Rada
Unii Europejskiej

Bruksela, 25 listopada 2022 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2021/0106(COD)

14954/22

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

PUBLIC

NOTA

Od:	Komitet Stałych Przedstawicieli (część I)
Do:	Rada
Nr poprz. dok.:	14336/22
Nr dok. Kom.:	8115/21
Dotyczy:	Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii – Podejście ogólne

I. WPROWADZENIE

1. W dniu 21 kwietnia 2021 r. Komisja przyjęła wniosek dotyczący rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (**akt o sztucznej inteligencji**).

2. Celem wniosku Komisji, jest zapewnienie, aby systemy sztucznej inteligencji wprowadzane do obrotu w Unii i wykorzystywane w Unii były bezpieczne i zgodne z obowiązującymi przepisami dotyczącymi praw podstawowych i z wartościami Unii, aby zagwarantować pewność prawa w celu ułatwienia inwestycji i innowacji w dziedzinie sztucznej inteligencji, poprawić zarządzanie i skuteczne egzekwowanie obowiązujących przepisów dotyczących praw podstawowych i bezpieczeństwa, a także ułatwić rozwój jednolitego rynku dla zgodnych z prawem, bezpiecznych i wiarygodnych zastosowań sztucznej inteligencji, a jednocześnie aby zapobiec fragmentacji rynku.

II. PRACA W INNYCH INSTYTUCJACH

3. W Parlamencie Europejskim dyskusjami kierują Komisja Rynku Wewnętrznego i Ochrony Konsumentów (IMCO; sprawozdawca: Brando Benifei, S&D, Włochy) oraz Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE; sprawozdawca: Dragos Tudorache, Renew, Rumunia) w ramach procedury wspólnych posiedzeń komisji. W pracach ustawodawczych biorą udział również – w ramach kompetencji dzielonych lub wyłącznych – Komisja Prawna (JURI), Komisja Przemysłu, Badań Naukowych i Energii (ITRE) oraz Komisja Kultury i Edukacji (CULT). Obaj współsprawozdawcy przedstawili projekt sprawozdania w kwietniu 2022 r., a głosowanie nad wspólnym sprawozdaniem komisji IMCO i LIBE zaplanowano na pierwszy kwartał 2023 r.

4. Europejski Komitet Ekonomiczno-Społeczny wydał opinię w sprawie wniosku w dniu 22 września 2021 r., natomiast Europejski Komitet Regionów wydał opinię w dniu 2 grudnia 2021 r.

5. W dniu 18 czerwca 2021 r. Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) wydali wspólną opinię na temat wniosku.

6. Europejski Bank Centralny (EBC) wydał swoją opinię w dniu 29 grudnia 2021 r. i przedstawił ją Grupie Roboczej ds. Telekomunikacji i Społeczeństwa Informacyjnego (grupie roboczej TELECOM) w dniu 10 lutego 2022 r.

III. STAN PRAC W RADZIE

1. Na forum Rady analiza wniosku została przeprowadzona przez grupę roboczą TELECOM. Grupa robocza TELECOM rozpoczęła omawianie wniosku podczas prezydencji portugalskiej na kilku posiedzeniach i warsztatach, które odbyły się w okresie od kwietnia do czerwca 2021 r. Prace nad wnioskiem kontynuowano podczas prezydencji słoweńskiej, która opracowała pierwszą, częściową propozycję kompromisową obejmującą **art. 1–7 i załączniki I-III**. Ponadto prezydencja słoweńska zorganizowała nieformalne półdniowe posiedzenie ministrów ds. telekomunikacji poświęcone wyłącznie wnioskowi dotyczącemu sztucznej inteligencji, podczas którego ministrowie potwierdzili swoje poparcie dla horyzontalnego i ukierunkowanego na człowieka podejścia przyjętego do uregulowania sztucznej inteligencji. Prezydencja francuska kontynuowała proces analizy i przed końcem swojego przewodnictwa przeredagowała pozostałe części tekstu **(art. 8–85 i załączniki IV-IX)** oraz przedstawiła cały pierwszy skonsolidowany wniosek kompromisowy dotyczący aktu w sprawie sztucznej inteligencji w dniu 17 czerwca 2022 r.

2. W dniu 5 lipca 2022 r. prezydencja czeska przeprowadziła debatę orientacyjną na forum grupy roboczej TELECOM na podstawie dokumentu dotyczącego wariantów strategicznych; wyniki tej debaty wykorzystano do przygotowania **drugiego tekstu kompromisowego**. Na podstawie reakcji delegacji na ten kompromis prezydencja czeska przygotowała **trzeci tekst kompromisowy**, który został przedstawiony i omówiony w grupie roboczej TELECOM w dniach 22 i 29 września 2022 r. Po tych dyskusjach delegacje zostały poproszone o przedstawienie dalszych pisemnych uwag, które zostały wykorzystane przez prezydencję czeską do przygotowania **czwartej propozycji kompromisu**. Na podstawie dyskusji na temat czwartej propozycji kompromisu, które odbyły się na forum grupy roboczej TELECOM w dniach 25 października 2022 r. i 8 listopada 2022 r., a także biorąc pod uwagę ostateczne uwagi pisemne państw członkowskich, prezydencja czeska przygotowała **ostateczną wersję tekstu kompromisowego**, która znajduje się w załączniku. W dniu 18 listopada Coreper przeanalizował tę kompromisową propozycję i **jednomyślnie – bez wprowadzania żadnych zmian – zgodził się przekazać ją Radzie ds. TTE (telekomunikacja) z myślą o wypracowaniu porozumienia ogólnego** na posiedzeniu w dniu 6 grudnia 2022 r.

PUBLIC

IV. GŁÓWNE ELEMENTY KOMPROMISOWEJ PROPOZYCJI

1. **Definicja systemu sztucznej inteligencji, zakazane praktyki związane ze sztuczną inteligencją, wykaz przypadków użycia sztucznej inteligencji wysokiego ryzyka w załączniku III oraz klasyfikowanie systemów sztucznej inteligencji jako systemów wysokiego ryzyka**

1.1 W celu zapewnienia, aby definicja systemu sztucznej inteligencji zawierała wystarczająco jasne kryteria rozróżniania sztucznej inteligencji od bardziej klasycznych systemów oprogramowania, tekst kompromisowy zawęża definicję zawartą w **art. 3 ust. 1** do systemów opracowanych przy wykorzystaniu mechanizmów uczenia się maszyn oraz podejściach opartych na logice i wiedzy.

1.2 W odniesieniu do przekazania Komisji uprawnień dotyczących aktualizacji definicji systemu sztucznej inteligencji skreślono **załącznik I** oraz odpowiadające mu uprawnienie Komisji dotyczące jego aktualizacji w drodze aktów delegowanych. W zamian dodano nowe **motywy 6a i 6b**, aby wyjaśnić, co należy rozumieć przez mechanizmy uczenia się maszyn oraz podejścia oparte na logice i wiedzy. W celu zapewnienia, aby akt w sprawie sztucznej inteligencji zachował elastyczność i aktualność, w **art. 4** dodano możliwość przyjmowania aktów wykonawczych w celu doprecyzowania i aktualizacji mechanizmów uczenia się maszyn oraz podejść opartych na logice i wiedzy.

1.3 W odniesieniu do zakazanych praktyk w zakresie sztucznej inteligencji, w **art. 5** tekst kompromisowy zawiera rozszerzenie zakazu wykorzystywania sztucznej inteligencji do celów oceny punktowej zachowań społecznych obywateli również na podmioty prywatne. Ponadto, przepis zakazujący korzystania z systemów sztucznej inteligencji, które wykorzystują podatność określonej grupy osób na zagrożenia, obecnie obejmuje również osoby znajdujące się w trudnym położeniu ze względu na ich sytuację społeczną lub ekonomiczną. W odniesieniu do zakazu stosowania przez organy ścigania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej, w tekście kompromisowym wyjaśniono cele, w przypadku których takie wykorzystanie uznaje się za absolutnie niezbędne do celów egzekwowania prawa i w związku z tym organy ścigania powinny mieć możliwość korzystania z takich systemów w drodze wyjątku.

PUBLIC

1.4 W odniesieniu do wykazu przypadków użycia sztucznej inteligencji wysokiego ryzyka w **załączniku III**, trzy z nich usunięto (wykrywanie treści typu „deepfake” przez organy ścigania, analiza przestępczości, weryfikacja autentyczności dokumentów podróży), dwa dodano (krytyczna infrastruktura cyfrowa oraz ubezpieczenie na życie i ubezpieczenie zdrowotne), a inne dopracowano. Jednocześnie zmieniono **art. 7 ust. 1**, aby przewidzieć możliwość nie tylko dodawania do wykazu w drodze aktów delegowanych przypadków użycia wysokiego ryzyka, ale również ich usuwania. Aby zapewnić odpowiednią ochronę praw podstawowych w przypadku takiego usunięcia, w **art. 7 ust. 3** dodano dodatkowe przepisy określające warunki, które musiałyby zostać spełnione, zanim akt delegowany będzie mógł zostać przyjęty.

1.5 W odniesieniu do klasyfikacji systemów sztucznej inteligencji jako systemów wysokiego ryzyka, propozycja kompromisowa obejmuje obecnie dodatkową warstwę poziomą oprócz klasyfikacji wysokiego ryzyka dokonanej w **załączniku III**, aby zapewnić, że nie będą uwzględniane systemy sztucznej inteligencji, które prawdopodobnie nie będą powodować poważnych naruszeń praw podstawowych ani innych istotnych zagrożeń. W szczególności **art. 6 ust. 3** zawiera nowe przepisy, zgodnie z którymi przy klasyfikowaniu systemów sztucznej inteligencji jako systemów wysokiego ryzyka należy również uwzględnić znaczenie wyników działania danego systemu sztucznej inteligencji w odniesieniu do odpowiedniego działania lub decyzji, która ma zostać podjęta. Znaczenie wyników działania systemu sztucznej inteligencji będzie oceniane na podstawie tego, czy ma on charakter wyłącznie pomocniczy w odniesieniu do odpowiedniego działania lub decyzji, które należy podjąć.

2. Wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka i obowiązki różnych podmiotów w łańcuchu wartości AI

2.1 Wiele z przewidzianych w **tytule III rozdział 2** wniosku wymogów dotyczących systemów sztucznej inteligencji wysokiego ryzyka doprecyzowano i dostosowano w taki sposób, aby były one bardziej wykonalne technicznie, a ich przestrzeganie było mniej uciążliwe dla zainteresowanych stron, na przykład w odniesieniu do jakości danych lub w odniesieniu do dokumentacji technicznej, która powinna zostać sporządzona przez MŚP w celu wykazania, że ich systemy sztucznej inteligencji wysokiego ryzyka spełniają wymogi.

2.2 Z uwagi na fakt, że systemy sztucznej inteligencji są opracowywane i dystrybuowane za pośrednictwem złożonych łańcuchów wartości, tekst kompromisowy zawiera zmiany wyjaśniające podział obowiązków i ról. Na przykład w **art. 13 i 14** dodano nowe przepisy, które umożliwiają skuteczniejszą współpracę między dostawcami a użytkownikami. Tekst kompromisowy ma również na celu wyjaśnienie związku między obowiązkami wynikającymi z aktu w sprawie sztucznej inteligencji a obowiązkami istniejącymi już na mocy innych przepisów, takich jak odpowiednie unijne przepisy dotyczące ochrony danych lub przepisy sektorowe, w tym w odniesieniu do sektora usług finansowych. Ponadto nowy **art. 23a** precyzyjniej wskazuje sytuacje, w których inne podmioty w łańcuchu wartości są zobowiązane do przejęcia obowiązków dostawcy.

3. **Systemy sztucznej inteligencji ogólnego przeznaczenia**

3.1 Dodano nowy **tytuł IA**, by uwzględnić sytuacje, w których systemy sztucznej inteligencji mogą być wykorzystywane do wielu różnych celów (sztuczna inteligencja ogólnego przeznaczenia) i w których mogą zaistnieć okoliczności, gdy technologia sztucznej inteligencji ogólnego przeznaczenia zostaje włączona do innego systemu, który może mieć charakter systemu wysokiego ryzyka. W tekście kompromisowym określa się w **art. 4b ust. 1**, że niektóre wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka będą mieć również zastosowanie do systemów sztucznej inteligencji ogólnego przeznaczenia. Jednak zamiast bezpośredniego stosowania tych wymogów, akt wykonawczy określi, w jaki sposób należy je stosować w odniesieniu do systemów sztucznej inteligencji ogólnego przeznaczenia, po przeprowadzeniu konsultacji i szczegółowej oceny skutków oraz z uwzględnieniem szczególnych cech tych systemów i odnośnego łańcucha wartości, a także wykonalności technicznej, rozwoju rynku i rozwoju technologicznego. Zastosowanie aktu wykonawczego zapewni odpowiednie zaangażowanie państw członkowskich i sprawi, że będą mogły nadal ostatecznie decydować, w jaki sposób stosować wymogi w przedmiotowym kontekście.

3.2 Ponadto kompromisowy tekst **art. 4b ust. 5** przewiduje również możliwość przyjmowania dalszych aktów wykonawczych, które określałyby warunki współpracy między dostawcami systemów sztucznej inteligencji ogólnego przeznaczenia a innymi dostawcami zamierzającymi wprowadzić do obrotu lub oddać do użytku w Unii takie systemy jako systemy sztucznej inteligencji wysokiego ryzyka, w szczególności w odniesieniu do dostarczania informacji.

4. **Wyjaśnienie zakresu proponowanego aktu w sprawie sztucznej inteligencji i przepisów dotyczących organów ścigania**

4.1 W **art. 2** zawarto wyraźne odniesienie do wyłączenia celów bezpieczeństwa narodowego, celów obronnych i wojskowych z zakresu aktu w sprawie sztucznej inteligencji. Podobnie wyjaśniono, że akt w sprawie sztucznej inteligencji nie powinien mieć zastosowania do systemów sztucznej inteligencji i ich wyników wykorzystywanych wyłącznie do celów badawczo-rozwojowych, ani w zakresie obowiązków osób korzystających ze sztucznej inteligencji do celów pozazawodowych, z wyjątkiem obowiązków w zakresie przejrzystości.

4.2 Aby uwzględnić szczególną specyfikę organów ścigania, wprowadzono szereg zmian do przepisów dotyczących wykorzystywania systemów sztucznej inteligencji do celów egzekwowania prawa. W szczególności niektóre powiązane definicje zawarte w **art. 3** takie jak „system zdalnej identyfikacji biometrycznej" oraz „system zdalnej identyfikacji biometrycznej »w czasie rzeczywistym«" doprecyzowano w celu wyjaśnienia, w jakich sytuacjach ich stosowanie jest zabronione lub uznawane za stwarzające wysokie ryzyko, a w jakich sytuacjach takie zagrożenie nie występuje. Tekst kompromisowy zawiera również inne zmiany, które – z zastrzeżeniem odpowiednich zabezpieczeń – mają na celu zapewnienie odpowiedniego poziomu elastyczności w wykorzystywaniu systemów sztucznej inteligencji wysokiego ryzyka przez organy ścigania lub uwzględnienie potrzeby poszanowania poufności szczególnie chronionych danych operacyjnych w związku z działalnością tych organów.

