki.

2. Zgodnie z art. 10 rozporządzenia (UE) nr 1025/2012 Komisja wydaje bez zbędnej zwłoki wnioski o normalizację obejmujące wszystkie wymogi ustanowione w sekcji 2 niniejszego rozdziału oraz, w stosownych przypadkach, wnioski o normalizację obejmujące obowiązki ustanowione w rozdziale V sekcja 2 i 3 niniejszego rozporządzenia. We wniosku o normalizację zwraca się również o przedstawienie wyników sprawozdawczości i procesów dokumentowania w celu poprawy skuteczności działania zasobów systemów AI, takich jak zmniejszenie zużycia energii i innych zasobów przez system 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.

Wydając 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 obowiązującego unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I, i mieć na celu zapewnienie, by systemy AI wysokiego ryzyka lub modele AI ogólnego przeznaczenia wprowadzane do obrotu lub oddawane do użytku w Unii spełniały odpowiednie wymogi lub obowiązki 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 Unii, do przyczynienia się do wzmocnienia globalnej współpracy w zakresie normalizacji, z uwzględnieniem istniejących w dziedzinie AI norm międzynarodowych zgodnych z wartościami Unii, prawami podstawowymi i interesem Unii, a także do poprawy zarządzania wielostronnego, 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 może przyjmować akty wykonawcze ustanawiające wspólne specyfikacje w odniesieniu do wymogów ustanowionych w sekcji 2 niniejszego rozdziału lub, w stosownych przypadkach, obowiązków ustanowionych w rozdziale V sekcja 2 i 3, 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, lub, w stosownych przypadkach, w odniesieniu do obowiązków ustanowionych w rozdziale V sekcja 2 i 3, 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, o których mowa w sekcji 2 niniejszego rozdziału, lub, w stosownych przypadkach, obowiązki, o których mowa w rozdziale V sekcja 2 i 3, zgodnie z przepisami rozporządzenia (UE) nr 1025/2012 i nie przewiduje się opublikowania takiego odniesienia w rozsądnym terminie.

Przygotowując projekt wspólnych specyfikacji, Komisja konsultuje się z forum doradczym, o którym mowa w art. 67.

Akty wykonawcze, o których mowa w akapicie pierwszym niniejszego ustępu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

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

3. W przypadku systemów AI wysokiego ryzyka lub modeli AI ogólnego przeznaczenia zgodnych ze wspólnymi specyfikacjami, o których mowa w ust. 1, lub z częściami tych specyfikacji domniemuje się, że są one zgodne z wymogami ustanowionymi w sekcji 2 niniejszego rozdziału lub, w stosownych przypadkach, spełniają obowiązki ustanowione w rozdziale V sekcja 2 i 3, w zakresie, w jakim te wspólne specyfikacje obejmują te wymogi i te obowiązki.

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 wymogi ustanowione w sekcji 2 niniejszego rozdziału lub, w stosownych przypadkach, te same obowiązki ustanowione w rozdziale V sekcja 2 i 3.

5. W przypadku gdy dostawcy systemów AI wysokiego ryzyka lub modeli AI ogólnego przeznaczenia nie zapewnią zgodności ze wspólnymi specyfikacjami, o których mowa w ust. 1, należycie wykazują oni, że przyjęli rozwiązania techniczne, które są zgodne z wymogami, o których mowa w rozdziale I sekcja 2, lub, w stosownych przypadkach, spełniają obowiązki ustanowione w rozdziale V sekcja 2 i 3, na poziomie co najmniej równoważnym tym wspólnym specyfikacjom.

6. W przypadku gdy państwo członkowskie uważa, że wspólna specyfikacja nie jest całkowicie zgodna z wymogami ustanowionymi w sekcji 2 lub, w stosownych przypadkach, nie spełnia całkowicie obowiązków ustanowionych w rozdziale V sekcja 2 i 3, 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. W przypadku systemów AI wysokiego ryzyka, które zostały wytrenowane i przetestowane przy użyciu danych odzwierciedlających określone otoczenie geograficzne, behawioralne, kontekstualne lub funkcjonalne, do wykorzystywania w którym są one przeznaczone, domniemuje się, że spełniają one odpowiednie wymogi ustanowione w art. 10 ust. 4.

2. W przypadku systemów 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*, domniemuje się, że spełniają one 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 postępuje zgodnie z procedurą oceny zgodności ustanowioną 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 postępuje zgodnie z odpowiednią procedurą 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. 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, 5, 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, pod warunkiem że producent ten zapewnił 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 wszystkie 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 jest przeznaczony do dalszej dystrybucji lub czy ma być nadal wykorzystywany przez obecny podmiot stosujący.

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 początkowej oceny zgodności i które są częścią informacji zawartych w dokumentacji technicznej, o której mowa w pkt 2 lit. f) załącznika IV.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 97 w celu zmiany załączników VI i VII poprzez ich zmianę w świetle postępu technicznego.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych 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 ryzyku dla zdrowia i bezpieczeństwa oraz ryzyku związanemu z ochroną praw podstawowych stwarzanemu przez takie systemy lub minimalizowaniu takiego ryzyka, 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 jest ważny.

3. Jeżeli jednostka notyfikowana ustali, 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.

Od decyzji jednostek notyfikowanych, w tym dotyczących wydanych certyfikatów zgodności, przysługuje odwołanie.

Artykuł 45

Obowiązki jednostek notyfikowanych w zakresie informowania

1. Jednostki notyfikowane informują organ notyfikujący:

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

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

c) o okolicznościach wpływających na zakres lub warunki notyfikacji;

d) o wystąpieniu przez organy nadzoru rynku z wnioskiem udzielenia informacji o czynnościach z zakresu oceny zgodności;

e) na wniosek, 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 o:

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

b) 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 wniosek – 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 wniosek – pozytywnymi wynikami oceny zgodności.

4. Organy notyfikujące zapewniają poufność otrzymywanych informacji zgodnie z art. 78.

Artykuł 46

Odstępstwo od procedury oceny zgodności

1. Na zasadzie odstępstwa od art. 43 i na należycie uzasadniony wniosek 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. Zezwolenie to 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 uzasadnionych pilnych przypadkach w związku z wystąpieniem nadzwyczajnych względów 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 wykorzystywania tego systemu lub tuż po nim. W przypadku odmowy wydania zezwolenia, o którym mowa w ust. 1, wykorzystywanie tego systemu AI wysokiego ryzyka wstrzymuje się ze skutkiem natychmiastowym, a wszystkie rezultaty i wyniki tego wykorzystania muszą zostać natychmiast odrzucone.

3. Zezwolenie, o którym mowa w ust. 1, wydaje się wyłącznie wówczas, gdy organ nadzoru rynku stwierdzi, że system AI wysokiego ryzyka jest zgodny z wymogami ustanowionymi w sekcji 2. Organ nadzoru rynku informuje Komisję i pozostałe państwa członkowskie o zezwoleniach wydanych zgodnie z ust. 1 i 2. Obowiązek ten nie obejmuje wrażliwych 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 sprzeciwu dotyczącego zezwolenia wydanego przez organ nadzoru rynku państwa członkowskiego zgodnie z ust. 1, takie zezwolenie uznaje się za uzasadnione.

5. Jeżeli w terminie 15 dni kalendarzowych od dnia otrzymania informacji, o której mowa w ust. 3, państwo członkowskie zgłosi sprzeciw dotyczący 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, 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 odpowiednich operatorów.

6. W przypadku gdy Komisja uzna zezwolenie za bezpodstawne, organ nadzoru rynku zainteresowanego państwa członkowskiego cofa je.

7. W przypadku systemów AI wysokiego ryzyka powiązanych z produktami objętymi zakresem stosowania unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I sekcja A stosuje się 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 wniosek.

2. W deklaracji zgodności UE stwierdza się, że dany system AI wysokiego ryzyka spełnia wymogi ustanowione w sekcji 2. Deklaracja zgodności UE zawiera informacje określone 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 przepisów 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 jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 97 w celu zmiany załącznika V poprzez zaktualizowanie treści deklaracji zgodności UE określonej w tym załączniku w celu wprowadzenia elementów, które stały się konieczne w świetle postępu technicznego.

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 w formie cyfrowej 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 taki sposób nie jest możliwe lub zasadne, oznakowanie to umieszcza się na opakowaniu lub – w stosownych przypadkach – w dołączonej do systemu dokumentacji.

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, według wskazówek jednostki notyfikowanej, dostawca lub jego upoważniony przedstawiciel. 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 lub oddaniem do użytku systemu AI wysokiego ryzyka wymienionego w załączniku III, z wyjątkiem systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 2, dostawca lub – w stosownych przypadkach – jego upoważniony przedstawiciel rejestrują się i swój system w bazie danych UE, 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 się i swój system w bazie danych UE, 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 będące publicznymi organami, instytucjami, organami lub jednostkami organizacyjnymi Unii lub osobami działającymi w ich imieniu rejestrują się, wybierają system i rejestrują jego wykorzystanie w bazie danych UE, o której mowa w art. 71.

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, rejestracji, o której mowa w ust. 1, 2 i 3 niniejszego artykułu, dokonuje się w bezpiecznej niepublicznej sekcji bazy danych UE, o której mowa w art. 71, i – stosownie do przypadku – zawiera wyłącznie następujące informacje, o których mowa w:

a) załączniku VIII sekcja A pkt 1–10, z wyjątkiem pkt 6, 8 i 9;

b) załączniku VIII sekcja B pkt 1–5 oraz pkt 8 i 9;

c) załączniku VIII sekcja C pkt 1–3;

d) załączniku IX pkt 1, 2, 3 i 5.

Do odpowiednich zastrzeżonych sekcji bazy danych UE 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 poziomie krajowym.