5. **Oceny zgodności, ramy zarządzania, nadzór rynku, egzekwowanie i kary**

5.1 Z myślą o uproszczeniu ram zgodności przewidzianych dla aktu w sprawie sztucznej inteligencji, tekst kompromisowy zawiera szereg uściśleń i uproszczeń odnośnie do przepisów dotyczących procedur oceny zgodności. Przepisy dotyczące nadzoru rynku również wyjaśniono i uproszczono, aby uczynić je bardziej skutecznymi i łatwiejszymi do wdrożenia, biorąc pod uwagę potrzebę proporcjonalnego podejścia w tym zakresie. Ponadto **art. 41** został poddany gruntownemu przeglądowi w celu ograniczenia swobody decyzyjnej Komisji w odniesieniu do przyjmowania aktów wykonawczych ustanawiających wspólne specyfikacje techniczne w zakresie wymogów dla systemów sztucznej inteligencji wysokiego ryzyka i systemów sztucznej inteligencji ogólnego przeznaczenia.

5.2 Tekst kompromisowy znacząco zmienił też przepisy dotyczące Rady ds. Sztucznej Inteligencji (zwanej dalej „Radą”) w celu zapewnienia większej autonomii i wzmocnienia jej roli w strukturze zarządzania przewidzianej w akcie w sprawie sztucznej inteligencji. W tym kontekście zmieniono **art. 56 i 58** w celu wzmocnienia roli tej Rady w taki sposób, aby była w stanie lepiej wspierać państwa członkowskie we wdrażaniu i egzekwowaniu aktu w sprawie sztucznej inteligencji. W szczególności rozszerzono zadania Rady i określono jej skład. W celu zapewnienia zaangażowania zainteresowanych stron we wszystkie kwestie związane z wdrażaniem aktu w sprawie sztucznej inteligencji, w tym w przygotowanie aktów wykonawczych i aktów delegowanych, dodano nowy wymóg, zgodnie z którym Rada ta powinna utworzyć stałą podgrupę służącą jako platforma dla szerokiego grona zainteresowanych stron. Należy również ustanowić dwie inne stałe podgrupy: dla organów nadzoru rynku i organów notyfikujących, by wzmocnić spójność zarządzania i egzekwowania aktu w sprawie sztucznej inteligencji w całej Unii.

5.3 W celu dalszego usprawnienia ram zarządzania tekst kompromisowy zawiera nowe **art. 68a i 68b**. **Art. 68a** zobowiązuje Komisję do wyznaczenia co najmniej jednej unijnej jednostki badawczej w obszarze sztucznej inteligencji, która powinna zapewniać niezależne doradztwo techniczne lub naukowe na wniosek Rady ds. Sztucznej Inteligencji lub organów nadzoru rynku, natomiast **art. 68b** nakłada na Komisję obowiązek utworzenia centralnej puli niezależnych ekspertów w celu wspierania działań w zakresie egzekwowania przepisów aktu w sprawie sztucznej inteligencji. I wreszcie nowy **art. 58a** wprowadza dla Komisji obowiązek opracowywania wytycznych w zakresie stosowania aktu w sprawie sztucznej inteligencji.

5.4 Jeżeli chodzi o kary za naruszenia przepisów aktu w sprawie sztucznej inteligencji, w **art. 71** tekstu kompromisowego przewidziano bardziej proporcjonalne pułapy administracyjnych kar pieniężnych dla MŚP i przedsiębiorstw typu start-up. Ponadto w **art. 71 ust. 6** dodano cztery dodatkowe kryteria ustalania wysokości administracyjnych kar pieniężnych, by jeszcze bardziej zabezpieczyć ich ogólną proporcjonalność.

6. **Przejrzystość i inne przepisy na rzecz osób, na które systemy sztucznej inteligencji mogą mieć wpływ**

6.1 Wniosek kompromisowy zawiera szereg zmian, które zwiększają przejrzystość w odniesieniu do wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka. W szczególności zaktualizowano **art. 51**, aby wskazać, iż niektórzy użytkownicy systemów sztucznej inteligencji wysokiego ryzyka będący publicznymi organami, agencjami lub jednostkami organizacyjnymi będą również zobowiązani do rejestracji w unijnej bazie danych systemów sztucznej inteligencji wysokiego ryzyka umieszczonych w załączniku III. Ponadto nowo dodany **art. 52 ust. 2a** kładzie nacisk na zobowiązanie użytkowników systemu służącego do rozpoznawania emocji do informowania osób fizycznych o stosowaniu wobec nich takiego systemu.

6.2 We wniosku kompromisowym wyjaśniono również w nowo dodanym **art. 63 ust. 11**, że osoba fizyczna lub prawna, która ma powody uważać, że doszło do naruszenia przepisów aktu w sprawie sztucznej inteligencji, może złożyć skargę do właściwego organu nadzoru rynku i może oczekiwać, że taka skarga zostanie rozpatrzona zgodnie ze specjalnymi procedurami tego organu.

7. **Środki wspierające innowacyjność**

7.1 W celu stworzenia ram prawnych bardziej sprzyjających innowacjom oraz w celu promowania opartego na dowodach uczenia się działań regulacyjnych w tekście kompromisowym zmieniono istotnie przepisy **art. 53** dotyczące środków wspierających innowacyjność. Przede wszystkim wyjaśniono, że piaskownice regulacyjne w zakresie sztucznej inteligencji, które mają stworzyć kontrolowane środowisko na potrzeby opracowywania, testowania i walidacji innowacyjnych systemów sztucznej inteligencji pod bezpośrednim nadzorem i zgodnie z wytycznymi właściwych organów krajowych, powinny również umożliwiać testowanie innowacyjnych systemów sztucznej inteligencji w warunkach rzeczywistych. Ponadto dodano nowe przepisy w **art. 54a i 54b** umożliwiające nienadzorowane testowanie systemów sztucznej inteligencji w warunkach rzeczywistych – przy spełnieniu szczególnych warunków i zachowaniu odpowiednich zabezpieczeń. W obu tych artykułach tekst kompromisowy wyjaśnia, w jaki sposób nowe przepisy mają być interpretowane w odniesieniu do innych istniejących przepisów sektorowych dotyczących piaskownic regulacyjnych.

7.2 Wreszcie, aby zmniejszyć obciążenia administracyjne dla mniejszych przedsiębiorstw, w **art. 55** tekstu kompromisowego zawarto wykaz działań, które Komisja ma podejmować, by wspierać takich operatów, a w **art. 55a** przewidziano pewne – ograniczone w zakresie i jasno sprecyzowane – odstępstwa.

PUBLIC

V. PODSUMOWANIE

1. W związku z powyższym Komitet Stałych Przedstawicieli jest proszony o:
   - przeanalizowanie tekstu kompromisowego przedstawionego w załączniku do niniejszej noty;
   - potwierdzenie podejścia ogólnego w sprawie wniosku dotyczącego rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) – na posiedzeniu Rady ds. TTE (telekomunikacja) w dniu 6 grudnia 2022 r.

ZAŁĄCZNIK

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

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

(Tekst mający znaczenie dla EOG)

PUBLIC

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 Komitetu Regionów[2],

uwzględniając opinię Europejskiego Banku Centralnego[3],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

[1] Dz.U. C […] z […], s. […].
[2] Dz.U. C […] z […], s. […].
[3] Odniesienie do opinii EBC

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

(2) Systemy sztucznej inteligencji mogą być łatwo wdrażane w wielu sektorach gospodarki i obszarach życia społecznego, w tym w wymiarze transgranicznym, i mogą być przedmiotem obrotu w całej Unii. Niektóre państwa członkowskie rozważały już przyjęcie przepisów krajowych w celu zapewnienia, aby sztuczna inteligencja była bezpieczna oraz rozwijana i wykorzystywana w sposób zgodny z obowiązkami wynikającymi z praw podstawowych. Zróżnicowane przepisy krajowe mogą prowadzić do rozdrobnienia rynku wewnętrznego i zmniejszenia pewności prawa dla operatorów, którzy opracowują, importują lub wykorzystują systemy sztucznej inteligencji. Należy zatem zapewnić spójny i wysoki poziom ochrony w całej Unii, zapobiegając jednocześnie rozbieżnościom utrudniającym swobodny obrót systemami sztucznej inteligencji oraz powiązanymi produktami i usługami na rynku wewnętrznym poprzez ustanowienie jednolitych obowiązków dla operatorów i zagwarantowanie jednolitej ochrony nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym, w oparciu o art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). W zakresie, w jakim niniejsze rozporządzenie zawiera określone przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w odniesieniu do ograniczenia wykorzystywania systemów sztucznej inteligencji do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa, podstawą niniejszego rozporządzenia w zakresie takich przepisów szczegółowych powinien być art. 16 TFUE. W świetle tych przepisów szczegółowych i odwołania się do art. 16 TFUE należy skonsultować się z Europejską Radą Ochrony Danych.

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

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

(5) Unijne ramy prawne określające zharmonizowane przepisy dotyczące sztucznej inteligencji są zatem niezbędne do wspierania rozwoju, wykorzystywania i upowszechniania sztucznej inteligencji na rynku wewnętrznym, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony interesów publicznych, takich jak zdrowie i bezpieczeństwo oraz ochrona praw podstawowych, uznanych i chronionych przez prawo Unii. Aby osiągnąć ten cel, należy ustanowić przepisy regulujące wprowadzanie do obrotu i oddawanie do użytku niektórych systemów sztucznej inteligencji, zapewniając w ten sposób sprawne funkcjonowanie rynku wewnętrznego i umożliwiając swobodny obrót tymi systemami zgodnie z zasadą swobodnego przepływu towarów i usług. Ustanawiając te zasady i w oparciu o prace grupy ekspertów wysokiego szczebla ds. AI – odzwierciedlone w wytycznych w zakresie etyki dotyczących godnej zaufania sztucznej inteligencji, niniejsze rozporządzenie wspiera realizację celu, jakim jest osiągnięcie przez Unię pozycji światowego lidera, jeśli chodzi o rozwój bezpiecznej, wiarygodnej i etycznej sztucznej inteligencji, zgodnie z konkluzjami Rady Europejskiej[4], oraz zapewnia ochronę zasad etycznych, zgodnie z wyraźnym żądaniem Parlamentu Europejskiego[5].

---

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

[5] 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).

(5a) Zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji określone w niniejszym rozporządzeniu powinny mieć zastosowanie we wszystkich sektorach i – zgodnie z podejściem przedstawionym w nowych ramach prawnych – powinny pozostawać bez uszczerbku dla obowiązującego prawa Unii, w szczególności w zakresie ochrony danych, ochrony konsumentów, praw podstawowych, zatrudnienia i bezpieczeństwa produktów, wobec którego niniejsze rozporządzenie ma charakter uzupełniający. W związku z tym wszystkie prawa i środki ochrony prawnej przyznane przez takie prawo Unii konsumentom lub innym osobom, na które systemy sztucznej inteligencji mogą mieć niekorzystny wpływ, w tym w zakresie odszkodowania za ewentualne szkody na podstawie dyrektywy 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, pozostają nienaruszone i mają pełne zastosowanie. Ponadto niniejsze rozporządzenie ma na celu zwiększenie skuteczności takich istniejących praw i środków ochrony prawnej poprzez ustanowienie szczegółowych wymogów i obowiązków, w tym w zakresie przejrzystości, dokumentacji technicznej i rejestrowania zdarzeń w ramach systemów sztucznej inteligencji. Co więcej obowiązki nałożone na mocy niniejszego rozporządzenia na różnych operatorów uczestniczących w łańcuchu wartości sztucznej inteligencji powinny mieć zastosowanie bez uszczerbku dla przepisów krajowych, zgodnych z prawem Unii, skutkujących ograniczeniem stosowania określonych systemów sztucznej inteligencji, gdy przepisy takie nie wchodzą w zakres niniejszego rozporządzenia lub służą innym uzasadnionym celom interesu publicznego 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 opracowany przez ONZ komentarz ogólny nr 25 z 2021 r. do Konwencji ONZ o prawach dziecka, w zakresie w jakim prawo to i przepisy nie dotyczą konkretnie systemów sztucznej inteligencji i służą innym uzasadnionym celom interesu publicznego.

PUBLIC

(6) Pojęcie systemu sztucznej inteligencji powinno być jasno zdefiniowane w celu zapewnienia pewności prawa, przy jednoczesnym zapewnieniu elastyczności umożliwiającej dostosowanie się do przyszłego rozwoju technologicznego. Definicja powinna opierać się na kluczowych cechach funkcjonalnych sztucznej inteligencji, takich jak jej zdolności w zakresie uczenia się, rozumowania lub modelowania, które odróżniają ją od prostszych systemów oprogramowania lub podejść do programowania. W szczególności, do celów niniejszego rozporządzenia, systemy sztucznej inteligencji rozumie się jako systemy zdolne – na podstawie danych i informacji dostarczonych maszynowo lub przez człowieka – do wywnioskowania, w jaki sposób osiągnąć dany zestaw celów określonych przez człowieka, przy wykorzystaniu mechanizmów uczenia się maszyn lub metod opartych na logice i wiedzy, oraz do generowania wyników takich jak treści w przypadku generatywnych systemów sztucznej inteligencji (np. tekst, materiały wideo lub obrazy), przewidywania, zalecenia lub decyzje wpływające na środowisko, z którym system wchodzi w interakcję, czy to w wymiarze fizycznym, czy cyfrowym. System stosujący zasady określone wyłącznie przez osoby fizyczne, by automatycznie wykonywać operacje, nie powinien być uznawany za system sztucznej inteligencji. Systemy sztucznej inteligencji mogą być zaprojektowane tak, aby działały na różnym poziomie autonomii i mogły być wykorzystywane jako samodzielne rozwiązania lub jako element produktu, niezależnie od tego, czy system jest fizycznie zintegrowany z produktem (wbudowany), czy też służy realizacji funkcji produktu, choć nie jest z nim zintegrowany (niewbudowany). Pojęcie autonomii systemu sztucznej inteligencji odnosi się do stopnia, w jakim taki system funkcjonuje bez udziału człowieka.

(6a) Mechanizmy uczenia się maszyn służą rozwijaniu systemów zdolnych do uczenia się i wyciągania wniosków z danych w celu rozwiązania problemu w zakresie danego zastosowania bez wyraźnego zaprogramowania systemu poprzez podanie instrukcji krok po kroku od etapu wprowadzenia danych wejściowych do uzyskania wyniku. Uczenie się odnosi się do obliczeniowego procesu optymalizacji parametrów modelu stosowanego do danych, będącego konstruktem matematycznym generującym dane wyjściowe na podstawie danych wejściowych. Problemy, które rozwiązuje się za pomocą uczenia się maszyn, zwykle obejmują zadania, w przypadku których inne metody nie sprawdzają się – dlatego, że brak odpowiedniej formalizacji problemu, lub dlatego, że nie jest możliwe rozwiązanie problemu przy zastosowaniu metod, w których nie występuje aspekt uczenia się. Mechanizmy uczenia się maszyn obejmują na przykład nadzorowane uczenie się maszyn, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, przy wykorzystaniu różnorodnych metod, w tym uczenia głębokiego z wykorzystaniem sieci neuronowych, technik statystycznych do uczenia się i wyciągania wniosków (w tym np. regresji logistycznej, estymacji bayesowskiej) oraz metod wyszukiwania i optymalizacji.

(6b) Metody oparte na logice i wiedzy służą rozwijaniu systemów posiadających zdolności logicznego rozumowania lub wiedzę potrzebne do rozwiązania problemu w zakresie danego zastosowania. Systemy takie zazwyczaj obejmują bazę wiedzy i silnik inferencyjny, który generuje wyniki w oparciu o poddanie bazy wiedzy analizie logicznej. Baza wiedzy, która jest zwykle kodowana przez ludzkich ekspertów, reprezentuje jednostki i logiczne relacje istotne dla problemu w zakresie danego zastosowania poprzez formalizmy oparte na zasadach, ontologiach lub wykresach wiedzy. Silnik inferencyjny korzysta z bazy wiedzy i pozyskuje nowe informacje poprzez operacje takie jak sortowanie, wyszukiwanie, dopasowywanie lub łączenie w łańcuchy. Metody oparte na logice i wiedzy obejmują na przykład reprezentację wiedzy, indukcyjne programowanie logiczne, bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne), systemy ekspertowe oraz metody wyszukiwania i optymalizacji.

(6c) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia w odniesieniu do mechanizmów uczenia się maszyn oraz metod opartych na logice i wiedzy, a także w celu uwzględnienia rozwoju rynku i rozwoju technologicznego, należy powierzyć Komisji uprawnienia wykonawcze.

(6d) Pojęcie „użytkownika”, o którym mowa w niniejszym rozporządzeniu, należy interpretować jako każdą osobę fizyczną lub prawną, w tym organ publiczny, agencję lub inny podmiot, która korzysta z systemu sztucznej inteligencji i która odpowiada za to wykorzystywanie. W zależności od rodzaju systemu sztucznej inteligencji korzystanie z takiego systemu może mieć wpływ na osoby inne niż użytkownik.

(7) Pojęcie danych biometrycznych stosowane w niniejszym rozporządzeniu powinno być interpretowane w sposób spójny z pojęciem danych biometrycznych zdefiniowanym w art. 4 pkt 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[6], art. 3 pkt 18 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[7] oraz art. 3 pkt 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680[8].

PUBLIC

[6] 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).

[7] 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).

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

(8) Pojęcie systemu zdalnej identyfikacji biometrycznej stosowane w niniejszym rozporządzeniu należy zdefiniować funkcjonalnie jako system sztucznej inteligencji służący do identyfikacji osób fizycznych co do zasady na odległość, bez aktywnego udziału tych osób, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, niezależnie od konkretnej technologii oraz konkretnych procesów lub rodzajów wykorzystywanych danych biometrycznych. Takie systemy zdalnej identyfikacji biometrycznej są zwykle wykorzystywane do jednoczesnego obserwowania (skanowania) wielu osób lub ich zachowania w celu znacznego ułatwienia identyfikacji określonych osób bez ich aktywnego udziału. Taka definicja wyklucza systemy weryfikacji/uwierzytelniania, których jedynym celem jest potwierdzanie, że określona osoba fizyczna jest osobą, za którą się podaje, a także systemy wykorzystywane do potwierdzania tożsamości osoby fizycznej wyłącznie w celu uzyskania przez nią dostępu do usługi, urządzenia lub lokalu. 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. W przypadku systemów działających „w czasie rzeczywistym” pobranie danych biometrycznych, porównanie i identyfikacja następują natychmiast, niemal natychmiast lub w każdym razie bez znacznego opóźnienia. W związku z tym nie powinno być możliwości obchodzenia przepisów niniejszego rozporządzenia dotyczących stosowania przedmiotowych systemów sztucznej inteligencji „w czasie rzeczywistym” poprzez wprowadzenie niewielkich opóźnień. Systemy identyfikacji „w czasie rzeczywistym” obejmują wykorzystanie materiału rejestrowanego „na żywo” lub „w czasie zbliżonym do rzeczywistego”, takiego jak materiał wideo generowany przez kamerę lub inne urządzenie o podobnej funkcjonalności. Natomiast w przypadku systemów identyfikacji „post factum” dane biometryczne zostały już pobrane, a porównanie i identyfikacja następują ze znacznym opóźnieniem. Dotyczy to materiałów, takich jak zdjęcia lub nagrania wideo generowane przez kamery telewizji przemysłowej lub urządzenia prywatne, które zostały wytworzone, zanim użyto systemu w stosunku do danej osoby fizycznej.

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

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

(11) Ze względu na swój cyfrowy charakter niektóre systemy sztucznej inteligencji powinny zostać objęte zakresem niniejszego rozporządzenia, nawet jeśli nie są wprowadzane do obrotu, oddawane do użytku ani wykorzystywane w Unii. Dotyczy to na przykład operatora mającego siedzibę w Unii, który zleca określone usługi operatorowi mającemu siedzibę poza Unią w związku z działaniem, które ma być wykonywane przez system sztucznej inteligencji, który zostałby zakwalifikowany jako system wysokiego ryzyka. W takich okolicznościach system sztucznej inteligencji wykorzystywany przez operatora spoza Unii mógłby przetwarzać dane, które legalnie zgromadzono w Unii i przekazano poza Unię, oraz przekazywać zlecającemu operatorowi z Unii wynik przetwarzania tych danych, natomiast sam system sztucznej inteligencji nie byłby przedmiotem wprowadzenia do obrotu lub oddania do użytku w Unii ani nie byłby w Unii wykorzystywany. Aby zapobiec obchodzeniu przepisów niniejszego rozporządzenia oraz zapewnić skuteczną ochronę osób fizycznych znajdujących się w Unii, niniejsze rozporządzenie powinno mieć również zastosowanie do dostawców i użytkowników systemów sztucznej inteligencji, którzy mają siedzibę w państwie trzecim, w zakresie, w jakim wyniki działania tych systemów są wykorzystywane w Unii. Aby uwzględnić jednak istniejące ustalenia i szczególne potrzeby w zakresie przyszłej współpracy z partnerami zagranicznymi, z którymi wymienia się informacje i dowody, niniejsze rozporządzenie nie powinno mieć zastosowania do organów publicznych państwa trzeciego i organizacji międzynarodowych działających w ramach zawartych na szczeblu krajowym lub europejskim umów międzynarodowych o współpracy organów ścigania i wymiarów sprawiedliwości z Unią lub jej państwami członkowskimi. Takie umowy zostały zawarte dwustronnie między państwami członkowskimi a państwami trzecimi lub między Unią Europejską, Europolem i innymi agencjami UE a państwami trzecimi i organizacjami międzynarodowymi. Będące odbiorcami organy państw członkowskich oraz instytucje, organy i jednostki organizacyjne Unii, a także jednostki korzystające z takich wyników w Unii pozostają odpowiedzialne za zapewnienie zgodności ich stosowania z prawem Unii. W przypadku zmiany takich umów międzynarodowych lub zawierania nowych w przyszłości umawiające się strony powinny dołożyć wszelkich starań, by dostosować takie umowy do wymogów niniejszego rozporządzenia.

(12) Niniejsze rozporządzenie powinno mieć również zastosowanie do instytucji, urzędów, organów i agencji Unii, gdy działają one jako dostawca lub użytkownik systemu sztucznej inteligencji.

PUBLIC

(-12a) Jeżeli i w zakresie w jakim systemy sztucznej inteligencji wprowadza się do obrotu , oddaje do użytku lub korzysta się z nich z modyfikacjami lub bez zmian – do celów wojskowych, obronnych lub celów bezpieczeństwa narodowego, systemy te należy wyłączyć z zakresu stosowania niniejszego rozporządzenia niezależnie od tego, jaki podmiot wykonuje te działania – nie ma znaczenia na przykład, czy jest podmiotem publicznym czy prywatnym. Jeżeli chodzi o cele wojskowe i obronne, takie wyłączenie jest uzasadnione zarówno art. 4 ust. 2 TUE, jak i specyfiką polityki obronnej państw członkowskich i wspólnej polityki obronnej Unii objętej tytułem V rozdział 2 Traktatu o Unii Europejskiej (TUE), które podlegają prawu międzynarodowemu publicznemu stanowiącemu zatem bardziej odpowiednie ramy prawne dla regulacji systemów sztucznej inteligencji w kontekście stosowania śmiercionośnej siły i innych systemów sztucznej inteligencji w kontekście działań wojskowych i obronnych. W odniesieniu do celów bezpieczeństwa narodowego wyłączenie to jest uzasadnione zarówno faktem, że za bezpieczeństwo narodowe wyłączną odpowiedzialność ponoszą państwa członkowskie zgodnie z art. 4 ust. 2 TUE, jak i faktem, że działania w zakresie bezpieczeństwa narodowego mają szczególny charakter, wiążą się ze szczególnymi potrzebami operacyjnymi i że zastosowanie do nich mają szczególne przepisy krajowe. Jeżeli jednak system sztucznej inteligencji opracowany, wprowadzony do obrotu, oddany do użytku lub wykorzystywany do celów wojskowych, obronnych lub celów bezpieczeństwa narodowego jest tymczasowo lub na stałe wykorzystywany do innych celów (na przykład do celów cywilnych lub humanitarnych, do celów egzekwowania prawa lub bezpieczeństwa publicznego), system taki objęty zostanie zakresem stosowania niniejszego rozporządzenia. W takim przypadku podmiot wykorzystujący taki system do celów inne niż cele wojskowe, obronne lub cele bezpieczeństwa narodowego zapewnia zgodność systemu z niniejszym rozporządzeniem, chyba że system ten jest już z nim zgodny. Systemy sztucznej inteligencji wprowadzane do obrotu lub oddawane do użytku do kilku celów – z których jeden należy do kategorii stanowiącej podstawę wykluczenia (tzn. cele wojskowe, obronne lub cele bezpieczeństwa narodowego), a pozostałe nie zaliczają się do takiej kategorii (np. cele cywilne, cele egzekwowania prawa itp.) – są objęte zakresem niniejszego rozporządzenia i dostawcy tych systemów powinni zapewnić zgodność z niniejszym rozporządzeniem. W takich przypadkach fakt, że system sztucznej inteligencji może wchodzić w zakres niniejszego rozporządzenia, nie powinien mieć wpływu na możliwość wykorzystywania – przez podmioty prowadzące działania dotyczące bezpieczeństwa narodowego, obrony i wojska, bez względu na rodzaj podmiotu prowadzącego te działania – systemów sztucznej inteligencji do celów bezpieczeństwa narodowego, celów wojskowych i obronnych, których wykorzystanie jest wyłączone z zakresu niniejszego rozporządzenia. System sztucznej inteligencji wprowadzany do obrotu do celów cywilnych lub do celów egzekwowania prawa, który jest wykorzystywany ze zmianami lub bez zmian do celów wojskowych, obronnych lub do celów bezpieczeństwa narodowego, nie powinien być objęty zakresem niniejszego rozporządzenia, bez względu na rodzaj podmiotu prowadzącego działania związane z tymi celami.

(12a) Niniejsze rozporządzenie nie powinno naruszać przepisów dotyczących odpowiedzialności usługodawców będących pośrednikami, określonych w dyrektywie 2000/31/WE Parlamentu Europejskiego i Rady [zmienionej aktem prawnym o usługach cyfrowych].

(12b) Niniejsze rozporządzenie nie powinno utrudniać działalności badawczo-rozwojowej i powinno respektować zasadę wolności nauki. Należy zatem wyłączyć z jego zakresu systemy sztucznej inteligencji opracowane i oddane do użytku wyłącznie do celów badań naukowych i rozwoju oraz zapewnić, by niniejsze rozporządzenie w inny sposób nie wpływało na badania naukowe i działalność rozwojową w zakresie systemów sztucznej inteligencji. Przepisy niniejszego rozporządzenia nie powinny mieć zastosowania również w odniesieniu do prowadzonej przez dostawców działalności badawczej ukierunkowanej na produkty. Pozostaje to bez uszczerbku dla obowiązku przestrzegania niniejszego rozporządzenia, gdy system sztucznej inteligencji objęty zakresem niniejszego rozporządzenia jest wprowadzany do obrotu lub oddawany do użytku w wyniku takiej działalności badawczo-rozwojowej, oraz dla stosowania przepisów dotyczących piaskownic regulacyjnych i testów w warunkach rzeczywistych. Ponadto bez uszczerbku dla powyższych zasad dotyczących systemów sztucznej inteligencji opracowanych wyłącznie do celów badań naukowych i rozwoju, wszelkie inne systemy sztucznej inteligencji, które mogą być wykorzystywane do prowadzenia wszelkich działań badawczo-rozwojowych, powinny podlegać przepisom niniejszego rozporządzenia. Bez względu na okoliczności wszelkie działania badawczo-rozwojowe powinny być prowadzone zgodnie z uznanymi normami etycznymi i zawodowymi dotyczącymi badań naukowych.

PUBLIC

(12c) W świetle charakteru i złożoności łańcucha wartości systemów sztucznej inteligencji konieczne jest objaśnienie roli podmiotów, które mogą przyczyniać się do rozwoju systemów sztucznej inteligencji, w szczególności systemów sztucznej inteligencji wysokiego ryzyka. Należy zwłaszcza wyjaśnić, że systemy sztucznej inteligencji ogólnego przeznaczenia to systemy, które zgodnie z przeznaczeniem przewidzianym przez dostawcę mają wykonywać funkcje ogólnego zastosowania, takie jak rozpoznawanie obrazów i mowy, i być wykorzystywane w wielu kontekstach. Mogą one być wykorzystywane jako samodzielne systemy sztucznej inteligencji wysokiego ryzyka lub stanowić element innych systemów sztucznej inteligencji wysokiego ryzyka. W związku z tym, ze względu na ich szczególny charakter oraz w celu zapewnienia sprawiedliwego podziału odpowiedzialności w całym łańcuchu wartości sztucznej inteligencji, systemy takie powinny podlegać proporcjonalnym i bardziej szczegółowym wymogom i obowiązkom na mocy niniejszego rozporządzenia, przy jednoczesnym zapewnianiu wysokiego poziomu ochrony praw podstawowych, zdrowia i bezpieczeństwa. Ponadto dostawcy systemów sztucznej inteligencji ogólnego przeznaczenia, niezależnie od tego, czy ich systemy są wykorzystywane jako systemy sztucznej inteligencji wysokiego ryzyka przez innych dostawców czy jako elementy systemów tego rodzaju, powinni współpracować, stosownie do przypadku, z dostawcami odpowiednich systemów sztucznej inteligencji wysokiego ryzyka, aby umożliwić im wypełnianie odpowiednich obowiązków wynikających z niniejszego rozporządzenia, oraz z właściwymi organami ustanowionymi na podstawie niniejszego rozporządzenia. W celu uwzględnienia specyfiki systemów sztucznej inteligencji ogólnego przeznaczenia oraz szybko zachodzących zmian rynkowych i technologicznych w tej dziedzinie Komisji należy powierzyć uprawnienia wykonawcze do szczegółowego określania i dostosowywania wymogów ustanowionych na podstawie niniejszego rozporządzenia do systemów sztucznej inteligencji ogólnego przeznaczenia oraz do określania informacji, które mają być udostępniane przez dostawców tego rodzaju systemów sztucznej inteligencji w celu umożliwiania dostawcom odnośnych systemów sztucznej inteligencji wysokiego ryzyka wypełnianie ich obowiązków wynikających z niniejszego rozporządzenia.