ROZDZIAŁ IV

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

Artykuł 50

Obowiązki w zakresie przejrzystości dla dostawców i podmiotów stosujących niektóre systemy AI

1. Dostawcy zapewniają, aby systemy AI przeznaczone do wchodzenia w bezpośrednią interakcję z osobami fizycznymi projektowano i rozwijano 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 wykorzystywania. Obowiązek ten nie ma zastosowania do systemów AI, których wykorzystywanie jest dozwolone na mocy prawa do celów wykrywania przestępstw, przeciwdziałania im, prowadzenia postępowań przygotowawczych w ich sprawie lub ścigania ich sprawców, z zastrzeżeniem odpowiednich zabezpieczeń w zakresie praw 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 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 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 ich 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 stosownie do przypadku zgodnie z rozporządzeniami (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywą (UE) 2016/680. Obowiązek ten nie ma zastosowania do systemów AI wykorzystywanych do kategoryzacji biometrycznej i rozpoznawania emocji, których wykorzystywanie jest dozwolone z mocy prawa do celów wykrywania przestępstw, przeciwdziałania im i prowadzenia postępowań przygotowawczych w przestępstwami ich sprawach, z zastrzeżeniem odpowiednich zabezpieczeń w zakresie praw 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 zmanipulowane. Obowiązek ten nie ma zastosowania, w przypadku gdy wykorzystywanie jest dozwolone na mocy prawa w celu wykrywania przestępstw, zapobiegania im, prowadzenia postępowań przygotowawczych w ich sprawie lub ścigania ich 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 zmanipulowany. Obowiązek ten nie ma zastosowania, w przypadku gdy wykorzystywanie jest dozwolone na mocy prawa w celu wykrywania przestępstw, zapobiegania im, prowadzenia postępowań przygotowawczych w ich sprawie lub ścigania ich sprawców lub w przypadku gdy treści wygenerowane przez AI zostały poddane 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 pierwszego stosowania. Informacje te muszą spełniać mające zastosowanie wymogi dostępności.

6. Ust. 1–4 nie mają wpływu na wymogi i obowiązki ustanowione 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 zachęca do opracowywania kodeksów praktyk na poziomie Unii i wspiera ich opracowanie, aby ułatwić skuteczne wykonywanie obowiązków w zakresie wykrywania i oznaczania treści sztucznie wygenerowanych lub zmanipulowanych. Komisja może przyjmować akty wykonawcze dotyczące zatwierdzenia tych kodeksów praktyk zgodnie z procedurą ustanowioną w art. 56 ust. 6. Jeżeli Komisja uzna, że kodeks nie jest odpowiedni, może przyjąć akt wykonawczy określający wspólne zasady wykonywania tych obowiązków zgodnie z procedurą sprawdzającą ustanowioną w art. 98 ust. 2.

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 którykolwiek z następujących warunków:

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. W przypadku modelu AI ogólnego przeznaczenia, którego łączna liczba obliczeń wykorzystywanych do jego trenowania mierzona w operacjach zmiennoprzecinkowych jest większa niż 10^{25}, domniemuje się za mający zdolności dużego oddziaływania zgodnie z ust. 1 lit. a),.

3. Komisja przyjmuje akty delegowane zgodnie z art. 97 w celu zmiany progów wymienionych w ust. 1 i 2 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 warunki, o których mowa w art. 51 ust. 1 lit. a), odpowiedni dostawca powiadamia Komisję niezwłocznie, a w każdym przypadku w terminie dwóch tygodni od spełnienia tego warunku lub od kiedy wiadomo, że zostanie on spełniony. Powiadomienie to zawiera informacje niezbędne do wykazania, że dany warunek został spełniony. 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 spełniający warunek, o którym mowa w art. 51 ust. 1 lit. a), modelu AI ogólnego przeznaczenia z ryzykiem systemowym może wraz ze swoim powiadomieniem przedstawić wystarczająco uzasadnione argumenty wykazujące, że wyjątkowo, pomimo spełniania przez ten model AI ogólnego przeznaczenia przedmiotowego warunku, nie stwarza on – z uwagi na swoje szczególne cechy – ryzyka systemowego i nie powinien być w związku z tym zaklasyfikowany 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, a dany model AI ogólnego przeznaczenia uważa się 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 jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 97 w celu zmiany załącznika XIII poprzez określenie i zaktualizowanie 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 bierze pod uwagę taki wniosek i może zdecydować o ponownej ocenie w celu stwierdzenia, czy dany model AI ogólnego przeznaczenia może być nadal uważany 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 z wnioskiem o ponowną ocenę najwcześniej sześć miesięcy po podjęciu decyzji o uznaniu. W przypadku gdy w wyniku ponownej oceny Komisja zdecyduje się utrzymać uznanie modelu za model AI ogólnego przeznaczenia z ryzykiem systemowym, dostawcy mogą zwrócić się z wnioskiem o ponowną ocenę najwcześniej sześć miesięcy po podjęciu 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 co najmniej informacje określone w załączniku XI do celów przekazania ich, na wniosek, Urzędowi ds. AI i właściwym organom krajowym;

b) sporządzają, aktualizują i udostępniają informacje i dokumentację dostawcom systemów AI, którzy zamierzają zintegrować model AI ogólnego przeznaczenia ze swoimi systemami AI. Bez uszczerbku dla potrzeby przestrzegania 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 spełnienie ich obowiązków zgodnie z niniejszym rozporządzeniem; oraz

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

c) wprowadzają politykę służącą zapewnieniu zgodności z prawem Unii dotyczącym prawa autorskiego i praw pokrewnych, w szczególności z myślą o identyfikacji i zastosowaniu się, w tym poprzez najnowocześniejsze technologie, do 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. Obowiązków określonych w ust. 1 lit. a) i b) nie stosuje się do dostawców modeli AI, które są udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania umożliwiającej dostęp, wykorzystanie, zmianę i dystrybucję modelu i których parametry, w tym wagi, informacje o architekturze modelu oraz informacje o wykorzystaniu modelu są podawane do wiadomości publicznej. Wyjątku tego nie stosuje się do 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 ustanowionych w ust. 1 niniejszego artykułu. Zgodność z europejskimi normami zharmonizowanymi stwarza dla dostawcy domniemanie spełnienia tych obowiązków w zakresie, w jakim normy te obejmują te obowiązki. Dostawcy modeli AI ogólnego przeznaczenia, którzy nie zobowiązują się do przestrzegania zatwierdzonego kodeksu praktyk lub nie zapewniają zgodności z europejską normą zharmonizowaną, przedstawiają Komisji do oceny adekwatne alternatywne środki służące zapewnieniu zgodności.

5. Do celu ułatwienia zgodności z załącznikiem XI, w szczególności jego pkt 2 lit. d) i e), Komisja jest uprawniona do przyjmowania zgodnie z art. 97 aktów delegowanych dotyczących szczegółowego określenia metod pomiaru i obliczeń umożliwiających porównywalną i weryfikowalną dokumentację.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych 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 ustanawiają – 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. Przekazuje on Urzędowi ds. AI na jego wniosek 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 danych kontaktowych dostawcy, który ustanowił danego upoważnionego przedstawiciela;

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

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

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

5. 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 natychmiast Urząd ds. AI o wypowiedzeniu pełnomocnictwa i o jego przyczynach.

6. Obowiązek określony w niniejszym artykule nie dotyczy dostawców modeli AI ogólnego przeznaczenia, które są udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania umożliwiającej dostęp, wykorzystanie, zmianę 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 i 54 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 rozwoju, 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. Zgodność z europejskimi normami zharmonizowanymi stwarza dla dostawcy domniemanie spełnienia tych obowiązków w zakresie, w jakim normy te obejmują te obowiązki. Dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym, którzy nie zobowiązują się do przestrzegania zatwierdzonego kodeksu praktyk lub nie zapewniają zgodności z europejską normą zharmonizowaną, przedstawiają Komisji do oceny 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.

SEKCJA 4

Kodeksy praktyk

Artykuł 56

Kodeksy praktyk

1. Urząd ds. AI zachęca do sporządzania kodeksów praktyk na poziomie 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 poziomie Unii, w tym, w stosownych przypadkach, jego źródła;

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

3. Urząd ds. AI może zwrócić się do wszystkich dostawców modeli AI ogólnego przeznaczenia oraz odpowiednich właściwych organów krajowych o wzięcie 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, w celu zapewnienia realizacji tych celów, oraz by uwzględniały w należytym stopniu potrzeby i interesy wszystkich zainteresowanych stron, w tym osób, na które AI ma wpływ, na poziomie 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 muszą odzwierciedlać różnice 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, i regularnie monitorują i oceniają realizację ich celów. Publikują one swoją ocenę adekwatności kodeksów praktyk.

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

7. Urząd ds. AI może zwracać się do 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 pełnym przystąpieniem do kodeksu.

8. Urząd ds. AI w stosownych przypadkach zachęca również do prowadzenia przeglądów i dostosowywania kodeksów praktyk oraz ułatwia takie przeglądy i dostosowania, w szczególności w świetle nowych norm. Urząd ds. AI udziela wsparcia w ocenie dostępnych norm.

9. Kodeksy praktyk muszą być gotowe najpóźniej do dnia 2 maja 2025 r. Urząd ds. AI podejmuje niezbędne kroki, w tym kieruje zachęty do dostawców zgodnie z ust. 7.

Jeśli do dnia 2 sierpnia 2025 r. opracowanie kodeks praktyk nie może zostać zakończone 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 wykonywania 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 poziomie krajowym przynajmniej jedną piaskownicę regulacyjną w zakresie AI, która musi zostać uruchomiona do dnia 2 sierpnia 2026 r. Piaskownica ta może również zostać ustanowiona wspólnie z właściwymi organami innych państw członkowskich. Komisja może zapewniać wsparcie techniczne, doradztwo i narzędzia do celów ustanowienia i działania piaskownic regulacyjnych w zakresie AI.

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

2. Można również ustanowić dodatkowe piaskownice regulacyjne w zakresie AI na poziomie 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 zapewnienia 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 na podstawie prawa Unii lub prawa krajowego. 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 rozwój, 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 dostawcami lub potencjalnymi dostawcami a właściwym organem. Takie piaskownice mogą obejmować testy w warunkach rzeczywistych nadzorowane w jej ramach.

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 ograniczających ryzyko oraz ich skuteczności w odniesieniu do obowiązków i wymogów niniejszego rozporządzenia oraz, w stosownych przypadkach, innych nadzorowanych w ramach danej piaskownicy przepisów prawa Unii i prawa krajowego.

7. Właściwe organy zapewniają dostawcom i potencjalnym dostawcom uczestniczącym w piaskownicy regulacyjnej w zakresie AI wskazówki dotyczące oczekiwań regulacyjnych oraz sposobów spełnienia wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu.

Na wniosek dostawcy lub potencjalnego dostawcy systemu AI właściwy organ przedstawia na piśmie 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 rezultatów i efektów uczenia się. Dostawcy mogą wykorzystywać taką dokumentację do wykazania swojej zgodności z niniejszym rozporządzeniem w ramach procesu oceny zgodności lub odpowiednich działań w zakresie nadzoru rynku. W tym względzie sprawozdania końcowe oraz dowody na piśmie przedstawione przez właściwy organ krajowy są uwzględniane pozytywnie 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 Unii i prawem 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 rynku Unii 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 powodu 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 nadzór 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 poziomie regionalnym lub lokalnym. Stwierdzenie istnienia jakiegokolwiek znaczącego ryzyka dla zdrowa i bezpieczeństwa oraz dla praw podstawowych na etapie rozwoju i testowania takich systemów AI powoduje konieczność właściwego ograniczenia tego ryzyka. Właściwe organy krajowe są uprawnione do tymczasowego lub trwałego zawieszenia procesu testowania lub udziału w piaskownicy, jeżeli skuteczne ograniczenie ryzyka 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 regulacyjnej 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, na podstawie mających zastosowanie przepisów prawa Unii i prawa krajowego dotyczących odpowiedzialności, za wszelkie szkody wyrządzone osobom trzecim w wyniku doświadczeń przeprowadzanych w piaskownicy. Organy nie nakładają jednak administracyjnych kar pieniężnych w związku z naruszeniem niniejszego rozporządzenia, pod warunkiem że potencjalny dostawca respektuje konkretny plan oraz warunki uczestnictwa, a także w dobrej wierze stosuje się do wytycznych właściwych organów krajowych. W przypadku gdy inne właściwe organy odpowiedzialne za inne przepisy prawa Unii lub przepisy 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, 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 zakończenia jej działalności – oraz sprawozdanie końcowe. Sprawozdania te zawierają informacje o postępach i rezultatach 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 stosowania innych przepisów prawa Unii objętego 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 bierze pod uwagę 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 uzyskiwania niewiążących wskazówek w zakresie zapewnienia zgodności innowacyjnych produktów, usług i modeli biznesowych zawierających zintegrowane 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 zasady dotyczące ustanawiania, opracowywania, wdrażania, działania piaskownic regulacyjnych w zakresie AI i nadzoru nad nimi. Te akty wykonawcze określają wspólne zasady dotyczące następujących kwestii:

a) kwalifikowalności i kryteriów wyboru dotyczących uczestnictwa w piaskownicy regulacyjnej w zakresie AI;

b) procedur składania wniosków, uczestnictwa, monitorowania, wychodzenia z piaskownicy regulacyjnej w zakresie AI i zakończenia jej działalności, 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 dostawcy lub potencjalnego dostawcy systemu AI spełniającego kryteria kwalifikowalności i wyboru, które muszą być przejrzyste i bezstronne, a właściwe organy krajowe informowały 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; dostawcy i potencjalni dostawcy mogą również składać wnioski we współpracy z podmiotami stosującymi oraz innymi odpowiednimi osobami trzecimi;

c) szczegółowe zasady i warunki dotyczące piaskownic regulacyjnych w zakresie AI w możliwie najlepszym stopniu wspierały swobodę właściwych organów krajowych w zakresie ustanawiania 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 bezstronny i proporcjonalny sposób mogą być uprawnione właściwe organy krajowe;

e) ułatwiały one dostawcom i 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, w tym przedsiębiorstwa typu start-up, przedsiębiorstwa, innowatorzy, ośrodki testowo-doświadczalne, laboratoria badawczo-doświadczalne, 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 wychodzenia 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, do ośrodków testowo-doświadczalnych, europejskich centrów innowacji cyfrowych oraz centrów 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 zabezpieczenia, mające na celu 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 rozwoju w interesie publicznym określonych systemów AI w ramach piaskownicy regulacyjnej w zakresie AI

1. Dane osobowe zebrane zgodnie z prawem w innych celach można przetwarzać, w ramach piaskownicy regulacyjnej w zakresie AI, wyłącznie do celów rozwoju, trenowania i testowania w ramach piaskownicy niektórych systemów AI, gdy spełnione są wszystkie następujące warunki:

a) systemy AI rozwija się w celu zabezpieczenia przez organ publiczny lub inną osobę fizyczną lub prawną istotnego 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 zapewnienia zgodności z co najmniej jednym 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 wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, określone w art. 35 rozporządzenia (UE) 2016/679 i art. 39 rozporządzenia (UE) 2018/1725, jakie może wystąpić w trakcie przeprowadzania doświadczeń w ramach piaskownicy, a także mechanizmy reagowania zapewniające możliwość szybkiego ograniczenia tego ryzyka 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, a dostęp do tych danych posiadają wyłącznie upoważnione osoby;

e) dostawcy mogą udostępniać dalej pierwotnie zebrane dane wyłącznie zgodnie z prawem Unii o ochronie danych; wszelkie dane osobowe stworzone w piaskownicy nie mogą być udostępniane poza piaskownicą;

f) przetwarzanie danych osobowych w kontekście piaskownicy nie prowadzi do wdrożenia środków lub podjęcia decyzji wywierających wpływ na osoby, których dane dotyczą, ani nie wpływa na stosowanie ich praw określonych w prawie Unii o ochronie danych osobowych;

g) 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, o ile prawo Unii lub prawo krajowe nie 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 streszczenie projektu w zakresie AI rozwiniętego w ramach piaskownicy, jego celów i oczekiwanych rezultatów zostało opublikowane na stronie internetowej właściwych organów; obowiązek ten nie obejmuje wrażliwych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych.

2. Do celów zapobiegania przestępstwom, prowadzenia postępowań przygotowawczych w ich sprawie, ich wykrywania lub ścigania lub wykonywania kar, 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 prawa Unii lub prawa krajowego 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 rozwoju, testowania lub trenowania innowacyjnych systemów AI lub jakiekolwiek inne podstawy prawnej, zgodnych 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.

Komisja określa w drodze aktów wykonawczych szczegółowe elementy planu testów w warunkach rzeczywistych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 98 ust. 2.

Niniejszy ustęp pozostaje bez uszczerbku dla przepisów prawa Unii lub prawa krajowego dotyczących testów w warunkach rzeczywistych systemów AI wysokiego ryzyka powiązanych z produktami objętymi unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I.

2. Dostawcy lub potencjalni dostawcy mogą przeprowadzać testy systemów AI wysokiego ryzyka, o których mowa w załączniku III, w warunkach rzeczywistych w dowolnym momencie przed wprowadzeniem systemu AI do obrotu lub oddaniem go do użytku, samodzielnie lub we współpracy z co najmniej jednym podmiotem stosującym lub potencjalnym podmiotem stosującym.

3. Testy systemów AI wysokiego ryzyka w warunkach rzeczywistych przeprowadzane na podstawie niniejszego artykułu pozostają bez uszczerbku dla oceny etycznej wymaganej prawem Unii lub prawem 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) organ nadzoru rynku w państwie członkowskim, w którym mają być przeprowadzone 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 terminie 30 dni, testy w warunkach rzeczywistych i plan testów w warunkach rzeczywistych uznaje się za zatwierdzone; w przypadku gdy prawo krajowe nie przewiduje milczącego zatwierdzenia, testy w warunkach rzeczywistych nadal wymagają 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 zgodnie z art. 71 ust. 4 pod ogólnounijnym niepowtarzalnym numerem identyfikacyjnym, podając informacje określone w załączniku IX; dostawca lub potencjalny dostawca 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 – zarejestrował testy w warunkach rzeczywistych w niepublicznej części bazy danych UE zgodnie z art. 49 ust. 4 lit. d), pod ogólnounijnym niepowtarzalnym numerem identyfikacyjnym, podając informacje określone w przywołanym przepisie; dostawca lub potencjalny dostawca systemów AI wysokiego ryzyka, o których mowa w załączniku III pkt 2, zarejestrował testy w warunkach rzeczywistych zgodnie z art. 49 ust. 5;

d) dostawca lub potencjalny dostawca przeprowadzający testy w warunkach rzeczywistych ma siedzibę w Unii lub ustanowił 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 dodatkowy okres sześciu miesięcy, z zastrzeżeniem uprzedniego powiadomienia organu nadzoru rynku przez dostawcę lub potencjalnego dostawcę, wraz z uzasadnieniem konieczności takiego przedłużenia;

g) uczestnicy testów w warunkach rzeczywistych, którzy z uwagi na swój wiek, niepełnosprawność są osobami, które należą do grup szczególnie wrażliwych lub są w odpowiednio chronieni;

h) w przypadku gdy dostawca lub potencjalny dostawca organizuje testy w warunkach rzeczywistych we współpracy z jednym podmiotem stosującym lub potencjalnym podmiotem stosującym, podmiot stosujący lub potencjalny podmiot stosujący został 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 podmiot stosujący lub potencjalny podmiot stosujący zawierają umowę określającą ich role i zakres odpowiedzialności w celu zapewnienia zgodności z przepisami dotyczącymi testów w warunkach rzeczywistych na podstawie niniejszego rozporządzenia oraz na podstawie innego mającego zastosowanie prawa Unii i prawa 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 musza zostać usunięte po przeprowadzeniu testów;

j) testy w warunkach rzeczywistych są skutecznie nadzorowane przez dostawcę lub potencjalnego dostawcę i podmioty stosujące lub potencjalne podmioty stosujące 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 się w dowolnym momencie z testów poprzez odwołanie świadomej zgody; mogą oni również zażądać natychmiastowego i trwałego usunięcia ich danych osobowych. Odwołanie świadomej zgody nie wpływa na już przeprowadzone działania.