PUBLIC

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

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

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

PUBLIC

(16) Techniki manipulacyjne wykorzystujące sztuczną inteligencję mogą być wykorzystywane do nakłaniania osób do niepożądanych zachowań lub do 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 określonych systemów sztucznej inteligencji istotnie zniekształcających ludzkie zachowanie, co w rezultacie może prowadzić do wystąpienia szkód fizycznych lub psychicznych, jest szczególnie niebezpieczne, a zatem należy takich systemów zakazać. Systemy tego rodzaju wykorzystują elementy działające podprogowo, takie jak bodźce dźwiękowe, bodźce będące obrazami lub materiałami wideo, których nie można dostrzec, ponieważ bodźce takie wykraczają poza świadomą ludzką percepcję, lub stosują techniki podprogowe, które podważają lub ograniczają autonomię człowieka, podejmowanie przez niego decyzji lub swobodę wyboru w taki sposób, że osoby narażone na działanie takich systemów nie są świadome lub nawet jeśli są świadome, nie mogą sprawować nad nimi kontroli ani się im sprzeciwić, na przykład w przypadku interfejsów maszyna–mózg lub w przypadku rzeczywistości wirtualnej. Ponadto systemy sztucznej inteligencji mogą również w inny sposób wykorzystywać słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność w rozumieniu dyrektywy (UE) 2019/882 lub szczególną sytuację społeczną lub ekonomiczną, która może sprawić, że osoby te będą bardziej narażone na wykorzystywanie, takie jak osoby żyjące w skrajnym ubóstwie, osoby z mniejszości etnicznych lub religijnych. Takie systemy sztucznej inteligencji mogą być wprowadzane do obrotu, oddawane do użytku lub wykorzystywane w celu lub ze skutkiem istotnego zniekształcenia zachowania danej osoby, oraz w sposób, który powoduje lub może powodować szkodę fizyczną lub psychiczną tej osoby, lub innej osoby lub grupy osób, w tym szkody akumulujące się z biegiem czasu. Nie można zakładać, że zaistniał zamiar zniekształcenia zachowania, jeżeli zniekształcenie to wynika z czynników, które mają charakter zewnętrzny w stosunku do systemu sztucznej inteligencji i są poza kontrolą dostawcy lub użytkownika, a zatem ani dostawca ani użytkownik systemu sztucznej inteligencji nie mogą ich racjonalnie przewidzieć ani im przeciwdziałać. W każdym przypadku nie ma znaczenia, czy dostawca lub użytkownik mieli zamiar wyrządzić szkodę fizyczną lub psychiczną, istotny jest fakt, że szkoda wynika z opartych na sztucznej inteligencji praktyk polegających na manipulacji lub wykorzystywaniu. Zakazy dotyczące takich praktyk w zakresie sztucznej sztucznej inteligencji stanowią uzupełnienie przepisów zawartych w dyrektywie 2005/29/WE, w szczególności przepisu zakazującego stosowanie we wszelkich okolicznościach nieuczciwych praktyk handlowych powodujących dla konsumentów szkody ekonomiczne lub finansowe, niezależnie od tego, czy praktyki te stosuje się w kontekście systemów sztucznej inteligencji 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, takiego jak terapia psychologiczna w związku z chorobą psychiczną lub rehabilitacja fizyczna, gdy praktyki te są prowadzone zgodnie z mającymi zastosowanie normami i przepisami medycznymi. Ponadto powszechne i zasadne praktyki handlowe, które są zgodne z mającym zastosowanie prawem, nie powinny być same w sobie uznawane za szkodliwe, polegające na manipulacji praktyki z wykorzystaniem sztucznej inteligencji.

(17) Systemy sztucznej inteligencji, które umożliwiają prowadzenie przez organy publiczne lub podmioty prywatne oceny punktowej zachowań społecznych osób fizycznych, mogą prowadzić do dyskryminacyjnych wyników i wykluczenia pewnych grup. Mogą one naruszać prawo do godności i niedyskryminacji oraz wartości, jakimi są równość i sprawiedliwość. Takie systemy sztucznej inteligencji oceniają lub klasyfikują osoby fizyczne na podstawie ich zachowań społecznych w wielu kontekstach lub na podstawie znanych lub przewidywanych cech osobistych lub cech osobowości. Ocena społeczna wystawiona przez takie systemy sztucznej inteligencji może prowadzić do krzywdzącego lub niekorzystnego traktowania osób fizycznych lub całych ich grup w kontekstach społecznych, które nie są związane z kontekstem, w którym pierwotnie wygenerowano lub zgromadzono dane, lub do krzywdzącego traktowania, które jest nieproporcjonalne lub nieuzasadnione w stosunku do wagi ich zachowań społecznych. Należy zatem zakazać systemów sztucznej inteligencji, w których stosuje się takie niedopuszczalne praktyki oceny punktowej. Zakaz ten nie powinien mieć wpływu na legalne praktyki oceny osób fizycznych stosowane w jednym konkretnym celu lub w kilku konkretnych celach – zgodnie z prawem.

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

(19) Wykorzystanie tych systemów do celów egzekwowania prawa powinno zatem być zabronione, z wyjątkiem zamkniętej listy wąsko zdefiniowanych sytuacji, w których wykorzystanie to jest absolutnie konieczne do realizacji istotnego interesu publicznego, którego waga przeważa nad ryzykiem. Sytuacje te obejmują poszukiwanie potencjalnych ofiar przestępstw, w tym zaginionych dzieci; zapobieganie niektórym zagrożeniom życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu; oraz wykrywanie, lokalizowanie, identyfikowanie lub ściganie sprawców przestępstw lub podejrzanych o popełnienie przestępstw, o których mowa w decyzji ramowej Rady 2002/584/WSiSW[9], jeżeli przestępstwa te podlegają w danym państwie członkowskim karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, i zostały zdefiniowane w prawie danego państwa członkowskiego. Taki próg kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności zgodnie z prawem krajowym pozwala zapewnić, aby przestępstwo było na tyle poważne, by potencjalnie uzasadniać wykorzystanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym". Ponadto spośród 32 przestępstw wymienionych w decyzji ramowej Rady 2002/584/WSiSW niektóre mogą w praktyce mieć większe znaczenie niż inne, ponieważ można przewidzieć, że korzystanie ze zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" będzie w bardzo różnym stopniu konieczne i proporcjonalne do praktycznych celów wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy poszczególnych wymienionych przestępstw lub podejrzanego o popełnienie tych przestępstw, przy uwzględnieniu prawdopodobnych różnic w odniesieniu do powagi, prawdopodobieństwa i skali szkody lub ewentualnych negatywnych konsekwencji. 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 osoby, która podczas kontroli tożsamości odmawia identyfikacji lub nie jest 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.

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

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

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

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

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

(24) Wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane ze stosowaniem systemów sztucznej inteligencji do identyfikacji biometrycznej, inne niż w związku z wykorzystywaniem systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa zgodnie z przepisami niniejszego rozporządzenia, powinno nadal spełniać wszystkie wymogi wynikające z art. 10 dyrektywy (UE) 2016/680. Do celów innych niż egzekwowanie prawa art. 9 ust. 1 rozporządzenia (UE) 2016/679 i art. 10 ust. 1 rozporządzenia (UE) 2018/1725 zakazują przetwarzania danych biometrycznych w celu jednorazowego zidentyfikowania osoby fizycznej, chyba że spełnione są warunki określone w odnośnych ust. 2 tych artykułów.

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

(26) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i TFUE, Dania nie jest związana przepisami określonymi w art. 5 ust. 1 lit. d) oraz art. 5 ust. 2, 3 i 4 niniejszego rozporządzenia przyjętymi na podstawie art. 16 TFUE, które dotyczą przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdziały 4 lub 5 TFUE, ani przepisy te nie mają do niej zastosowania.

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

PUBLIC

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

(29) Jeżeli chodzi o systemy sztucznej inteligencji wysokiego ryzyka, które są związanymi z bezpieczeństwem elementami produktów lub systemów objętych zakresem rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008[10], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 167/2013[11], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013[12], dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE[13], dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/797[14], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858[15], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139[16] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2144[17] lub które same są takimi produktami lub systemami, wskazane jest wprowadzenie zmian do tych aktów w celu zapewnienia, aby przyjmując wszelkie stosowne przyszłe akty delegowane lub wykonawcze na podstawie wspomnianych aktów, Komisja uwzględniła – w oparciu o techniczną i regulacyjną charakterystykę każdego sektora oraz bez ingerowania w istniejące mechanizmy zarządzania, oceny zgodności i egzekwowania oraz powołane na mocy tych aktów organy – obowiązkowe wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka określone w niniejszym rozporządzeniu.

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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).

(30) W przypadku systemów sztucznej inteligencji, które są związanymi z bezpieczeństwem elementami produktów lub które same są produktami objętymi zakresem stosowania niektórych przepisów unijnego prawodawstwa harmonizacyjnego, systemy te należy klasyfikować jako systemy wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, jeżeli dany produkt jest poddawany procedurze oceny zgodności przez jednostkę oceniającą zgodność będącą osobą trzecią na podstawie tych stosownych przepisów unijnego prawodawstwa harmonizacyjnego. W szczególności produktami takimi są maszyny, zabawki, dźwigi, urządzenia i systemy ochronne przeznaczone do użytku w atmosferze potencjalnie wybuchowej, urządzenia radiowe, urządzenia ciśnieniowe, wyposażenie rekreacyjnych jednostek pływających, urządzenia kolei linowych, urządzenia spalające paliwa gazowe, wyroby medyczne oraz wyroby medyczne do diagnostyki in vitro.

(31) Klasyfikacja systemu sztucznej inteligencji jako systemu wysokiego ryzyka na podstawie niniejszego rozporządzenia nie powinna koniecznie oznaczać, że produkt, którego związanym z bezpieczeństwem elementem jest system sztucznej inteligencji, lub sam system sztucznej inteligencji jako produkt uznaje się za produkt „wysokiego ryzyka" zgodnie z kryteriami ustanowionymi w stosownym unijnym prawodawstwie harmonizacyjnym, które ma zastosowanie do tego produktu. Ma to miejsce w szczególności w przypadku rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745[18] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746[19], w których ocenę zgodności przeprowadzaną przez osobę trzecią przewidziano dla produktów średniego i wysokiego ryzyka.

[18] 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).

[19] 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).

(32) Jeżeli chodzi o systemy sztucznej inteligencji wysokiego ryzyka inne niż te, które są związanymi z bezpieczeństwem elementami produktów lub które same są produktami, należy je klasyfikować jako systemy wysokiego ryzyka, jeżeli w związku z ich przeznaczeniem stwarzają one wysokie ryzyko powstania szkody dla zdrowia i bezpieczeństwa lub praw podstawowych osób, biorąc pod uwagę zarówno skalę potencjalnych szkód, jak i prawdopodobieństwo ich wystąpienia, oraz jeżeli są one wykorzystywane w szeregu ściśle określonych z góry obszarów wskazanych w rozporządzeniu. Identyfikacja tych systemów opiera się na tej samej metodyce i tych samych kryteriach, które przewidziano także dla wszelkich przyszłych zmian w wykazie systemów sztucznej inteligencji wysokiego ryzyka. Ważne jest również wyjaśnienie, że w ramach scenariuszy wysokiego ryzyka, o których mowa w załączniku III, mogą istnieć systemy, które nie generują istotnego ryzyka dla interesów prawnych chronionych w ramach tych scenariuszy, z uwagi na wyniki działania danego systemu sztucznej inteligencji. Dlatego też system sztucznej inteligencji generujący dane wyniki powinien być uznany za system wysokiego ryzyka jedynie wtedy, gdy wyniki te mają duże znaczenie (tj. nie mają wyłącznie pomocniczego charakteru) w odniesieniu do odpowiedniego działania lub decyzji, tak że mogą stworzyć istotne ryzyko dla chronionych interesów prawnych. Na przykład jeżeli informacje przekazywane człowiekowi przez systemy sztucznej inteligencji polegają na profilowaniu osób fizycznych w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679, art. 3 pkt 4 dyrektywy (UE) 2016/680 oraz art. 3 pkt. 5 rozporządzenia (UE) 2018/1725, informacji takich nie należy zazwyczaj uznawać za mające charakter pomocniczy w kontekście systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III. Jeżeli jednak wynik działania systemu sztucznej inteligencji ma jedynie znikome lub niewielkie znaczenie dla działania człowieka lub jego decyzji, system taki można uznać za czysto pomocniczy, w tym na przykład systemy sztucznej inteligencji wykorzystywane do tłumaczenia w celach informacyjnych lub do zarządzania dokumentami.

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

(34) W odniesieniu do zarządzania infrastrukturą krytyczną i jej funkcjonowania wskazane jest klasyfikowanie jako systemy wysokiego ryzyka systemów sztucznej inteligencji, które mają być użytkowane jako związane z bezpieczeństwem elementy procesów zarządzania i obsługi krytycznej infrastruktury cyfrowej wymienionej w załączniku I pkt 8 dyrektywy w sprawie odporności podmiotów krytycznych, ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło i energię elektryczną, ponieważ ich awaria lub nieprawidłowe działanie mogą stanowić zagrożenie dla życia i zdrowia osób na dużą skalę i prowadzić do znacznych zakłóceń w zwykłym prowadzeniu działalności społecznej i gospodarczej. Związane z bezpieczeństwem elementy infrastruktury krytycznej, w tym krytycznej infrastruktury cyfrowej, to systemy, które są wykorzystywane do bezpośredniej ochrony fizycznej integralności infrastruktury krytycznej lub zdrowia i bezpieczeństwa osób i mienia, ale które nie są konieczne do funkcjonowania systemu. Awaria lub nieprawidłowe działanie takich elementów mogą bezpośrednio prowadzić do zagrożenia fizycznej integralności infrastruktury krytycznej, a co za tym idzie, do zagrożeń dla zdrowia i bezpieczeństwa osób i mienia. Elementy przeznaczone do stosowania wyłącznie do celów cyberbezpieczeństwa nie powinny być kwalifikowane jako elementy bezpieczeństwa. Jako przykłady elementów bezpieczeństwa takiej infrastruktury krytycznej można wymienić systemy monitorowania ciśnienia wody lub systemy sterowania alarmem przeciwpożarowym w centrach przetwarzania danych w chmurze.