6. Zgodnie z art. 75 państwa członkowskie powierzają swoim organom nadzoru rynku uprawnienia do zwracania się do dostawców i potencjalnych dostawców z wnioskiem o przedstawienie informacji, do przeprowadzania niezapowiedzianych zdalnych kontroli lub kontroli na miejscu oraz kontroli przeprowadzania testów w warunkach rzeczywistych i powiązanych systemów AI. 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 szybkiego wycofania systemu AI z użytku 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 mających zastosowanie przepisów prawa Unii i prawa krajowego dotyczących odpowiedzialności, odpowiedzialność za wszelkie szkody spowodowane w trakcie testów w warunkach rzeczywistych.

Artykuł 61

Świadoma zgoda na udział 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 zabezpieczeniach 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, 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 niniejszym ustępie, 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, podmiotów stosujących 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, podmiotami stosującymi, 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 wysokość tych opłat 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 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 zapewnienia 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 lub obowiązków ustanowionych 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 poziomie 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 na podstawie niniejszego rozporządzenia Urzędowi ds. AI.

Artykuł 65

Ustanowienie i struktura Europejskiej Rady ds. Sztucznej Inteligencji

1. Ustanawia się Europejską Radę ds. Sztucznej Inteligencji (zwaną dalej „Radą 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 władze, organy lub ekspertów, w przypadku gdy omawiane kwestie są dla nich istotne.

3. 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, 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 zbieranie 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 ustanawia dwie stałe podgrupy służące jako platforma współpracy i wymiany między organami nadzoru rynku oraz powiadamiające organy w kwestiach 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.

W stosownych przypadkach Rada ds. AI może utworzyć 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 wniosek 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 zainteresowanych organów 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 w tym zakresie 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 w zakresie AI oraz testów w warunkach rzeczywistych, o których mowa w art. 57, 59 i 60;

e) na wniosek Komisji lub z własnej inicjatywy wydawać zalecenia i opinie na piśmie na temat wszelkich istotnych zagadnień związanych z wdrażaniem niniejszego rozporządzenia oraz z jego spójnym i skutecznym stosowaniem, w tym:

   (i) w zakresie opracowywania 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 UE, o której mowa w art. 71, przygotowania aktów delegowanych lub wykonawczych oraz w odniesieniu do ewentualnego dostosowania niniejszego rozporządzenia do unijnego prawodawstwa harmonizacyjnego wymienionego 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, upowszechnianie 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 kompetencje w zakresie AI, świadomości społecznej oraz zrozumienia w odniesieniu do korzyści, ryzyka, zabezpieczeń, praw i obowiązków związanych z wykorzystaniem systemów AI;

g) ułatwiać opracowywanie wspólnych kryteriów i wspólnego rozumienia przez podmioty gospodarcze i właściwe organy odpowiednich koncepcji 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 w zakresie AI oraz ułatwiać współpracę i wymianę informacji między piaskownicami regulacyjnymi w zakresie AI;

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 dobór 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 powołuje członków forum doradczego spośród zainteresowanych stron, którzy dysponują 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. Forum doradcze 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 uwagi na piśmie.

9. W stosownych przypadkach forum doradcze może utworzyć 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 (zwanego dalej „panelem naukowym"), 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 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 ewentualnym ryzyku systemowym na poziomie Unii związanym z modelami AI ogólnego przeznaczenia;

   (ii) przyczynianie się do opracowywania 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 unijnej procedury 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 interesów, którą podaje się do wiadomości publicznej. Urząd ds. AI ustanawia systemy i procedury mające na celu aktywne zarządzanie i zapobieganie potencjalnym konfliktom interesów.

5. Akt wykonawczy, o którym mowa w ust. 1, zawiera przepisy dotyczące warunków, procedur i szczegółowych zasad 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 zespołu ekspertów

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 wysokość 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 wolny od uprzedzeń, 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 obowiązków. 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. Do dnia 2 sierpnia 2025 r. państwa członkowskie podają, do wiadomości publicznej, za pośrednictwem środków komunikacji elektronicznej, informacje o sposobach kontaktowania się z właściwymi organami i pojedynczymi punktami kontaktowymi. Państwa członkowskie wyznaczają organ nadzoru rynku do działania w charakterze 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 zapewniają, 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, ryzyka 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 podejmują odpowiednie środki w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa.

5. Wykonując swoje zadania, właściwe organy krajowe działają zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 78.

6. Do dnia 2 sierpnia 2025 r., a następnie co dwa lata państwa członkowskie przekazują Komisji sprawozdania dotyczące stanu zasobów finansowych i ludzkich właściwych organów krajowych wraz z oceną ich odpowiedniości. 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. W każdym przypadku gdy właściwe organy krajowe zamierzają udzielić wskazówek i porad dotyczących systemu AI w dziedzinach objętych innymi przepisami prawa Unii, są zobowiązane – w stosownych przypadkach –zasięgnąć opinii właściwych organów krajowych wyznaczonych na podstawie tych przepisów prawa Unii.

9. W przypadku gdy instytucje, organy i jednostki organizacyjne Unii są objęte zakresem niniejszego rozporządzenia, Europejski Inspektor Ochrony Danych działa w charakterze właściwego organu odpowiedzialnego za sprawowanie nad nimi nadzoru.

ROZDZIAŁ VIII

BAZA DANYCH UE DLA SYSTEMÓW AI WYSOKIEGO RYZYKA

Artykuł 71

Baza danych UE dla systemów AI wysokiego ryzyka wymienionych w załączniku III

1. Komisja – we współpracy z państwami członkowskimi – tworzy i prowadzi bazę danych UE 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 zostały zarejestrowane zgodnie z art. 49 i 60 oraz systemów AI, których nie uznaje się za systemy AI wysokiego ryzyka na podstawie art. 6 ust. 3 i które zostały zarejestrowane zgodnie z art. 6 ust. 4 i art. 49. 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 sekcje A i B są wprowadzane do bazy danych UE przez dostawcę lub – w stosownych przypadkach – przez upoważnionego przedstawiciela.

3. Dane wymienione w załączniku VIII sekcja C są wprowadzane do bazy danych UE przez podmiot stosujący będący organem publicznym, agencją lub jednostką organizacyjną zgodnie z art. 49 ust. 3 i 4, 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. 4 lit. c), informacje zawarte w bazie danych UE 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 ogółowi społeczeństwa.

5. Baza danych UE zawiera dane osobowe wyłącznie w zakresie, w jakim jest to konieczne do celów związanych ze zbieraniem i przetwarzaniem informacji zgodnie z niniejszym rozporządzeniem. Informacje te obejmują imiona i nazwiska oraz dane kontaktowe osób fizycznych, które są odpowiedzialne za rejestrację systemu i są upoważnione do reprezentowania dostawcy lub, w stosownych przypadkach, podmiotu stosującego.

6. Komisja pełni funkcję administratora bazy danych UE. Komisja zapewnia dostawcom, potencjalnym dostawcom oraz podmiotom stosującym odpowiednie wsparcie techniczne i administracyjne. Baza danych UE musi być zgodna z mającymi zastosowanie wymogami dostępności.

ROZDZIAŁ IX

MONITOROWANIE PO WPROWADZENIU DO OBROTU, WYMIANA INFORMACJI ORAZ 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 z wykorzystaniem 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 zbiera 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 lub mogą być zbierane z innych źródeł; system ten pozwala dostawcy oceniać, czy zapewniona jest ciągła zgodność systemów AI z wymogami ustanowionymi 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 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. Do dnia 2 lutego 2026 r. Komisja przyjmuje akt wykonawczy zawierające szczegółowe przepisy określające wzór planu monitorowania po wprowadzeniu do obrotu oraz wykaz elementów, które należy zawrzeć w tym planie. 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 zapewnia ono równoważny poziom ochrony.

Akapit pierwszy niniejszego artykułu stosuje się również 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 przepisów prawa Unii 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 Unii zgłaszają wszelkie poważne incydenty organom nadzoru rynku tego państwa członkowskiego, w którym wystąpił dany incydent.

2. Zgłoszenia, o którym mowa w ust. 1, dokonuje się natychmiast po ustaleniu przez dostawcę związku przyczynowego między systemem AI a poważnym incydentem lub dostatecznie wysokiego prawdopodobieństwa wystąpienia takiego związku, nie później jednak niż w terminie 15 dni od dnia, w którym dostawca lub, w stosownych przypadkach, podmiot stosujący dowiedzieli się o wystąpieniu poważnego incydentu.

Termin na dokonanie zgłoszenia, o którym mowa w akapicie pierwszym, uwzględnia dotkliwość danego poważnego incydentu.

3. Niezależnie od ust. 2 niniejszego artykułu w przypadku powszechnego naruszenia lub poważnego incydentu zdefiniowanego w art. 3 pkt 49 lit. b) zgłoszenia, o którym mowa w ust. 1 niniejszego artykułu, dokonuje się natychmiast, nie później jednak niż w terminie dwóch dni od dnia, w którym dostawca lub, w stosownych przypadkach, podmiot stosujący dowiedzieli się o wystąpieniu tego incydentu.

4. Niezależnie od ust. 2 w przypadku gdy nastąpi śmierć osoby, zgłoszenia dokonuje się natychmiast po stwierdzeniu przez dostawcę lub podmiot stosujący wystąpienia lub podejrzenia wystąpienia 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.

5. W przypadku gdy jest to konieczne do zapewnienia terminowego zgłoszenia, dostawca lub, w stosownych przypadkach, podmiot stosujący mogą dokonać niepełnego zgłoszenia wstępnego, a następnie zgłoszenia kompletnego.

6. 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.

7. Po otrzymaniu zgłoszenia dotyczącego poważnego incydentu, o którym mowa w art. 3 pkt 49 lit. c), odpowiedni organ nadzoru rynku informuje o tym krajowe organy lub podmioty publiczne, o których mowa w art. 77 ust. 1. Komisja opracowuje specjalne wskazówki ułatwiające spełnienie obowiązków ustanowionych w ust. 1 niniejszego artykułu. Wskazówki wydaje się do dnia 2 sierpnia 2025 r. i podlegają one regularnej ocenie.

8. W terminie siedmiu dni od daty otrzymania powiadomienia, o którym mowa w ust. 1 niniejszego artykułu, organ nadzoru rynku podejmuje odpowiednie środki przewidziane w art. 19 rozporządzenia (UE) 2019/1020 i postępuje zgodnie z procedurami powiadamiania przewidzianymi w tym rozporządzeniu.