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

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

PUBLIC

(37) Innym obszarem, w którym stosowanie systemów sztucznej inteligencji zasługuje na szczególną uwagę, jest dostęp do niektórych podstawowych usług i świadczeń prywatnych i publicznych niezbędnych ludziom do pełnego uczestnictwa w życiu społecznym lub do poprawy poziomu życia oraz korzystanie z tych usług i świadczeń. W szczególności systemy sztucznej inteligencji wykorzystywane do przeprowadzania punktowej oceny kredytowej lub oceny zdolności kredytowej osób fizycznych należy klasyfikować jako systemy wysokiego ryzyka, ponieważ decydują one o dostępie tych osób do zasobów finansowych lub podstawowych usług, takich jak mieszkalnictwo, energia elektryczna i usługi telekomunikacyjne. Systemy sztucznej inteligencji wykorzystywane w tym celu mogą prowadzić do dyskryminacji osób lub grup i utrwalać historyczne wzorce dyskryminacji, na przykład ze względu na pochodzenie rasowe lub etniczne, niepełnosprawność, wiek, orientację seksualną, lub powodować powstawanie dyskryminujących skutków w nowej postaci. Biorąc pod uwagę bardzo ograniczoną skalę skutków i dostępność na rynku alternatywnych rozwiązań, wskazane jest wyłączenie systemów sztucznej inteligencji stosowanych do oceny zdolności kredytowej i punktowej oceny kredytowej, w przypadku gdy są one oddawane do użytku do własnych celów przez mikroprzedsiębiorstwa lub małe przedsiębiorstwa zdefiniowane w załączniku do zalecenia Komisji 2003/361/WE. Osoby fizyczne ubiegające się o podstawowe świadczenia i usługi w ramach pomocy publicznej zapewniane przez organy publiczne lub korzystające z takich świadczeń i usług są zazwyczaj zależne od tych świadczeń i usług oraz znajdują się w słabszym położeniu względem odpowiedzialnych organów. Jeżeli systemy sztucznej inteligencji są wykorzystywane do ustalenia, czy organy powinny odmówić takich świadczeń i usług, ograniczyć je, cofnąć lub odzyskać, w tym 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 odwoławczego. W związku z tym systemy te należy klasyfikować jako systemy wysokiego ryzyka. Niniejsze rozporządzenie nie powinno jednak utrudniać rozwoju i stosowania innowacyjnych rozwiązań w administracji publicznej, która może odnieść korzyści z powszechniejszego wykorzystywania spełniających odnośne wymogi i bezpiecznych systemów sztucznej inteligencji, pod warunkiem że systemy te nie stwarzają wysokiego ryzyka dla osób prawnych i fizycznych. Ponadto systemy sztucznej inteligencji wykorzystywane do wysyłania służb pierwszej pomocy w sytuacjach nadzwyczajnych lub ustalania priorytetów w ich wysyłaniu również należy klasyfikować jako systemy wysokiego ryzyka, ponieważ służą one do podejmowania decyzji o krytycznym znaczeniu dla życia i zdrowia osób oraz ich mienia. Systemy sztucznej inteligencji są również w coraz większym stopniu wykorzystywane do oceny ryzyka w odniesieniu do osób fizycznych i ustalania stawek w przypadku ubezpieczeń na życie i ubezpieczeń zdrowotnych, co – jeżeli nie zostaną one odpowiednio zaprojektowane, opracowane i nie będą odpowiednio wykorzystywane – może prowadzić do poważnych konsekwencji dla życia i zdrowia ludzi, w tym wykluczenia finansowego i dyskryminacji. Aby zapewnić spójne podejście w sektorze usług finansowych, wyżej wymieniony wyjątek powinien mieć zastosowanie do mikroprzedsiębiorstw lub małych przedsiębiorstw w kontekście własnych potrzeb w zakresie, w jakim one same dostarczają i oddają do użytku system sztucznej inteligencji do celów sprzedaży własnych produktów ubezpieczeniowych.

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

(39) Systemy sztucznej inteligencji wykorzystywane w zarządzaniu migracją, azylem i kontrolą graniczną mają wpływ na osoby, które często znajdują się w szczególnie trudnej sytuacji i które są zależne od rezultatów działań właściwych organów publicznych. Dokładność, niedyskryminujący charakter i przejrzystość systemów sztucznej inteligencji wykorzystywanych w tych kontekstach są zatem szczególnie istotne w celu zapewnienia poszanowania praw podstawowych osób, na które system może mieć wpływ, w szczególności ich prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji. Za systemy wysokiego ryzyka należy zatem uznać systemy sztucznej inteligencji przeznaczone do wykorzystywania przez właściwe organy publiczne odpowiedzialne za wykonywanie zadań w dziedzinach zarządzania migracją, azylem i kontrolą graniczną jako poligrafy i podobne narzędzia lub do wykrywania stanu emocjonalnego osoby fizycznej; w celu oceny niektórych zagrożeń stwarzanych przez osoby fizyczne wjeżdżające na terytorium państwa członkowskiego lub ubiegające się o wizę lub azyl; *w* celu udzielenia pomocy właściwym organom publicznym przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do celu, jakim jest ustalenie kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu. Systemy sztucznej inteligencji w obszarze zarządzania migracją, azylem i kontrolą graniczną objęte niniejszym rozporządzeniem powinny być zgodne z odpowiednimi wymogami proceduralnymi określonymi w dyrektywie Parlamentu Europejskiego i Rady 2013/32/UE[20], rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 810/2009[21] i innych właściwych przepisach.

[20] 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).

[21] 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).

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

(41) Faktu, że dany system sztucznej inteligencji został sklasyfikowany jako system wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, nie należy interpretować jako wskazującego na to, że korzystanie z tego systemu jest zgodne z prawem na gruncie innych aktów prawa Unii lub prawa krajowego zgodnego z prawem Unii, na przykład w zakresie ochrony danych osobowych, stosowania poligrafów i podobnych narzędzi lub innych systemów służących wykrywaniu stanu emocjonalnego osób fizycznych. Każde takie wykorzystanie należy kontynuować wyłącznie w sposób zgodny z mającymi zastosowanie wymogami wynikającymi z Karty oraz z mającymi zastosowanie aktami prawa wtórnego Unii i prawa krajowego. Niniejszego rozporządzenia nie należy rozumieć jako ustanawiającego podstawę prawną przetwarzania danych osobowych, w tym w stosownych przypadkach szczególnych kategorii danych osobowych, o ile w niniejszym rozporządzeniu wyraźnie nie przewidziano inaczej.

(42) Aby ograniczyć ryzyko stwarzane przez systemy sztucznej inteligencji wysokiego ryzyka wprowadzone do obrotu lub w inny sposób oddawane do użytku na rynku unijnym, należy wprowadzić pewne obowiązkowe wymogi, z uwzględnieniem przeznaczenia systemu oraz zgodnie z systemem zarządzania ryzykiem, który ma zostać ustanowiony przez dostawcę. W szczególności system zarządzania ryzykiem powinien obejmować ciągły, iteracyjny proces planowany i realizowany przez cały cykl życia systemu sztucznej inteligencji wysokiego ryzyka. Proces ten powinien zapewniać, aby dostawca identyfikował i analizował zagrożenia dla zdrowia, bezpieczeństwa i praw podstawowych osób, na które system może mieć wpływ, w świetle jego przeznaczenia, z uwzględnieniem ewentualnych zagrożeń wynikających z interakcji między systemem sztucznej inteligencji a środowiskiem, w którym działa, oraz na tej podstawie przyjmował odpowiednie środki zarządzania ryzykiem w świetle aktualnego stanu techniki.

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

(44) Wysoka jakość danych ma zasadnicze znaczenie dla skuteczności działania wielu systemów sztucznej inteligencji, w szczególności w przypadku stosowania technik obejmujących trenowanie modeli, w celu zapewnienia, aby system sztucznej inteligencji wysokiego ryzyka działał zgodnie z przeznaczeniem i bezpiecznie oraz aby nie stał się źródłem zakazanej przez prawo Unii dyskryminacji. Wysokiej jakości zbiory danych treningowych, walidacyjnych i testowych wymagają wdrożenia odpowiednich praktyk w zakresie zarządzania danymi. Zbiory danych treningowych, walidacyjnych i testowych powinny być wystarczająco adekwatne, reprezentatywne oraz charakteryzować się odpowiednimi właściwościami statystycznymi, w tym w odniesieniu do osób lub grup osób, wobec których system sztucznej inteligencji wysokiego ryzyka ma być wykorzystywany. Te zbiory danych powinny być również jak najbardziej wolne od błędów i kompletne z punktu widzenia przeznaczenia systemu sztucznej inteligencji, z uwzględnieniem – w sposób proporcjonalny – wykonalności technicznej i aktualnego stanu techniki, dostępności danych i wdrożenia odpowiednich środków zarządzania ryzykiem, tak aby należycie wyeliminować ewentualne niedociągnięcia w zbiorach danych. Wymóg, aby zbiory danych były kompletne i wolne od błędów, nie powinien wpływać na stosowanie technik ochrony prywatności w kontekście rozwoju i testowania systemów sztucznej inteligencji. Zbiory danych treningowych, walidacyjnych i testowych powinny uwzględniać – w zakresie wymaganym w zależności od ich przeznaczenia – cechy, właściwości lub elementy, które są specyficzne dla określonego kontekstu geograficznego, behawioralnego lub funkcjonalnego lub okoliczności, w których system sztucznej inteligencji ma być wykorzystywany. Aby chronić prawa innych osób przed dyskryminacją, która może wynikać z tendencyjności systemów sztucznej inteligencji, dostawcy powinni mieć możliwość przetwarzania również szczególnych kategorii danych osobowych przez wzgląd na istotny interes publiczny w rozumieniu art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679 oraz art. 10 ust. 2 lit. g) rozporządzenia (UE) 2018/1725 w celu zapewnienia monitorowania, wykrywania i eliminowania tendencyjności w systemach sztucznej inteligencji wysokiego ryzyka.

(44a) Stosując zasady, o których mowa w art. 5 ust. 1 lit. c) rozporządzenia 2016/679 i art. 4 ust. 1 lit. c) rozporządzenia 2018/1725, w szczególności zasadę minimalizacji danych, w odniesieniu do zbiorów danych treningowych, walidacyjnych i testowych na podstawie niniejszego rozporządzenia, należy w odpowiednim stopniu uwzględnić cały cykl życia systemu sztucznej inteligencji.

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

(46) Dysponowanie informacjami na temat tego, w jaki sposób opracowano systemy sztucznej inteligencji wysokiego ryzyka i jak działają one w całym cyklu życia, ma zasadnicze znaczenie dla weryfikacji zgodności z wymogami określonymi w niniejszym rozporządzeniu. Wymaga to prowadzenia rejestrów zdarzeń oraz zapewnienia dostępności dokumentacji technicznej zawierającej informacje niezbędne do oceny zgodności systemu sztucznej inteligencji z odpowiednimi wymogami. Informacje takie powinny obejmować ogólne właściwości, możliwości i ograniczenia systemu, algorytmy, dane, procesy związane z trenowaniem, testowaniem i walidacją, a także dokumentację dotyczącą odpowiedniego systemu zarządzania ryzykiem. Dokumentacja techniczna powinna podlegać aktualizacji. Ponadto dostawcy lub użytkownicy powinni prowadzić rejestry zdarzeń generowane automatycznie przez system sztucznej inteligencji wysokiego ryzyka, w tym na przykład dane wyjściowe, datę i godzinę uruchomienia itp., w zakresie, w jakim taki system i powiązane rejestry znajdują się pod ich kontrolą, przez okres, jaki będzie odpowiedni, by umożliwić im wypełnienie ich obowiązków.

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

(48) Systemy sztucznej inteligencji wysokiego ryzyka należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie. W tym celu przed wprowadzeniem systemu do obrotu lub jego oddaniem do użytku dostawca systemu powinien określić odpowiednie środki związane z nadzorem ze strony człowieka. W szczególności, w stosownych przypadkach, takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka–operatora systemu, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru ze strony człowieka, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji. 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 użytkownik nie mógł podejmować żadnych działań ani decyzji na podstawie identyfikacji wynikającej z systemu, chyba że zostało to oddzielnie zweryfikowane i potwierdzone przez co najmniej dwie osoby fizyczne. Osoby te mogą pochodzić z co najmniej jednego podmiotu i może być wśród nich osoba obsługująca system lub z niego korzystająca. Wymóg ten nie powinien powodować niepotrzebnych obciążeń ani opóźnień i może wystarczyć, że odrębne weryfikacje dokonywane przez różne osoby będą automatycznie rejestrowane w wygenerowanych przez system rejestrach zdarzeń.

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

(50) Kluczowym wymogiem dotyczącym systemów sztucznej inteligencji wysokiego ryzyka jest solidność techniczna. Powinny być odporne na szkodliwe lub w inny sposób niepożądane zachowania, które mogą wynikać z ograniczeń w systemach lub środowisku, w którym te systemy działają (np. błędy, usterki, niespójności, nieoczekiwane sytuacje). Systemy sztucznej inteligencji wysokiego ryzyka powinny zatem być projektowane i rozwijane z wykorzystaniem odpowiednich rozwiązań technicznych w celu zapobiegania szkodliwym lub w inny sposób niepożądanym zachowaniom lub ich minimalizowania, takich jak na przykład mechanizmy umożliwiające bezpieczne przerwanie działania systemu (plany zapewniające przejście systemu w stan bezpieczny) w przypadku wystąpienia pewnych anomalii lub gdy działanie odbywa się poza określonymi wcześniej granicami. Brak ochrony przed tymi zagrożeniami może mieć konsekwencje dla bezpieczeństwa lub negatywnie wpłynąć na prawa podstawowe, na przykład z powodu błędnych decyzji bądź nieprawidłowych lub tendencyjnych wyników działania generowanych przez system sztucznej inteligencji.

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

(52) W ramach unijnego prawodawstwa harmonizacyjnego przepisy mające zastosowanie do wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji wysokiego ryzyka należy ustanowić zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku produktów[22], decyzją Parlamentu Europejskiego i Rady nr 768/2008/WE w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu[23] oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/1020 w sprawie nadzoru rynku i zgodności produktów („nowe ramy prawne")[24].

(52a) Zgodnie z zasadami nowych ram prawnych należy określić szczegółowe obowiązki odpowiednich operatorów w łańcuchu wartości sztucznej inteligencji, aby zagwarantować pewność prawa i ułatwić przestrzeganie przepisów. W niektórych sytuacjach operatorzy ci mogą pełnić więcej niż jedną rolę jednocześnie i w związku z tym powinni łącznie wypełniać wszystkie odpowiednie obowiązki związane z tymi rolami. Na przykład operator może występować jednocześnie jako dystrybutor i importer.

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

---

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

23 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).

24 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (tekst mający znaczenie dla EOG) (Dz.U. L 169 z 25.6.2019, s. 1–44).

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

(54a) Aby zapewnić pewność prawa, należy wyjaśnić, że pod pewnymi określonymi warunkami każda osoba fizyczna lub prawna powinna zostać uznana za dostawcę nowego systemu sztucznej inteligencji wysokiego ryzyka i w związku z tym przyjąć na siebie wszystkie odpowiednie obowiązki. Miałoby to miejsce na przykład w sytuacji, gdyby osoba ta umieszczała swoje imię i nazwisko lub znak towarowy na systemie sztucznej inteligencji wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku, lub jeżeli osoba ta zmodyfikowałaby przeznaczenie wprowadzonego już do obrotu lub oddanego do użytku systemu sztucznej inteligencji niebędącego systemem wysokiego ryzyka w taki sposób, że ten zmodyfikowany system stałby się systemem sztucznej inteligencji wysokiego ryzyka. Przepisy te powinny mieć zastosowanie bez uszczerbku dla bardziej szczegółowych przepisów ustanowionych w niektórych sektorowych przepisach nowych ram prawnych, wraz z którymi niniejsze rozporządzenie powinno być stosowane łącznie. Na przykład do systemów sztucznej inteligencji wysokiego ryzyka będących wyrobami medycznymi w rozumieniu rozporządzenia 745/2017, powinien nadal mieć zastosowanie art. 16 ust. 2 tego rozporządzenia stwierdzający, że niektórych zmian nie należy uznawać za za modyfikację wyrobu, która może wpłynąć na jego zgodność z obowiązującymi wymogami.

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

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

(56a) W przypadku dostawców, którzy nie mają siedziby w Unii, kluczową rolę w zapewnianiu zgodności systemów sztucznej inteligencji wysokiego ryzyka wprowadzanych przez tych dostawców do obrotu lub oddawanych do użytku w Unii oraz w pełnieniu funkcji osoby kontaktowej mającej siedzibę w Unii odgrywa upoważniony przedstawiciel. Biorąc pod uwagę tę kluczową rolę oraz w celu zapewnienia przyjęcia odpowiedzialności do celów egzekwowania niniejszego rozporządzenia, należy wprowadzić odpowiedzialność solidarną upoważnionego przedstawiciela wraz z dostawcą za wadliwe systemy sztucznej inteligencji wysokiego ryzyka. Odpowiedzialność upoważnionego przedstawiciela przewidziana w niniejszym rozporządzeniu pozostaje bez uszczerbku dla przepisów dyrektywy 85/374/EWG w sprawie odpowiedzialności za produkty wadliwe.

(57) [skreśla się]

(58) Ze względu na naturę systemów sztucznej inteligencji oraz zagrożenia dla bezpieczeństwa i praw podstawowych, jakie mogą wiązać się z ich wykorzystywaniem, w tym uwzględniając potrzebę zapewnienia właściwego monitorowania skuteczności działania systemu sztucznej inteligencji w warunkach rzeczywistych, należy określić szczególne obowiązki użytkowników. Użytkownicy powinni w szczególności korzystać z systemów sztucznej inteligencji wysokiego ryzyka zgodnie z instrukcjami obsługi, a w stosownych przypadkach należy przewidzieć określone inne obowiązki w odniesieniu do monitorowania funkcjonowania systemów sztucznej inteligencji oraz rejestrowania zdarzeń. Obowiązki te powinny pozostawać bez uszczerbku dla innych obowiązków użytkowników w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka na mocy prawa Unii lub prawa krajowego i nie powinny mieć zastosowania, w przypadku gdy stosowanie tych systemów odbywa się w ramach osobistej działalności pozazawodowej.

(58a) Należy wyjaśnić, że niniejsze rozporządzenie nie wpływa na wynikające z prawa Unii w zakresie ochrony danych osobowych obowiązki dostawców i użytkowników systemów sztucznej inteligencji, którzy pełnią funkcję administratorów danych lub podmiotów przetwarzających, w zakresie, w jakim projektowanie, opracowywanie lub wykorzystywanie systemów sztucznej inteligencji wiąże się z przetwarzaniem danych osobowych. Należy również wyjaśnić, że osoby, których dane dotyczą, zatrzymują wszystkie prawa i gwarancje przyznane im na mocy takiego prawa Unii, w tym prawa związane z całkowicie zautomatyzowanym podejmowaniem decyzji w indywidualnych przypadkach, w tym z profilowaniem. Zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów sztucznej inteligencji ustanowione na mocy niniejszego rozporządzenia powinny ułatwiać skuteczne wdrażanie i umożliwiać korzystanie przez osoby, których dane dotyczą, z praw i innych środków ochrony prawnej zagwarantowanych na mocy prawa Unii dotyczącego ochrony danych osobowych i innych praw podstawowych.

(59) [skreśla się]

(60) [skreśla się]

PUBLIC

(61) Kluczową rolę w dostarczaniu dostawcom rozwiązań technicznych – zgodnie ze stanem techniki – w celu zapewnienia zgodności z niniejszym rozporządzeniem powinna odgrywać normalizacja. Zgodność z normami zharmonizowanymi określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1025/2012[25], które z założenia mają odzwierciedlać stan techniki, powinna stanowić dla dostawców sposób wykazania zgodności z wymogami niniejszego rozporządzenia. Jednak w przypadku braku odpowiednich odniesień do norm zharmonizowanych Komisja powinna mieć możliwość ustanowienia, w drodze aktów wykonawczych, wspólnych specyfikacji w odniesieniu do niektórych wymogów określonych w niniejszym rozporządzeniu jako wyjątkowego rozwiązania awaryjnego, aby ułatwić dostawcy spełnienie wymogów niniejszego rozporządzenia, w przypadku gdy proces normalizacji jest zablokowany lub gdy występują opóźnienia w ustanowieniu odpowiedniej normy zharmonizowanej. Jeżeli takie opóźnienie wynika ze złożoności technicznej danej normy, Komisja powinna rozważyć tę kwestię, zanim rozpocznie analizę dotyczącą ustanowienia wspólnych specyfikacji. Odpowiedni udział małych i średnich przedsiębiorstw w opracowywaniu norm wspierających wdrażanie niniejszego rozporządzenia ma zasadnicze znaczenie dla promowania innowacji i konkurencyjności w dziedzinie sztucznej inteligencji w Unii. Taki udział powinien być należycie zapewniony zgodnie z art. 5 i 6 rozporządzenia 1025/2012.

[25] 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).

(61a) Stosownym jest, by bez uszczerbku dla stosowania zharmonizowanych norm i wspólnych specyfikacji dostawcy korzystali z domniemania zgodności z odpowiednim wymogiem dotyczącym danych, jeżeli ich system sztucznej inteligencji wysokiego ryzyka został wytrenowany i przetestowany na danych odzwierciedlających szczególne uwarunkowania geograficzne, behawioralne lub funkcjonalne, w których system sztucznej inteligencji ma być wykorzystywany. Podobnie, zgodnie z art. 54 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881, zakłada się, że systemy sztucznej inteligencji wysokiego ryzyka, które zostały certyfikowane lub w odniesieniu do których wydano deklarację zgodności w ramach systemu certyfikacji cyberbezpieczeństwa na podstawie tego rozporządzenia i do których odniesienia opublikowano w Dzienniku Urzędowym Unii Europejskiej, spełniają wymóg w zakresie cyberbezpieczeństwa określony w niniejszym rozporządzeniu. Pozostaje to bez uszczerbku dla dobrowolnego charakteru tego systemu certyfikacji cyberbezpieczeństwa.

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

PUBLIC

(63) Aby zminimalizować obciążenie dla operatorów i uniknąć ewentualnego powielania działań, zgodność systemów sztucznej inteligencji wysokiego ryzyka, które wchodzą w zakres obowiązującego unijnego prawodawstwa harmonizacyjnego zgodnie z podejściem opartym na nowych ramach prawnych, z wymogami niniejszego rozporządzenia należy oceniać w ramach oceny zgodności przewidzianej już w tym prawodawstwie. Stosowanie wymogów niniejszego rozporządzenia nie powinno zatem wpływać na szczególną logikę, metodykę lub ogólną strukturę oceny zgodności określone w odpowiednim szczegółowym prawodawstwie opartym na nowych ramach prawnych. Podejście to znajduje pełne odzwierciedlenie w zależnościach między niniejszym rozporządzeniem a [rozporządzeniem w sprawie maszyn]. Chociaż w wymogach niniejszego rozporządzenia uwzględniono zagrożenia dla bezpieczeństwa związane z systemami sztucznej inteligencji zapewniającymi funkcje bezpieczeństwa w maszynach, określone wymogi szczegółowe zawarte w [rozporządzeniu w sprawie maszyn] zapewnią bezpieczną integrację systemu sztucznej inteligencji z całą maszyną w sposób, który nie zagraża bezpieczeństwu maszyny jako całości. W [rozporządzeniu w sprawie maszyn] zawarto tę samą definicję systemu sztucznej inteligencji co w niniejszym rozporządzeniu. W odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka związanych z produktami objętymi rozporządzeniami 745/2017 i 746/2017 w sprawie wyrobów medycznych konieczność zastosowania się do wymogów niniejszego rozporządzenia nie powinna naruszać logiki zarządzania ryzykiem i oceny stosunku korzyści do ryzyka przeprowadzanych w ramach prawnych dotyczących wyrobów medycznych, a także tę logikę i ocenę uwzględniać.

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

(65) Do celów przeprowadzanej przez osobę trzecią oceny zgodności systemów sztucznej inteligencji przeznaczonych do zdalnej identyfikacji biometrycznej osób właściwe organy krajowe powinny dokonać na podstawie niniejszego rozporządzenia notyfikacji jednostek notyfikowanych, pod warunkiem że spełniają one szereg wymogów, w szczególności dotyczących niezależności, kompetencji i braku konfliktu interesów. 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 decyzji 768/2008.

(66) 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 sztucznej inteligencji wysokiego ryzyka z niniejszym rozporządzeniem (np. zmiana systemu operacyjnego lub architektury oprogramowania), lub gdy zmienia się przeznaczenie danego systemu – uznać ten system sztucznej inteligencji za nowy system sztucznej inteligencji, który powinien zostać poddany nowej ocenie zgodności. Za istotną zmianę nie należy jednak uznawać zmian w algorytmie oraz w skuteczności działania systemu sztucznej inteligencji, który po wprowadzeniu do obrotu lub oddaniu do użytku nadal się „uczy” (tj. automatycznie dostosowuje sposób wykonywania funkcji), pod warunkiem że zmiany te zostały z góry zaplanowane przez dostawcę i ocenione w momencie przeprowadzania oceny zgodności.

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

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

(69) Aby ułatwić pracę Komisji i państw członkowskich w dziedzinie sztucznej inteligencji, jak również zwiększyć przejrzystość wobec ogółu społeczeństwa, dostawców systemów sztucznej inteligencji wysokiego ryzyka innych niż systemy powiązane z produktami objętymi zakresem odpowiedniego istniejącego unijnego prawodawstwa harmonizacyjnego należy zobowiązać, by dokonali swojej rejestracji oraz rejestracji informacji na temat swoich systemów sztucznej inteligencji wysokiego ryzyka w unijnej bazie danych, którą utworzy i którą zarządzać będzie Komisja. Przed zastosowaniem systemu sztucznej inteligencji wysokiego ryzyka wymienionego w załączniku III użytkownicy systemów sztucznej inteligencji wysokiego ryzyka będący publicznymi organami, agencjami lub jednostkami organizacyjnymi, z wyjątkiem organów ścigania, organów kontroli granicznej, organów imigracyjnych lub organów odpowiedzialnych za udzielanie azylu, oraz organy będące użytkownikami systemów sztucznej inteligencji wysokiego ryzyka w obszarze infrastruktury krytycznej, również rejestrują się w takiej bazie danych i wybierają system, który zamierzają wykorzystywać. Komisja powinna być administratorem tej bazy danych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725[26]. W celu zapewnienia pełnej funkcjonalności tej bazy danych po jej wdrożeniu procedura ustanawiania bazy danych powinna obejmować opracowanie przez Komisję specyfikacji funkcjonalnych oraz sprawozdanie z niezależnego audytu.

[26] 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).

(70) Niektóre systemy sztucznej inteligencji przeznaczone do wchodzenia w interakcję z osobami fizycznymi lub tworzenia treści mogą stwarzać szczególne ryzyko podawania się za inną osobę lub świadomego wprowadzania w błąd, niezależnie od tego, czy kwalifikują się jako systemy wysokiego ryzyka, czy też nie. W pewnych okolicznościach korzystanie z tych systemów powinno zatem podlegać szczególnym obowiązkom w zakresie przejrzystości bez uszczerbku dla wymogów i obowiązków określonych dla systemów sztucznej inteligencji wysokiego ryzyka. W szczególności osoby fizyczne powinny być informowane o tym, że prowadzą interakcję z systemem sztucznej inteligencji, chyba że jest to oczywiste z punktu widzenia osoby fizycznej, która jest dostatecznie poinformowana, uważna i ostrożna, z uwzględnieniem okoliczności i kontekstu korzystania. Przy realizacji takiego obowiązku należy – w zakresie, w jakim system sztucznej inteligencji ma również wchodzić w interakcję z tymi grupami – uwzględnić cechy osób należących do grup szczególnie wrażliwych ze względu na ich wiek lub niepełnosprawność. Ponadto osoby fizyczne powinny być powiadamiane, jeżeli są poddawane działaniu systemów, które poprzez przetwarzanie ich danych biometrycznych mogą zidentyfikować lub odgadnąć 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 lub inne aspekty, takie jak orientacja seksualna lub orientacja polityczna. Tego rodzaju informacje i powiadomienia należy przekazywać w formatach dostępnych dla osób z niepełnosprawnościami. Ponadto użytkownicy, którzy wykorzystują system sztucznej inteligencji do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi w sposób sprawiający, że zaczynają one łudząco przypominać istniejące osoby, miejsca lub zdarzenia, przez co dana osoba mogłaby niesłusznie uznać je za autentyczne, powinny ujawnić, że dane treści zostały sztucznie stworzone lub zmanipulowane poprzez odpowiednie oznakowanie wyniku działania sztucznej inteligencji i ujawnienie, że źródłem danych treści jest system sztucznej inteligencji. Przestrzeganie obowiązków informacyjnych, o których mowa powyżej, nie powinno być interpretowane jako wskazanie, że korzystanie z systemu lub jego wyników jest zgodne z prawem na podstawie niniejszego rozporządzenia lub innych przepisów prawa Unii i prawa państwa członkowskiego, i powinno pozostawać bez uszczerbku dla innych ustanowionych w prawie Unii lub prawie krajowym obowiązków w zakresie przejrzystości spoczywających na użytkownikach systemów sztucznej inteligencji. Nie należy ponadto rozumieć, że korzystanie z systemu lub jego wyników ogranicza prawo do wolności wypowiedzi i prawo do wolności sztuk i nauk zagwarantowane w Karcie praw podstawowych UE, w szczególności ww przypadku, gdy treści te stanowią część dzieła lub programu mającego wyraźnie charakter twórczy, satyryczny, artystyczny lub fikcyjny, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.