9. 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 49 lit. c).

10. W przypadku systemów AI wysokiego ryzyka, które są 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 49) lit. c) niniejszego rozporządzenia, i dokonuje się go do właściwego organu krajowego wybranego do tego celu przez państwo członkowskie, w którym wystąpił dany incydent.

11. Właściwe organy krajowe natychmiast 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. Do systemów AI objętych niniejszym rozporządzeniem stosuje się 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 stosowania niniejszego rozporządzenia.

2. W ramach swoich obowiązków w zakresie sprawozdawczości określonych w 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 one sprawozdania również Komisji dotyczące stwierdzonego w danym roku stosowania zakazanych praktyk oraz podjętych w tym względzie środków.

3. W przypadku systemów AI wysokiego ryzyka, które są powiązane 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 akapitu pierwszego i w odpowiednich okolicznościach państwa członkowskie mogą wyznaczyć do działania w charakterze organu nadzoru rynku inny odpowiedni organ, pod warunkiem że zapewnią koordynację między odpowiednimi sektorowymi organami nadzoru rynku odpowiedzialnymi za egzekwowanie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I.

4. Procedur, o których mowa w art. 79–83 niniejszego rozporządzenia, nie stosuje się do systemów AI, które są powiązane 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 stosuje się procedury sektorowe.

5. Bez uszczerbku dla uprawnień organów nadzoru rynku na podstawie art. 14 rozporządzenia (UE) 2019/1020 do celów zapewnienia skutecznego egzekwowania przepisów 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 wprowadzonych do obrotu, oddanych do użytku lub wykorzystywanych przez instytucje finansowe podlegające przepisom prawa Unii dotyczącym usług finansowych organem nadzoru rynku do celów niniejszego rozporządzenia jest odpowiedni organ krajowy odpowiedzialny na mocy tych przepisów prawa 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 w dyrektywie 2013/36/UE, które uczestniczą w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem (UE) nr 1024/2013, powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zebrane w trakcie prowadzonych przez siebie działań w zakresie nadzoru rynku, które potencjalnie mogą mieć znaczenie z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego.

8. W odniesieniu do systemów AI wysokiego ryzyka wymienionych w załączniku III pkt 1 do niniejszego rozporządzenia, 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 wyznaczają jako organy nadzoru rynku do celów niniejszego rozporządzenia właściwe organy nadzorcze ds. ochrony danych na podstawie rozporządzenia (UE) 2016/679 lub dyrektywy (UE) 2016/680 albo inne organy wyznaczone 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 czynności związanych ze sprawowaniem przez nie wymiaru sprawiedliwości.

9. W przypadku gdy zakresem stosowania niniejszego rozporządzenia objęte są instytucje, organy i jednostki organizacyjne Unii, Europejski Inspektor Ochrony Danych działa w stosunku do nich w charakterze organu nadzoru rynku, z wyjątkiem Trybunał Sprawiedliwości Unii Europejskiej w przypadkach sprawowania przez niego sprawiedliwości.

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 w innych przepisach prawa 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 w rozporządzeniu (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 rozwoju 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 na ich uzasadniony wniosek dostępu do kodu źródłowego systemu AI wysokiego ryzyka 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 ustanowionymi 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 zostały rozwinięte 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 zadań w zakresie monitorowania i nadzoru Urząd ds. AI ma uprawnienia organu nadzoru rynku przewidziane w niniejszej sekcji i w rozporządzeniu (UE) 2019/1020.

2. W przypadku gdy odpowiednie organy nadzoru rynku mają wystarczające powody, by systemy AI ogólnego przeznaczenia, które mogą być wykorzystywane bezpośrednio przez podmioty stosujące do co najmniej jednego celu, który zgodnie z niniejszym rozporządzeniem został zaklasyfikowany 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 pozostałe organy nadzoru rynku.

3. W przypadku gdy 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 ogólnego przeznaczenia 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. 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 w celu 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. 58 organy nadzoru rynku weryfikują zgodność z 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 ustanowionych 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 ustanowione 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 oraz podmiot stosujący i potencjalny podmiot stosujący 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. W przypadku gdy organ nadzoru rynku podjął decyzję, o której mowa w ust. 3, informuje w stosownych przypadkach 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 w zakresie ochrony praw podstawowych, w tym prawa do niedyskryminacji, w odniesieniu do wykorzystywania systemów AI wysokiego ryzyka, o których mowa w załączniku III, są uprawnione do wystąpienia z wnioskiem o przedstawienie 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 właściwości. Odpowiedni organ lub podmiot publiczny informuje organ nadzoru rynku zainteresowanego państwa członkowskiego o każdym takim wniosku.

2. Do dnia 2 listopada 2024 r. każde państwo członkowskie wskazuje organy lub podmioty publiczne, o których mowa w ust. 1, i podaje 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 prawa Unii w zakresie 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 wystąpiły z wnioskiem.

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 przestrzegają, zgodnie z prawem Unii lub prawem krajowym, poufności informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności, aby w szczególności chronić:

a) prawa własności intelektualnej oraz poufne informacje handlowe lub tajemnice przedsiębiorstwa osoby fizycznej lub prawnej, w tym kod źródłowy, z wyjątkiem przypadków, o których mowa w art. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 ([57]);

b) skuteczne wdrożenie niniejszego rozporządzenia, w szczególności na potrzeby kontroli, postępowań lub audytów;

c) interesy bezpieczeństwa publicznego i narodowego;

d) przebieg postępowań karnych i administracyjnych;

e) informacje niejawne zgodnie z prawem Unii lub prawem krajowym.

2. Organy zaangażowane w stosowanie niniejszego rozporządzenia zgodnie z ust. 1 zwracają się z wnioskiem o przedstawienie wyłącznie takich danych, które są im bezwzględnie konieczne do oceny ryzyka stwarzanego przez systemy AI i do wykonywania ich uprawnień zgodnie z niniejszym rozporządzeniem i z rozporządzeniem (UE) 2019/1020. Wprowadzają one odpowiednie i skuteczne środki w zakresie cyberbezpieczeństwa, aby chronić bezpieczeństwo i poufność uzyskanych informacji i danych oraz usuwają zebrane dane, gdy tylko przestaną one być potrzebne do celu, w jakim je uzyskano, zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym.

3. Bez uszczerbku dla 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, w przypadku gdy systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7, wykorzystują 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 wrażliwych 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 wniosek 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 nie mają wpływu na prawa i obowiązki Komisji, państw członkowskich i ich odpowiednich organów, a także jednostek notyfikowanych, w zakresie wymiany informacji i rozpowszechnianie ostrzeżeń, w tym w kontekście współpracy transgranicznej; nie mają one również wpływu 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 osób.

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 względem jego zgodności ze wszystkimi wymogami i obowiązkami ustanowionymi w niniejszym rozporządzeniu. Szczególną uwagę należy zwrócić na systemy AI stwarzające ryzyko dla grup szczególnie wrażliwych. W przypadku gdy zostanie stwierdzone ryzyko dla praw podstawowych, organ nadzoru rynku informuje o tym również odpowiednie krajowe organy lub podmioty publiczne, o których mowa w art. 77 ust. 1, i współpracuje z nimi w pełnym zakresie. Odpowiedni operatorzy współpracują w razie potrzeby z organem nadzoru rynku i innymi krajowymi organami lub podmiotami publicznymi, o których mowa w art. 77 ust. 1.

([57]) 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).

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, ustalą, że system AI nie jest zgodny z wymogami i obowiązkami ustanowionymi w niniejszym rozporządzeniu, bez zbędnej zwłoki zobowiązuje odpowiedniego operatora do podjęcia wszelkich odpowiednich działań naprawczych, aby zapewnić zgodność tego systemu AI z wymogami, wycofać ten system z rynku lub z użytku w terminie, który może zostać wyznaczony przez organ nadzoru rynku, 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, stosuje się art. 18 rozporządzenia (UE) 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 systemów AI, które udostępnił na rynku Unii.

5. W przypadku niepodjęcia przez operatora systemu AI odpowiednich działań naprawczych w terminie, o którym mowa w ust. 2, organ nadzoru rynku podejmuje 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 z użytku. 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 niezgodności systemu AI, pochodzenie systemu AI i informacje na temat jego łańcucha dostaw, charakter zarzucanej niezgodności i związanego z nią ryzyka, charakter i okres obowiązywania podjętych środków krajowych oraz argumenty przedstawione przez odpowiedniego operatora. W szczególności organy nadzoru rynku wskazują, czy niezgodność wynika z 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) niezgodności z art. 50.

7. Organy nadzoru rynku 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 danego systemu AI, a w przypadku gdy nie zgadzają się ze środkiem krajowym, o którym zostały powiadomione – o swoim sprzeciwie.

8. W przypadku gdy w terminie trzech miesięcy od dnia powiadomienia, o którym mowa w ust. 5 niniejszego artykułu, 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 niniejszego rozporządzenia.

9. Organy nadzoru rynku zapewniają, by bez zbędnej zwłoki zostały podjęte odpowiednie środki ograniczające w odniesieniu do danego produktu lub systemu AI, takie jak wycofanie produktu lub systemu AI z podległego im rynku.

Artykuł 80

Procedura postępowania w przypadku systemów AI zaklasyfikowanych 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 zaklasyfikowany 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 ustanowionych w art. 6 ust. 3 i wytycznych Komisji.

2. W przypadku gdy w trakcie tej oceny organ nadzoru rynku ustali, że dany system AI jest systemem wysokiego ryzyka, bez zbędnej zwłoki zobowiązuje danego dostawcę do 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, który może zostać wyznaczony 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 systemów AI, które udostępnił na rynku Unii.