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

PUBLIC

(72) Piaskownice regulacyjne w zakresie sztucznej inteligencji powinny mieć na celu: wspieranie innowacji w zakresie sztucznej inteligencji poprzez ustanowienie kontrolowanego środowiska do eksperymentów i testów na etapie rozwoju i przed wprowadzeniem do obrotu, z myślą o zapewnieniu zgodności innowacyjnych systemów sztucznej inteligencji z niniejszym rozporządzeniem oraz z innymi odnośnymi przepisami Unii i państw członkowskich; zwiększenie pewności prawa dla innowatorów, a także usprawnienie nadzoru ze strony właściwych organów oraz podnoszenie poziomu ich wiedzy na temat możliwości, pojawiających się rodzajów ryzyka oraz skutków związanych z wykorzystywaniem sztucznej inteligencji, a także przyspieszenie dostępu do rynków, w tym poprzez usuwanie barier dla małych i średnich przedsiębiorstw (MŚP), w tym przedsiębiorstw typu start-up. Uczestnictwo w piaskownicy regulacyjnej w zakresie sztucznej inteligencji powinno koncentrować się na kwestiach, które powodują niepewność prawa dla dostawców i potencjalnych dostawców w zakresie innowacji, eksperymentowania ze sztuczną inteligencją w Unii oraz powinno przyczyniać się do opartego na dowodach uczenia się działań regulacyjnych. Nadzór nad systemami sztucznej inteligencji w piaskownicy regulacyjnej w zakresie sztucznej inteligencji powinien zatem obejmować ich opracowywanie, trenowanie, testowanie i walidację przed wprowadzeniem systemów do obrotu lub oddaniem do użytku, a także pojęcie i występowanie istotnych zmian, które mogą wymagać nowej procedury oceny zgodności. 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 sztucznej inteligencji, takich jak krajowe lub europejskie organizacje normalizacyjne, jednostki notyfikowane, ośrodki testowo-doświadczalne, laboratoria badawcze i doświadczalne, centra innowacji oraz organizacje zrzeszające odpowiednie zainteresowane strony i społeczeństwo obywatelskie. Aby zapewnić wdrożenie w całej Unii oraz korzyści skali, należy ustanowić wspólne przepisy regulujące uruchamianie piaskownic regulacyjnych oraz ramy współpracy między odpowiednimi organami uczestniczącymi w nadzorze nad piaskownicami regulacyjnymi. Piaskownice regulacyjne w zakresie sztucznej inteligencji ustanowione na mocy niniejszego rozporządzenia powinny pozostawać bez uszczerbku dla innego prawodawstwa umożliwiającego tworzenie innych piaskownic mających na celu zapewnienie przestrzegania prawodawstwa innego niż niniejsze rozporządzenie. W stosownych przypadkach odpowiednie właściwe organy odpowiedzialne za te inne piaskownice regulacyjne powinny przeanalizować korzyści płynące ze stosowania tych piaskownic również do celów zapewnienia zgodności systemów sztucznej inteligencji z niniejszym rozporządzeniem. Po osiągnięciu porozumienia pomiędzy właściwymi organami krajowymi oraz uczestnikami piaskownicy regulacyjnej w zakresie sztucznej inteligencji w ramach piaskownicy regulacyjnej w zakresie sztucznej inteligencji mogą być również prowadzone i nadzorowane testy w warunkach rzeczywistych.

(-72a) Niniejsze rozporządzenie powinno zapewnić uczestnikom piaskownicy regulacyjnej w zakresie sztucznej inteligencji podstawę prawną do wykorzystywania danych osobowych zebranych w innych celach do opracowywania, w ramach piaskownicy regulacyjnej w zakresie sztucznej inteligencji, określonych systemów sztucznej inteligencji w interesie publicznym zgodnie z art. 6 ust. 4 i art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679 i art. 5 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 rozporządzenia (UE) 2016/679, rozporządzenia (UE) 2018/1725 i 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. Uczestnicy korzystający z piaskownicy regulacyjnej powinni zapewnić odpowiednie zabezpieczenia i współpracować z właściwymi organami, w tym przestrzegać wytycznych tych organów, a także podejmować w dobrej wierze bezzwłoczne działania w celu ograniczenia wszelkiego rodzaju wysokiego ryzyka dla bezpieczeństwa i praw podstawowych, jakie może powstać w trakcie opracowywania produktów oraz prowadzenia eksperymentów w ramach piaskownicy regulacyjnej. Przy podejmowaniu przez właściwe organy decyzji o ewentualnym nałożeniu administracyjnej kary pieniężnej na podstawie art. 83 ust. 2 rozporządzenia 2016/679 oraz art. 57 dyrektywy 2016/680 należy uwzględnić postępowanie uczestników korzystających z piaskownicy regulacyjnej.

(72a) Aby przyspieszyć proces opracowywania i wprowadzania do obrotu systemów sztucznej inteligencji wysokiego ryzyka wymienionych w załączniku III, 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 sztucznej inteligencji. Jednak w takich przypadkach oraz uwzględniając potencjalne konsekwencje takiego testowania dla obywateli, należy zapewnić, by rozporządzenie wprowadzało odpowiednie i wystarczające gwarancje i warunki dla dostawców lub potencjalnych dostawców. Takie gwarancje powinny obejmować między innymi wymóg udzielenia świadomej zgody przez osoby fizyczne, które mają brać udział w testach w warunkach rzeczywistych, z wyjątkiem organów ścigania w przypadkach, gdy konieczność wystąpienia o świadomą zgodę uniemożliwiłaby testowanie systemu sztucznej inteligencji. Zgoda podmiotów testów na udział w takich testach na podstawie niniejszego rozporządzenia ma odrębny charakter i pozostaje bez uszczerbku dla zgody osób, których dane dotyczą, na przetwarzanie ich danych osobowych na podstawie odpowiedniego prawa ochrony danych.

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

(73a) W celu promowania i ochrony innowacji do realizacji celów niniejszego rozporządzenia powinny przyczyniać się platforma „Sztuczna inteligencja na żądanie", wszystkie odpowiednie finansowane przez UE programy i projekty, takie jak program „Cyfrowa Europa", „Horyzont Europa", wdrażane przez Komisję i państwa członkowskie na szczeblu krajowym lub unijnym.

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

(74a) Ponadto, w celu zapewnienia proporcjonalności, z uwagi na bardzo mały rozmiar niektórych operatorów w odniesieniu do kosztów innowacji, należy zwolnić mikroprzedsiębiorstwa z najbardziej kosztownych obowiązków, takich jak ustanowienie systemu zarządzania jakością, co zmniejszyłoby obciążenie administracyjne i koszty ponoszone przez te przedsiębiorstwa bez wpływu na poziom ochrony oraz konieczność zapewnienia zgodności z wymogami dotyczącymi systemów sztucznej inteligencji wysokiego ryzyka.

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

PUBLIC

(76) Aby ułatwić sprawne, skuteczne i zharmonizowane wdrożenie niniejszego rozporządzenia, należy ustanowić Europejską Radę ds. Sztucznej Inteligencji. Rada powinna odzwierciedlać różne interesy ekosystemu sztucznej inteligencji i składać się z przedstawicieli państw członkowskich. Aby zapewnić udział odpowiednich zainteresowanych podmiotów, należy utworzyć stałą podgrupę Rady. Rada powinna odpowiadać za szereg zadań doradczych, w tym wydawanie opinii lub zaleceń oraz udzielanie porad lub udział w tworzeniu wskazówek w dziedzinach związanych z wdrażaniem niniejszego rozporządzenia, także w kwestiach egzekwowania, specyfikacji technicznych lub istniejących norm dotyczących wymogów ustanowionych w niniejszym rozporządzeniu, jak również za udzielanie porad i wsparcia Komisji oraz państwom członkowskim i ich właściwym organom krajowym w konkretnych kwestiach związanych ze sztuczną inteligencją. Aby zapewnić państwom członkowskim pewną elastyczność w wyznaczaniu swoich przedstawicieli do Rady ds. Sztucznej Inteligencji, takimi przedstawicielami mogą być wszelkie osoby należące do podmiotów publicznych, które powinny mieć odpowiednie kompetencje i uprawnienia, aby ułatwiać koordynację na szczeblu krajowym i przyczyniać się do realizacji zadań Rady. Rada 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 działać do celów niniejszego rozporządzenia jako grupa współpracy administracyjnej ds. nadzoru rynku (ADCO) w rozumieniu art. 30 rozporządzenia (UE) 2019/1020. Zgodnie z rolą i zadaniami Komisji określonymi w art. 33 rozporządzenia (UE) 2019/1020 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 może również tworzyć inne stałe lub tymczasowe podgrupy na potrzeby zbadania konkretnych kwestii. Rada powinna również w stosownych przypadkach współpracować z odpowiednimi organami UE, grupami ekspertów i sieciami działającymi w kontekście odpowiedniego prawodawstwa UE, w tym w szczególności z tymi, które działają na podstawie odpowiednich unijnych przepisów dotyczących danych, produktów i usług cyfrowych.

(76a) Komisja powinna aktywnie wspierać państwa członkowskie i podmioty gospodarcze we wdrażaniu i egzekwowaniu niniejszego rozporządzenia. W tym względzie Komisja powinna opracować wytyczne dotyczące konkretnych zagadnień mające na celu ułatwienie stosowania niniejszego rozporządzenia, ze zwróceniem szczególnej uwagi na potrzeby MŚP i przedsiębiorstw typu start-up w sektorach, na które niniejsze rozporządzenie będzie miało najprawdopodobniej największy wpływ. Aby wspierać odpowiednie egzekwowanie przepisów i możliwości państw członkowskich, należy ustanowić unijne jednostki badawcze w zakresie sztucznej inteligencji oraz grupę odpowiednich ekspertów, które to jednostki i grupa powinny być do dyspozycji państw członkowskich.

(77) Państwa członkowskie odgrywają kluczową rolę w stosowaniu i egzekwowaniu niniejszego rozporządzenia. W tym zakresie każde państwo członkowskie powinno wyznaczyć co najmniej jeden właściwy organ krajowy do celów sprawowania nadzoru nad stosowaniem i wdrażaniem niniejszego rozporządzenia. 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.

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

PUBLIC

(79) Aby zapewnić odpowiednie i skuteczne egzekwowanie wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, które należy do unijnego prawodawstwa harmonizacyjnego, system nadzoru rynku i zgodności produktów ustanowiony rozporządzeniem (UE) 2019/1020 powinien mieć zastosowanie w całości. Organy nadzoru rynku wyznaczone zgodnie z niniejszym rozporządzeniem powinny mieć wszystkie uprawnienia w zakresie egzekwowania przepisów wynikające z niniejszego rozporządzenia oraz z rozporządzenia (UE) 2019/1020 i powinny wykonywać swoje uprawnienia i obowiązki w sposób niezależny, bezstronny i wolny od uprzedzeń. Chociaż większość systemów sztucznej inteligencji nie podlega szczególnym wymogom i obowiązkom na podstawie niniejszego rozporządzenia, organy nadzoru rynku mogą przyjmować środki w odniesieniu do wszystkich systemów sztucznej inteligencji, 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.

(79a) Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji, zadań, uprawnień i niezależności odpowiednich krajowych organów lub podmiotów publicznych, które nadzorują stosowanie prawa Unii w zakresie ochrony praw podstawowych, w tym organów ds. równości i organów ochrony danych. W przypadku gdy jest to niezbędne do wykonywania ich mandatu, te krajowe organy lub podmioty publiczne, powinny również mieć dostęp do wszelkiej dokumentacji sporządzonej na podstawie niniejszego rozporządzenia. Należy ustanowić specjalną procedurę w sprawie środków ochronnych w celu zapewnienia odpowiedniego i terminowego egzekwowania przepisów dotyczących systemów sztucznej inteligencji stwarzających zagrożenie dla zdrowia, bezpieczeństwa i praw podstawowych. Procedurę dotyczącą takich systemów sztucznej inteligencji stwarzających ryzyko należy stosować w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka stwarzających ryzyko, zakazanych systemów wprowadzonych do obrotu, oddanych do użytku lub wykorzystywanych z naruszeniem zasad dotyczących zakazanych praktyk ustanowionych w niniejszym rozporządzeniu, oraz systemów sztucznej inteligencji, które zostały udostępnione z naruszeniem ustanowionych w niniejszym rozporządzeniu wymogów przejrzystości i które stwarzają ryzyko.

(80) Przepisy Unii dotyczące usług finansowych obejmują zasady i wymogi dotyczące zarządzania wewnętrznego i zarządzania ryzykiem, które mają zastosowanie do objętych regulacją instytucji finansowych podczas świadczenia tych usług, w tym wówczas, gdy korzystają one z systemów sztucznej inteligencji. Aby zapewnić spójne stosowanie i egzekwowanie obowiązków ustanowionych w niniejszym rozporządzeniu oraz odpowiednich zasad i wymogów ustanowionych w przepisach Unii dotyczących usług finansowych, organy odpowiedzialne za nadzór nad przepisami dotyczącymi usług finansowych i ich egzekwowanie, należy wyznaczyć jako właściwe organy do celów nadzoru nad wdrażaniem niniejszego rozporządzenia, w tym do celów działań związanych z nadzorem rynku, w odniesieniu do systemów sztucznej inteligencji dostarczanych lub wykorzystywanych przez objęte regulacją i nadzorem instytucje finansowe, 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 sprawie nadzoru rynku w celu egzekwowania wymogów i obowiązków wynikających z niniejszego rozporządzenia, w tym uprawnienia do prowadzenia działań ex post w zakresie nadzoru rynku, które można w stosownych przypadkach włączyć do ich istniejących mechanizmów i procedur nadzorczych na podstawie odpowiednich unijnych przepisów dotyczących usług finansowych. Należy przewidzieć, by w przypadku gdy będą występowały w charakterze organów nadzoru rynku na podstawie niniejszego rozporządzenia, krajowe organy odpowiedzialne za nadzór instytucji kredytowych uregulowanych na podstawie dyrektywy 2013/36/UE, które uczestniczą w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem Rady nr 1024/2013, powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zidentyfikowane w trakcie prowadzonych przez nie działań z zakresu nadzoru rynku, które potencjalnie mogą mieć znaczenie dla Europejskiego Banku Centralnego z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego. Aby dodatkowo zwiększyć spójność między niniejszym rozporządzeniem a przepisami mającymi zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE[27], niektóre obowiązki proceduralne dostawców związane z zarządzaniem ryzykiem, monitorowaniem po wprowadzeniu do obrotu oraz dokumentowaniem należy również włączyć do istniejących obowiązków i procedur przewidzianych w dyrektywie 2013/36/UE. Aby uniknąć nakładania się przepisów, należy również przewidzieć ograniczone odstępstwa dotyczące systemu zarządzania jakością dostawców oraz obowiązku monitorowania nałożonego na użytkowników systemów sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim mają one zastosowanie do instytucji kredytowych objętych regulacją na mocy dyrektywy 2013/36/UE. Ten sam system powinien mieć zastosowanie do zakładów ubezpieczeń i zakładów reasekuracji oraz ubezpieczeniowych spółek holdingowych na podstawie dyrektywy 2009/138/UE (Wypłacalność II) oraz pośredników ubezpieczeniowych na mocy dyrektywy (UE) 2016/97, a także do innych rodzajów instytucji finansowych objętych wymogami dotyczącymi ich systemu zarządzania

[27] 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).

wewnętrznego, uzgodnień lub procedur ustanowionych zgodnie z odpowiednimi unijnymi przepisami dotyczącymi usług finansowych, w celu zapewnienia spójności i równego traktowania w sektorze finansowym.

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

(82) Istotne jest, aby systemy sztucznej inteligencji związane z produktami, które nie są systemami wysokiego ryzyka w rozumieniu niniejszego rozporządzenia, a zatem nie muszą spełniać ustanowionych w nim wymogów, były mimo to bezpieczne w chwili wprowadzenia ich do obrotu lub oddawania ich do użytku. Aby przyczynić się do osiągnięcia tego celu, dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady[28] miałaby zastosowanie jako „bezpiecznik”.