6. W przypadku gdy dostawca danego systemu AI nie podejmie odpowiednich działań naprawczych w terminie, o którym mowa w ust. 2 niniejszego artykułu, stosuje się 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 zaklasyfikowany jako system niebędący systemem wysokiego ryzyka w celu obejścia stosowania wymogów ustanowionych 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 bazie danych UE, 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 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 podjęcie bez zbędnej zwłoki odpowiednich środków ograniczających w odniesieniu do danego systemu AI, takich jak zobowiązujące do wycofania tego systemu AI z ich rynku, oraz informują o tym Komisję. W przypadku gdy Komisja uzna środek krajowy za nieuzasadniony, zainteresowane państwo członkowskie cofa 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 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 ustali, 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 dany system AI po wprowadzeniu do obrotu lub oddaniu do użytku nie stwarzał już takiego ryzyka, w terminie, który może zostać wyznaczony przez ten organ.

2. Dostawca lub inny właściwy operator zapewniają podjęcie działań naprawczych w odniesieniu do wszystkich systemów AI, które udostępnili na rynku Unii, w terminie wyznaczonym przez organ nadzoru rynku państwa członkowskiego, o którym mowa w ust. 1.

3. Państwa członkowskie natychmiast 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 danego systemu AI, pochodzenie systemu AI i informacje na temat jego łańcucha dostaw, charakter przedmiotowego ryzyka oraz charakter i okres obowiązywania podjętych środków krajowych.

4. Komisja bez zbędnej zwłoki przystępuje do konsultacji z zainteresowanymi państwami członkowskim i właściwymi operatorami i ocenia podjęte środki krajowe. Na podstawie wyników tej oceny Komisja podejmuje decyzję, czy środek krajowy jest uzasadniony i w razie potrzeby proponuje inne odpowiednie środki.

5. Komisja natychmiast przekazuje swoją decyzję do zainteresowanych państw członkowskich i operatorów. Komisja powiadamia również pozostałe państwa członkowskie.

Artykuł 83

Niezgodność formalna

1. Organ nadzoru rynku państwa członkowskiego zobowiązuje właściwego dostawcę do usunięcia niezgodności w terminie, który może zostać wyznaczony przez ten organ, w przypadku gdy ustali, że:

a) oznakowanie CE zostało umieszczone z naruszeniem art. 48;

b) oznakowanie CE nie zostało umieszczone;

c) deklaracja zgodności UE, o której mowa w art. 47, nie została sporządzona;

d) deklaracja zgodności UE, o której mowa w art. 47, została sporządzona nieprawidłowo;

e) rejestracja w bazie danych, o której mowa w art. 71, UE nie została dokonana;

f) upoważniony przedstawiciel nie został, w stosownych przypadkach, ustanowiony;

g) brakuje dokumentacji technicznej.

2. W przypadku gdy niezgodność, o której mowa w ust. 1, utrzymuje się, krajowy organ nadzoru rynku zainteresowanego państwa członkowskiego podejmuje 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) 2019/1020.

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 skargę do odpowiedniego organu nadzoru rynku.

Zgodnie z rozporządzeniem (UE) 2019/1020 takie skargi bierze się pod uwagę do celów prowadzenia działań w zakresie nadzoru rynku i rozpatruje się je zgodnie ze specjalnymi procedurami ustanowionymi w związku z tym przez organy nadzoru rynku.

Artykuł 86

Prawo do uzyskania wyjaśnienia na temat procedury podejmowania decyzji w indywidualnej sprawie

1. Każda osoba, na którą AI ma wpływ, będąca przedmiotem decyzji podjętej przez podmiot stosujący na podstawie wyników systemu AI wysokiego ryzyka wymienionego w załączniku III, z wyjątkiem systemów wymienionych w pkt 2 tego załącznika, która to decyzja wywołuje 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 jasnego i merytorycznego wyjaśnienia roli tego systemu AI w procedurze podejmowania decyzji oraz głównych elementów podjętej decyzji.

2. Ust. 1 nie stosuje się do wykorzystywania systemów AI, w odniesieniu do których z prawa Unii lub zgodnego z prawem Unii prawa krajowego wynikają wyjątki lub ograniczenia dotyczące stosowania obowiązku ustanowionego w tym ustępie.

3. Niniejszy artykuł stosuje się jedynie w zakresie, w jakim prawo, o którym mowa w ust. 1, nie zostało inaczej ustanowione w prawie Unii.

Artykuł 87

Zgłaszanie naruszeń i ochrona osób dokonujących zgłoszeń

Do zgłaszania naruszeń niniejszego rozporządzenia oraz w kwestiach ochrony osób zgłaszających takie naruszenia stosuje się 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 jest 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 podejmować działania niezbędne do monitorowania skutecznego wdrożenia i zapewnienia zgodności z niniejszym rozporządzeniem 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, stosowne 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 warunki, 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 uprawnienia ustanowione w niniejszej sekcji do celów oceny danej sprawy. 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 z wnioskiem o przedstawienie dokumentacji i informacji

1. Komisja może zwrócić się do dostawcy danego modelu AI ogólnego przeznaczenia z wnioskiem o przedstawienie dokumentacji sporządzonej przez niego zgodnie art. 53 i 55 lub wszelkich dodatkowych informacji niezbędnych do celów oceny zgodności 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 przedstawienie informacji, w przypadku gdy dostęp do informacji jest niezbędny i proporcjonalny do realizacji zadań panelu naukowego na podstawie art. 68 ust. 2.

4. We wniosku o przekazanie informacji wskazuje się podstawę prawną i cel wniosku, podaje, jakie informacje stanowią przedmiot wniosku oraz określa się termin na przekazanie tych informacji, a także wskazuje przewidziane w art. 101 kary pieniężne za dostarczenie informacji nieprawidłowych, niekompletnych lub wprowadzających w błąd.

5. Dostawca danego modelu AI ogólnego przeznaczenia lub jego przedstawiciel dostarczają informacje stanowiące przedmiot wniosku. 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 w imieniu dostawcy danego modelu AI ogólnego przeznaczenia informacje stanowiące przedmiot wniosku. Prawnicy należycie upoważnieni do działania mogą dostarczać informacje w imieniu swoich klientów. Klienci ponoszą jednak pełną odpowiedzialność, jeśli dostarczone 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 spełniania 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 ostrzeżenia kwalifikowanego panelu naukowego zgodnie z art. 90 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 muszą spełniać kryteria określone w art. 68 ust. 2.

3. Do celów ust. 1 Komisja może zwrócić się z wnioskiem o udzielenie dostępu 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 wskazuje 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 ich przedstawiciele dostarczają informacji stanowiących przedmiot wniosku. W przypadku osób prawnych, spółek lub firm lub w przypadku gdy dostawca nie posiada osobowości prawnej, osoby upoważnione do ich reprezentowania z mocy prawa lub na podstawie aktu założycielskiego udzielają w imieniu danego dostawcy modelu AI ogólnego przeznaczenia dostępu stanowiącego przedmiot wniosku.

6. Komisja przyjmuje akty wykonawcze określające szczegółowe zasady i warunki przeprowadzania ocen, w tym szczegółowe zasady 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 wystąpieniem z wnioskiem o udzielenie dostępu 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 w celu zapobieżenia ryzyku systemowemu oraz innych wewnętrznych procedur i środków, jakie dostawca podjął w celu ograniczenia takiego ryzyka.

Artykuł 93

Uprawnienia do żądania podjęcia środków

1. W miarę konieczności i w stosownych przypadkach Komisja może zwrócić się do dostawców z żądaniem dotyczącym:

a) podjęcia odpowiednich środków w celu spełnienia obowiązków określonych w art. 53 i 54;

b) wdrożenia środków zaradczych, w przypadku gdy z oceny przeprowadzonej zgodnie z art. 92 wynika poważna i uzasadniona obawa wystąpienia ryzyka systemowego na poziomie Unii;

c) ograniczenia udostępniania modelu na rynku, wycofania modelu z rynku lub z użytku.

2. Przed wystąpieniem z żądaniem podjęcia 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 wdrożenia 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 będących dostawcami modeli AI ogólnego przeznaczenia

Art. 18 rozporządzenia (UE) 2019/1020 stosuje się odpowiednio do dostawców modeli AI ogólnego przeznaczenia, bez uszczerbku dla bardziej szczególnych 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 zachęcają do opracowywania kodeksów postępowania, w tym powiązanych mechanizmów zarządzania, i ułatwiają opracowywanie takich kodeksów, których celem jest propagowanie dobrowolnego stosowania w odniesieniu do systemów AI niebędących systemami wysokiego ryzyka niektórych lub wszystkich wymogów ustanowionych 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 ułatwiają opracowywanie kodeksów postępowania dotyczących dobrowolnego stosowania, również przez podmioty stosujące, szczególnych wymogów w odniesieniu do wszystkich systemów AI, na podstawie jasnych celów i kluczowych wskaźników skuteczności działania służących do pomiaru stopnia realizacji tych celów, w tym między innymi następujących elementów:

a) mające zastosowanie elementy przewidziane w unijnych wytycznych etycznych dotyczących godnej zaufania AI;

b) ocena i minimalizacja oddziaływania 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 rozwojem, działaniem 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, w tym przy udziale 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 opracowywania kodeksów postępowania i ułatwiania ich opracowywania 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 pkt 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 może mieć największy wpływ.

Wytyczne, o których mowa w akapicie pierwszym niniejszego ustępu, 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 wcześniej wytyczne, jeżeli zostanie to uznane za konieczne.

ROZDZIAŁ XI

PRZEKAZANIE UPRAWNIEŃ I PROCEDURA KOMITETOWA

Artykuł 97

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 6 ust. 6 i 7, 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 1 sierpnia 2024 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem 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 i 7, 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 lub 7, art. 7 ust. 1 lub 3, art. 11 ust. 3, art. 43 ust. 5 lub 6, art. 47 ust. 5, art. 51 ust. 3, art. 52 ust. 4 lub art. 53 ust. 5 lub 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 przepisów niniejszego rozporządzenia przez operatorów i podejmują wszelkie niezbędne środki w celu zapewnienia ich właściwego i skutecznego wykonywania, 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 sprawcą naruszenia jest 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. Nieprzestrzeganie któregokolwiek z przepisów dotyczących operatorów lub jednostek notyfikowanych, innych niż przepisy ustanowione w art. 5, podlega administracyjnej karze pieniężnej w wysokości do 15 000 000 EUR lub – jeżeli sprawcą naruszenia jest 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 zgodnie z art. 26;

f) wymogi i obowiązki jednostek notyfikowanych zgodnie z art. 31, art. 33 ust. 1, 3 i 4 lub art. 34;

g) obowiązki dostawców i podmiotów stosujących w zakresie przejrzystości zgodnie z art. 50.

5. Dostarczanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym lub właściwym organom krajowym w odpowiedzi na ich wniosek podlega administracyjnej karze pieniężnej w wysokości do 7 500 000 EUR lub – jeżeli sprawcą naruszenia jest 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, wysokość kary pieniężnej, o której mowa w niniejszym artykule, nie przekracza wartości procentowej lub kwoty, o których mowa w ust. 3, 4 i 5, w zależności od tego, która z tych kwot jest niższa.

7. Przy podejmowaniu decyzji o nałożeniu administracyjnej kary pieniężnej, oraz przy ustalaniu jej wysokości w każdej indywidualnej sprawie, 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 konsekwencji, przy uwzględnieniu przeznaczenia systemu AI, a także, w stosownych przypadkach, liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody;

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

c) to, 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 odpowiednie 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 powiązane bezpośrednio lub pośrednio z danym naruszeniem osiągnięte korzyści finansowe lub uniknięte straty;

f) stopień współpracy z właściwymi organami krajowymi 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 uprawnień na podstawie 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 o nałożeniu administracyjnej kary pieniężnej 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, w stosownych przypadkach, liczby poszkodowanych osób oraz rozmiaru poniesionej przez nie szkody;

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 w zakresie 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 sprawie 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, muszą zostać 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 rocznego światowego obrotu w poprzednim roku obrotowym lub 15 000 000 EUR, w zależności od tego, która z tych kwot jest wyższa, jeśli ustali, że dostawca celowo lub w wyniku zaniedbania:

a) naruszył odpowiednie przepisy niniejszego rozporządzenia;

b) nie zastosował się do wniosku o przedstawienie dokumentu lub informacji zgodnie z art. 91 lub dostarczył 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 na podstawie ust. 1 Komisja przekazuje swoje wstępne ustalenia dostawcy modelu AI ogólnego przeznaczenia i daje mu możliwość bycia wysłuchanym.

3. Kary pieniężne nakładane zgodnie z niniejszym artykułem muszą być 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 przeprowadzania kontroli decyzji Komisji ustalających karę pieniężną na podstawie niniejszego artykułu. Trybunał Sprawiedliwości Unii Europejskiej może uchylić, obniżyć lub podwyższyć nałożoną karę pieniężną.

6. Komisja przyjmuje akty wykonawcze zawierające szczegółowe zasady oraz zabezpieczenia proceduralne dotyczące postępowania w celu ewentualnego przyjęcia decyzji na podstawie 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 zatwierdzania sprzętu służącego do ochrony i korzystania z niego w przypadku systemów AI w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 (*) uwzględnia się wymogi ustanowione w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

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) 2024/1689 (*), uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

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) 2024/1689 (*), uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

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) 2024/1689 (*), 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 rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

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) 2024/1689 (*), uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

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) 2024/1689 (*), uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

Artykuł 108

Zmiany w rozporządzeniu (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) 2024/1689 (*), uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”;

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) 2024/1689, uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.”;

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

„4. Przy przyjmowaniu aktów wykonawczych na podstawie ust. 1 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia (UE) 2024/1689, uwzględnia się wymogi określone w rozdziale III sekcja 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) 2024/1689, uwzględnia się wymogi określone w rozdziale III sekcja 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) 2024/1689, uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.”;

6) w art. 58 dodaje się ustęp w brzmieniu:

„3. Przy przyjmowaniu aktów delegowanych na podstawie ust. 1 i 2 dotyczących systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami w rozumieniu rozporządzenia (UE) 2024/1689, uwzględnia się wymogi określone w rozdziale III sekcja 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) 2024/1689 (*), uwzględnia się wymogi określone w rozdziale III sekcja 2 tego rozporządzenia.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”;

Artykuł 110

Zmiana dyrektywy (UE) 2020/1828

W załączniku I do dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/1828 ([58]) dodaje się punkt w brzmieniu:

„(68) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).”.

Artykuł 111

Systemy AI już wprowadzone do obrotu lub oddane do użytku oraz modele AI ogólnego przeznaczenia już wprowadzone do obrotu

1. Bez uszczerbku dla stosowania art. 5 zgodnie z art. 113 akapit trzeci 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 2 sierpnia 2027 r.

Wymogi ustanowione w niniejszym rozporządzeniu uwzględnia się w ocenach każdego 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 zgodnie z art. 113 akapit trzeci lit. a) niniejsze rozporządzenie stosuje się 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 2 sierpnia 2026 r. tylko wtedy, gdy po tej dacie w systemach tych wprowadzane będą istotne zmiany w ich projekcie. W każdym razie dostawcy systemów AI wysokiego ryzyka i podmioty stosujące takie systemy, które są przeznaczone do wykorzystywania przez organy publiczne, podejmują niezbędne kroki w celu zapewnienia zgodności z wymogami i spełnienia obowiązków ustanowionych w niniejszym rozporządzeniu do dnia 2 sierpnia 2030 r.

3. Dostawcy modeli AI ogólnego przeznaczenia, które zostały wprowadzone do obrotu przed dniem 2 sierpnia 2025 r., podejmują niezbędne kroki w celu spełnienia obowiązków ustanowionych w niniejszym rozporządzeniu do dnia 2 sierpnia 2027 r.

([58]) 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 112

Ocena i przegląd

1. Komisja ocenia potrzebę wprowadzenia zmian w wykazie zawartym w załączniku III oraz w ustanowionym w art. 5 wykazie zakazanych praktyk w zakresie AI raz w roku, począwszy od dnia wejścia w życie niniejszego rozporządzenia do końca okresu przekazania uprawnień ustanowionych w art. 97. Komisja przedstawia ustalenia z tej oceny Parlamentowi Europejskiemu i Radzie.

2. Do dnia 2 sierpnia 2028 r., a następnie co cztery lata Komisja przeprowadza ocenę i przedkłada 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 2 sierpnia 2029 r., 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 Unii. 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 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 2 sierpnia 2028 r. Komisja ocenia funkcjonowanie Urzędu ds. AI, 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 egzekucji, a także zwiększenie jego zasobów. Komisja przedkłada sprawozdanie z oceny Parlamentowi Europejskiemu i Radzie.

6. Do dnia 2 sierpnia 2028 r., a następnie co cztery lata, Komisja przedkłada sprawozdanie z przeglądu postępów w opracowywaniu dokumentów normalizacyjnych dotyczących wydajnego pod względem energii rozwoju modeli AI ogólnego przeznaczenia oraz ocenia konieczność podjęcia dalszych środków lub działań, w tym wiążących środków lub działań. Sprawozdanie to przedkłada się Parlamentowi Europejskiemu i Radzie i podaje do wiadomości publicznej.

7. Do dnia 2 sierpnia 2028 r., a następnie co trzy lata Komisja ocenia wpływ i skuteczność dobrowolnych kodeksów postępowania mających na celu propagowanie wymogów ustanowionych w rozdziale III 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 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 określonego w załączniku III, łącznie z rozszerzeniem istniejących nagłówków dotyczących obszarów lub dodaniem nowych nagłówków dotyczących obszarów w tym załączniku;

b) określonego w art. 5 wykazu zakazanych praktyk; oraz

c) wykazu systemów AI wymagających dodatkowych środków w zakresie przejrzystości zgodnie z art. 50.

12. Wszelkie zmiany niniejszego rozporządzenia 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 2 sierpnia 2031 r. Komisja przeprowadza ocenę egzekwowania niniejszego rozporządzenia i przedkłada sprawozdanie z tej oceny Parlamentowi Europejskiemu, Radzie i Europejskiemu Komitetowi Ekonomiczno-Społecznemu, uwzględniając pierwsze lata stosowania niniejszego rozporządzenia. Na podstawie dokonanych 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 Unii.

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 2 sierpnia 2026 r.

Jednakże:

a) rozdziały I i II stosuje się od dnia 2 lutego 2025 r.;

b) rozdział III sekcja 4, rozdział V, rozdział VII i rozdział XII oraz art. 78 stosuje się od dnia 2 sierpnia 2025 r., z wyjątkiem art. 101;

c) art. 6 ust. 1 i odpowiadające mu obowiązki ustanowione w niniejszym rozporządzeniu stosuje się od dnia 2 sierpnia 2027 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 13 czerwca 2024 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	M. MICHEL

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);

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 akapit pierwszy lit. h) ppkt (iii)

Przestępstwa, o których mowa w art. 5 ust. 1 akapit pierwszy lit. h) 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 prawa Unii lub prawa krajowego:

   a) systemy zdalnej identyfikacji biometrycznej.

      Nie obejmuje to systemów AI przeznaczonych do wykorzystania przy weryfikacji biometrycznej, której jedynym celem jest potwierdzenie, że określona osoba fizyczna jest osobą, za którą się podaje;

   b) systemy AI przeznaczone do wykorzystania przy kategoryzacji biometrycznej, według wrażliwych lub chronionych atrybutów lub cech na podstawie wywnioskowania tych atrybutów lub cech;

   c) systemy AI przeznaczone do wykorzystania przy rozpoznawaniu emocji.

2. Infrastruktura krytyczna: systemy AI przeznaczone do wykorzystywania jako związane z bezpieczeństwem elementy procesów zarządzania krytyczną infrastrukturą cyfrową, ruchem drogowym i procesów ich działania lub zaopatrzenia w wodę, gaz, ciepło lub energię elektryczną.

3. Kształcenie i szkolenie zawodowe:

   a) systemy AI przeznaczone do wykorzystywania do celów podejmowania decyzji o dostępie lub przyjęciu do instytucji edukacyjnych i instytucji szkolenia zawodowego lub przydzielania osób do tych instytucji na wszystkich poziomach;

   b) systemy AI przeznaczone do wykorzystywania 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 wykorzystywania 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 na wszystkich poziomach;

   d) systemy AI przeznaczone do wykorzystywania do celów monitorowania i wykrywania niedozwolonego zachowania uczniów podczas testów w kontekście lub w ramach instytucji edukacyjnych i instytucji szkolenia zawodowego na wszystkich poziomach.

4. Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia:

   a) systemy AI przeznaczone do wykorzystywania 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 wykorzystywania do celów podejmowania decyzji wpływających na warunki stosunków pracy, decyzji o awansie lub rozwiązaniu umownego stosunku pracy, przydzielania zadań w oparciu o indywidualne zachowanie lub cechy osobowości lub charakter lub 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, odwoływania lub żądania zwrotu takich świadczeń i usług;

   b) systemy AI przeznaczone do wykorzystywania do celów oceny zdolności kredytowej osób fizycznych lub ustalenia ich scoringu kredytowego, z wyjątkiem systemów AI wykorzystywanych w celu wykrywania oszustw finansowych;

   c) systemy AI przeznaczone do wykorzystywania 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 wykorzystywanie przedmiotowych systemów jest dozwolone na podstawie odpowiednich przepisów prawa Unii lub prawa krajowego:

a) systemy AI przeznaczone do wykorzystywania przez organy ścigania lub w ich imieniu lub przez instytucje, organy i jednostki organizacyjne Unii w ramach wsparcia udzielanego organom 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 w ramach wsparcia udzielanego organom ścigania;

c) systemy AI przeznaczone do wykorzystywania przez organy ścigania lub w ich imieniu lub przez instytucje, organy i jednostki organizacyjne Unii w ramach wsparcia udzielanego organom 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 w ramach wsparcia udzielanego organom ścigania do oceny ryzyka, że osoba fizyczna popełni lub ponownie popełni przestępstwo, przeprowadzanej nie tylko 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 w ramach wsparcia udzielanego organom 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 wykorzystywanie przedmiotowych systemów jest dozwolone na podstawie odpowiednich przepisów prawa Unii lub prawa krajowego:

a) systemy AI przeznaczone do wykorzystywania przez właściwe organy publiczne lub w ich imieniu lub przez instytucje, organy i jednostki organizacyjne Unii jako wariografy lub 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 lub 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 wykorzystywania przez właściwe organy publiczne lub w ich imieniu lub przez 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 wymiaru sprawiedliwości lub w jego imieniu w celu wspomagania organu wymiaru sprawiedliwości 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 wykorzystywania 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, imię i nazwisko lub nazwę dostawcy i wersję systemu wraz z informacją dotyczącą jej związku 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 postaci, 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;

   h) instrukcja obsługi dla podmiotu stosującego oraz, w stosownych przypadkach, podstawowy opis interfejsu użytkownika, który dostarczono podmiotowi stosującemu;

2. Szczegółowy opis elementów systemu AI oraz procesu jego rozwoju, w tym:

   a) metody i działania zastosowane w celu rozwoju systemu AI, w tym, w stosownych przypadkach, skorzystanie z systemów, które zostały poddane pretreningowi, lub narzędzi dostarczonych przez osoby trzecie oraz wskazanie, w jaki sposób dostawca wykorzystał, zintegrował lub zmienił 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 systemu oraz jakości tego wyniku; decyzje dotyczące wszelkich możliwych kompromisów w zakresie rozwiązań technicznych przyjętych w celu zapewnienia zgodności z wymogami określonymi 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 rozwoju, 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 interpretacji wyników 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 i źródeł ryzyka dla zdrowia i bezpieczeństwa, praw podstawowych i ryzyka powodującego 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 interpretacji wyników systemów AI; w stosownych przypadkach specyfikacji dotyczących danych wejściowych;

4. Opis adekwatności wskaźników skuteczności działania 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 cyklu jego życia;

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, o której mowa w art. 47;

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. Imię i nazwisko lub nazwę oraz adres dostawcy lub, w stosownych przypadkach, jego upoważnionego przedstawiciela;
3. Oświadczenie, że deklarację zgodności UE, o której mowa w art. 47, wydano na wyłączną odpowiedzialność dostawcy;
4. Oświadczenie, że system AI jest zgodny z niniejszym rozporządzeniem oraz, w stosownych przypadkach, z wszelkimi innymi odpowiednimi przepisami prawa Unii, w których przewidziano wydanie deklaracji zgodności UE, o której mowa w art. 47;
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, 3 i 4.
2. Dostawca sprawdza, czy ustanowiony system zarządzania jakością jest zgodny z wymogami 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 rozwoju 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, rozwoju 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) imię i nazwisko lub nazwę i adres dostawcy oraz, jeśli wniosek jest składany przez upoważnionego przedstawiciela, również jego imię i nazwisko lub nazwę 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 wprowadzonych procedur zapewniających stałą adekwatność i skuteczność systemu zarządzania jakością;

f) oświadczenie na piśmie, 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 decyzję dotyczącą dokonanej oceny wraz z uzasadnieniem.

3.3. Zatwierdzony system zarządzania jakością 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 decyzję dotyczącą dokonanej oceny wraz z uzasadnieniem.

4. Kontrola dokumentacji technicznej

4.1. Oprócz wniosku, o którym mowa w pkt 3, dostawca składa wniosek do wybranej przez siebie jednostki notyfikowanej o przeprowadzenie oceny 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) imię i nazwisko lub nazwę i adres dostawcy;

b) oświadczenie na piśmie, że tego samego wniosku nie złożono w innej jednostce notyfikowanej;

c) dokumentację techniczną, o której mowa w załączniku IV.

4.3. Analizy dokumentacji technicznej dokonuje jednostka notyfikowana. W stosownych przypadkach, i w zakresie ograniczonym do tego, co jest niezbędne do wykonywania zadań jednostki notyfikowanej, otrzymuje ona 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 zwrócić się do dostawcy o przedstawienie dalszych dowodów lub przeprowadzenie 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, przeprowadza sama 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 prawa Unii 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 decyzję dotyczącą dokonanej oceny wraz z uzasadnieniem.

W przypadku gdy system AI spełnia wymogi określone w rozdziale III sekcja 2, jednostka notyfikowana wydaje unijny certyfikat oceny dokumentacji technicznej. Certyfikat ten zawiera imię i nazwisko lub nazwę 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 wykorzystywania.

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 retrenowaniu. W takim przypadku decyzja jednostki notyfikowanej o odmowie wydania unijnego certyfikatu oceny dokumentacji technicznej wraz z uzasadnieniem 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 uzupełnienia 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 uzupełnienie 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, rozwój 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 przekazywane 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. Imię i nazwisko lub nazwa, adres i dane kontaktowe dostawcy;

2. W przypadku gdy w imieniu dostawcy informacje przekazuje inna osoba, /imię i nazwisko lub nazwa, adres i dane kontaktowe tej osoby;

3. W stosownych przypadkach imię i nazwisko lub nazwa, 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 system (dane, dane wejściowe) oraz logika jego działania;

7. Status systemu AI (w obrocie lub użytkowany; niedostępny już w obrocie / już nieużytkowany, wycofany z użytku);

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. Państwa członkowskie, w których system AI został wprowadzony do obrotu, oddany do użytku lub udostępniony 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 lub 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. Imię i nazwisko lub nazwa, adres i dane kontaktowe dostawcy;

2. W przypadku gdy w imieniu dostawcy informacje przekazuje inna osoba, imię i nazwisko lub nazwa, adres i dane kontaktowe tej osoby;

3. W stosownych przypadkach imię i nazwisko lub nazwa, 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 powodów, dla których system AI jest uznawany za niebędący systemem wysokiego ryzyka w wyniku zastosowania procedury na podstawie art. 6 ust. 3;

8. Status systemu AI (w obrocie lub użytkowany; niedostępny już w obrocie / już nieużytkowany, wycofany z użytku);

9. Państwa członkowskie, w których system AI został wprowadzony do obrotu, oddany do użytku lub udostępniony w Unii.

Sekcja C – Informacje przekazywane przez podmioty stosujące systemy AI wysokiego ryzyka zgodnie z art. 49 ust. 3

W odniesieniu do systemów AI wysokiego ryzyka, które podlegają rejestracji zgodnie z art. 49 ust. 3, przekazuje się, a następnie aktualizuje następujące informacje:

1. Imię i nazwisko lub nazwa, adres i dane kontaktowe podmiotu stosującego AI;
2. Imię i nazwisko lub nazwa, adres i dane kontaktowe osoby przekazującej informacje w imieniu podmiotu stosującego;
3. Adres URL wpisu systemu AI do bazy danych UE dokonanego przez jego dostawcę;
4. Streszczenie ustaleń oceny skutków dla praw podstawowych przeprowadzonej zgodnie z art. 27;
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 przedkładane 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. Imię i nazwisko lub nazwę oraz dane kontaktowe dostawcy lub potencjalnego dostawcy i podmiotów stosujących 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

Akty prawne Unii 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:

   rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1358 z dnia 14 maja 2024 r. w sprawie ustanowienia systemu Eurodac do porównywania danych biometrycznych w celu skutecznego stosowania rozporządzeń Parlamentu Europejskiego i Rady (UE) 2024/1315 i (UE) 2024/1350 i dyrektywy Rady 2001/55/WE oraz w celu identyfikowania nielegalnie przebywających obywateli państw trzecich oraz bezpaństwowców, w sprawie występowania z wnioskami o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, w sprawie zmiany rozporządzeń Parlamentu Europejskiego i Rady (UE) 2018/1240 i (UE) 2019/818 oraz w sprawie uchylenia rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 603/2013 (Dz.U. L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. System wjazdu/wyjazdu:

   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:

   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 oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726, (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW (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 oraz zmieniające rozporządzenia (UE) 2018/1726, (UE) 2018/1862 i (UE) 2019/816 (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, które 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 rozwoju, 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 treningowy, 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), 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 ewaluacji. Strategie ewaluacji obejmują kryteria ewaluacji, 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 rozwoju, 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 metod 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 oddziaływanie 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) liczbę obliczeń wykorzystanych do trenowania modelu, mierzoną w operacjach zmiennoprzecinkowych 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, poziom jego autonomii i skalowalności, narzędzia, do których ma dostęp;

f) czy ze względu na swój zasięg ma duże oddziaływanie 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.