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

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

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

(85) Aby zapewnić możliwość dostosowania w razie potrzeby ram regulacyjnych, należy powierzyć Komisji uprawnienia do przyjmowania aktów na podstawie art. 290 TFUE w celu zmiany unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II, systemów sztucznej inteligencji wysokiego ryzyka wymienionych w załączniku III, przepisów dotyczących dokumentacji technicznej wymienionych w załączniku IV, treści deklaracji zgodności UE zawartej w załączniku V, przepisów dotyczących procedur oceny zgodności zawartych w załącznikach VI i VII oraz przepisów określających systemy sztucznej inteligencji wysokiego ryzyka, do których powinna mieć zastosowanie procedura oceny zgodności oparta na ocenie systemu zarządzania jakością oraz ocenie dokumentacji technicznej. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[29]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych. Takie konsultacje i wsparcie doradcze powinny być prowadzone także w ramach działań Rady ds. Sztucznej Inteligencji i jej podgrup.

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

PUBLIC

(86) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[30]. Szczególnie ważne jest, aby – zgodnie z zasadami ustanowionymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa – gdy tylko na wczesnym etapie przygotowywania projektów aktów wykonawczych potrzebna będzie szersza wiedza fachowa, Komisja, w stosownych przypadkach, korzystała z pomocy grup ekspertów, konsultowała się z określonymi zainteresowanymi stronami lub prowadziła konsultacje publiczne. Takie konsultacje i wsparcie doradcze powinny być również prowadzone w kontekście działań Rady ds. Sztucznej Inteligencji i jej podgrup, w tym przygotowywania aktów wykonawczych dotyczących art. 4, 4b i 6.

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

(87a) Aby zapewnić pewność prawa, zapewnić operatorom odpowiedni okres na dostosowanie się i uniknąć zakłóceń na rynku, w tym poprzez zapewnienie ciągłości korzystania z systemów sztucznej inteligencji, niniejsze rozporządzenie powinno mieć zastosowanie do systemów sztucznej inteligencji 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 zostaną wprowadzone istotne zmiany w ich projekcie lub przeznaczeniu. Należy wyjaśnić, że w tym względzie pojęcie istotnej zmiany należy rozumieć jako równoważne znaczeniowo z pojęciem istotnej zmiany, które stosuje się wyłącznie w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka zdefiniowanych w niniejszym rozporządzeniu.

[30] 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).

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

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

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

TYTUŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się:

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

a) zakazy dotyczące określonych praktyk w zakresie sztucznej inteligencji;

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

c) zharmonizowane przepisy dotyczące przejrzystości w przypadku niektórych systemów sztucznej inteligencji;

d) przepisy dotyczące monitorowania po wprowadzeniu do obrotu, nadzoru rynku i zarządzania;

e) środki wspierające innowacyjność.

Artykuł 2
Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do:

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

b) użytkowników systemów sztucznej inteligencji, którzy przebywają fizycznie lub mają siedzibę w Unii;

c) dostawców i użytkowników systemów sztucznej inteligencji, którzy przebywają fizycznie lub mają siedzibę w państwie trzecim, jeżeli wyniki działania systemu są wykorzystywane w Unii;

d) importerów i dystrybutorów systemów sztucznej inteligencji;

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

f) mających siedzibę w Unii upoważnionych przedstawicieli dostawców.

2. W przypadku systemów sztucznej inteligencji zaklasyfikowanych jako systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 ust. 1 i 2 dotyczącymi produktów objętych unijnym prawodawstwem harmonizacyjnym wymienionym w sekcji B załącznika II, zastosowanie ma wyłącznie art.84 niniejszego rozporządzenia. Art. 53 stosuje się wyłącznie w zakresie, w jakim wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka określone w niniejszym rozporządzeniu zostały włączone do tego unijnego prawodawstwa harmonizacyjnego.

PUBLIC

3. Niniejsze rozporządzenie nie ma zastosowania do systemów sztucznej inteligencji, jeśli i w stopniu jakim wprowadzono je do obrotu, oddano do użytku lub korzysta się z nich z modyfikacjami lub bez zmian – do celów działań, które nie wchodzą w zakres prawa Unii, a w każdym razie do działań powiązanych z wojskiem, obroną lub bezpieczeństwem narodowym, niezależnie od rodzaju podmiotu prowadzącego te działania.

   Ponadto niniejsze rozporządzenie nie ma zastosowania do systemów sztucznej inteligencji, które nie są wprowadzone do obrotu ani oddane do użytku w Unii, a których wyniki są wykorzystywane w Unii do celów działań, które nie wchodzą w zakres prawa Unii, a w każdym razie do działań powiązanych z wojskiem, obroną lub bezpieczeństwem narodowym, niezależnie od rodzaju podmiotu prowadzącego te działania.

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

5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania przepisów dotyczących odpowiedzialności usługodawców będących pośrednikami ustanowionych w rozdziale II sekcja 4 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady[31] [*które zostaną zastąpione odpowiednimi przepisami aktu o usługach cyfrowych*].

6. Niniejsze rozporządzenie nie ma zastosowania do systemów sztucznej inteligencji, w tym ich wyników, specjalnie opracowanych i oddanych do użytku wyłącznie do celów badań naukowych i rozwojowych.

7. Niniejsze rozporządzenie nie ma zastosowania do żadnych działań badawczo-rozwojowych dotyczących systemów sztucznej inteligencji.

8. Niniejsze rozporządzenie nie ma zastosowania do obowiązków użytkowników będących osobami fizycznymi korzystającymi z systemów sztucznej inteligencji w ramach czysto osobistej działalności pozazawodowej, z wyjątkiem art. 52.

---

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

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „system sztucznej inteligencji” oznacza system, który zaprojektowano do działania w sposób częściowo autonomiczny i który, w oparciu o dane i informacje dostarczone maszynowo lub przez człowieka, wnioskuje w jaki sposób osiągnąć zadany zestaw celów – z wykorzystaniem technologii uczenia się maszyn lub metod opartych na logice i wiedzy, i który generuje wyniki, takie jak treści (generatywne systemy sztucznej inteligencji), przewidywania, zalecenia lub decyzje, wpływające na środowiska, z którymi system ten wchodzi w interakcję;

1a) „cykl życia systemu sztucznej inteligencji” oznacza czas istnienia systemu sztucznej inteligencji, od etapu projektowania do wycofania z eksploatacji. Bez uszczerbku dla uprawnień organów nadzoru rynku, takie wycofanie z eksploatacji może nastąpić w dowolnym momencie podczas monitorowania po wprowadzeniu do obrotu w wyniku decyzji dostawcy i oznacza, że system nie może być dalej wykorzystywany. Cykl życia systemu sztucznej inteligencji kończy się również w wyniku istotnej modyfikacji tego systemu przez dostawcę lub inną osobę fizyczną lub prawną, w którym to przypadku taki istotnie zmodyfikowany system sztucznej inteligencji uznaje się za nowy system sztucznej inteligencji.

1b) „system sztucznej inteligencji ogólnego przeznaczenia” oznacza system sztucznej inteligencji, który – niezależnie od sposobu, w jaki jest wprowadzany do obrotu lub oddawany do użytku, w tym jako otwarte oprogramowanie – zgodnie z przeznaczeniem przewidzianym przez dostawcę ma wykonywać funkcje ogólnego zastosowania, takie jak rozpoznawanie obrazów i mowy, wytwarzanie dźwięku lub treści wideo, wykrywanie wzorców, udzielanie odpowiedzi na pytania, tłumaczenie lub inne; system sztucznej inteligencji ogólnego przeznaczenia może być wykorzystywany w wielu kontekstach i być zintegrowany z wieloma innymi systemami sztucznej inteligencji;

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

3) [skreśla się]

3a) „małe i średnie przedsiębiorstwo” (MŚP) oznacza przedsiębiorstwo zdefiniowane w załączniku do zalecenia Komisji 2003/361/WE dotyczącego definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw;

4) „użytkownik” oznacza osobą fizyczną lub prawną, w tym organ publiczny, agencję lub inny podmiot, która odpowiada za wykorzystywanie systemu sztucznej inteligencji;

5) „upoważniony przedstawiciel” oznacza dowolną osobę fizyczną lub prawną przebywającą fizycznie lub mającą siedzibę w Unii, która otrzymała i zaakceptowała pisemne pełnomocnictwo od dostawcy systemu sztucznej inteligencji do realizacji w jego imieniu obowiązków i procedur ustanowionych w niniejszym rozporządzeniu;

5a) „producent produktu” oznacza producenta w rozumieniu unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II;

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

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

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

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

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

11) „oddanie do użytku” oznacza dostarczenie systemu sztucznej inteligencji do pierwszego użycia bezpośrednio użytkownikowi lub do użytku własnego – na terytorium Unii, zgodnie z przeznaczeniem systemu;

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

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

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

15) „instrukcja obsługi” oznacza informacje podane przez dostawcę w celu poinformowania użytkownika w szczególności o przeznaczeniu i właściwym użytkowaniu systemu sztucznej inteligencji;

16) „wycofanie systemu sztucznej inteligencji od użytkowników” oznacza dowolny środek mający na celu doprowadzenie do zwrotu dostawcy systemu sztucznej inteligencji udostępnionego użytkownikom, wyłączenia takiego systemu z eksploatacji lub uniemożliwienia korzystania z niego;

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

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

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

20) „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;

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

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

23) „istotna zmiana” oznacza zmianę w systemie sztucznej inteligencji po jego wprowadzeniu do obrotu lub oddaniu do użytku, która wpływa na zgodność systemu sztucznej inteligencji z wymogami określonymi w tytule III rozdział 2 niniejszego rozporządzenia lub zmianę przeznaczenia, pod kątem którego oceniono system sztucznej inteligencji. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, które nadal uczą się po wprowadzeniu ich do obrotu lub po oddaniu ich do użytku, istotnej zmiany nie stanowią zmiany w systemie sztucznej inteligencji wysokiego ryzyka i jego skuteczności działania, które dostawca z góry zaplanował w chwili przeprowadzania pierwotnej oceny zgodności i które są częścią informacji zawartych w dokumentacji technicznej, o której mowa w pkt 2 lit. f) załącznika IV;

24) „oznakowanie zgodności CE” (oznakowanie CE) oznacza oznakowanie, za pomocą którego dostawca wskazuje, że system sztucznej inteligencji spełnia wymogi określone w tytule III rozdział 2 lub w art. 4b niniejszego rozporządzenia i innego mającego zastosowanie aktu prawnego Unii harmonizującego warunki wprowadzania produktów do obrotu („unijne prawodawstwo harmonizacyjne”), przewidującego umieszczanie takiego oznakowania;

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

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

PUBLIC

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

28) „wspólne specyfikacje” oznaczają specyfikacje techniczne zdefiniowane w art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012 zapewniające środki umożliwiające spełnienie niektórych wymogów określonych na podstawie niniejszego rozporządzenia;

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

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

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

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

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

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

35) „system kategoryzacji biometrycznej” oznacza system sztucznej inteligencji służący do przypisywania osób fizycznych do określonych kategorii na podstawie danych biometrycznych tych osób;

36) „system zdalnej identyfikacji biometrycznej” oznacza system sztucznej inteligencji służący do identyfikacji osób fizycznych co do zasady na odległość, bez aktywnego udziału tych osób, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych;

37) „system zdalnej identyfikacji biometrycznej »w czasie rzeczywistym«” oznacza system zdalnej identyfikacji biometrycznej, w którym zbieranie danych biometrycznych, ich porównywanie i identyfikacja odbywają się natychmiastowo lub niemal natychmiastowo;

38) [skreśla się]

39) „przestrzeń publiczna” oznacza każde miejsce fizyczne, będące własnością prywatną czy publiczną, dostępne dla nieokreślonej liczby osób fizycznych niezależnie od tego, czy określone warunki lub okoliczności dostępu zostały z góry sprecyzowane, oraz niezależnie od potencjalnych ograniczeń pojemności;

40) „organ ścigania” oznacza:

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

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

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

42) [skreśla się]

PUBLIC

43) „właściwy organ krajowy” oznacza którykolwiek z następujących organów: organ notyfikujący i organ nadzoru rynku; W odniesieniu do systemów sztucznej inteligencji oddanych do użytku lub wykorzystywanych przez instytucje, organy, urzędy i agencje UE, Europejski Inspektor Ochrony Danych wypełnia obowiązki, które w państwach członkowskich powierzone są właściwym organom krajowym, a zatem wszelkie odniesienia do właściwych organów krajowych lub organów nadzoru rynku umieszczone w niniejszym rozporządzeniu należy w stosownych przypadkach rozumieć jako odniesienia do Europejskiego Inspektor Ochrony Danych;

44) „poważny incydent” oznacza każdy incydent lub nieprawidłowe działanie systemu sztucznej inteligencji, 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 i jej funkcjonowaniu;

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

d) poważnego uszkodzenia mienia lub szkody dla środowiska.

45) „infrastruktura krytyczna” oznacza składnik infrastruktury, system lub jego część niezbędne do świadczenia usługi kluczowej dla utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej w rozumieniu art. 2 ust. 4 i 5 dyrektywy .../... w sprawie odporności podmiotów krytycznych;

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

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

48) „testy w warunkach rzeczywistych” oznaczają tymczasowe testowanie systemu sztucznej inteligencji zgodnie z jego przeznaczeniem w warunkach rzeczywistych – poza środowiskiem laboratoryjnym lub środowiskiem symulowanym innego typu – w celu zgromadzenia wiarygodnych i solidnych danych oraz w celu oceny i weryfikacji zgodności systemu sztucznej inteligencji z wymogami niniejszego rozporządzenia; testów w warunkach rzeczywistych nie uznaje się za wprowadzenie systemu sztucznej inteligencji do obrotu ani oddanie go do użytku w rozumieniu niniejszego rozporządzenia, pod warunkiem spełnienia wszystkich warunków określonych w art. 53 lub 54a;

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

50) „podmiot testów” do celów testów w warunkach rzeczywistych oznacza osobę fizyczną, która uczestniczy w testach tego typu;

51) „świadoma zgoda” oznacza swobodne i dobrowolne wyrażenie przez podmiot testów 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 podmiot testów; w przypadku małoletnich i niezdolnych do wyrażenia zgody podmiotów testów świadomej zgody udziela ich wyznaczony zgodnie z prawem przedstawiciel;

52) „piaskownica regulacyjna w zakresie sztucznej inteligencji” oznacza konkretne ramy ustanowione przez właściwy organ krajowy, umożliwiające dostawcom lub potencjalnym dostawcom systemów sztucznej inteligencji możliwość opracowywania, trenowania, walidowania i testowania – w stosownych przypadkach w warunkach rzeczywistych – innowacyjnych systemów sztucznej inteligencji, w oparciu o szczegółowy plan, w ograniczonym czasie i pod nadzorem regulacyjnym.

PUBLIC

Artykuł 4

Akty wykonawcze

W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia w odniesieniu do mechanizmów uczenia się maszyn i metod opartych na logice i wiedzy, o których mowa w art. 3 pkt 1, Komisja może przyjmować akty wykonawcze w celu określenia technicznych elementów tych mechanizmów i metod, z uwzględnieniem rozwoju rynku i rozwoju technologicznego. Wspomniane akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

TYTUŁ IA

SYSTEM SZTUCZNEJ INTELIGENCJI OGÓLNEGO PRZEZNACZENIA

Artykuł 4a

Zgodność systemów sztucznej inteligencji ogólnego przeznaczenia z niniejszym rozporządzeniem

1. Bez uszczerbku dla art. 5, 52, 53 i 69 niniejszego rozporządzenia systemy sztucznej inteligencji ogólnego przeznaczenia spełniają jedynie wymogi i obowiązki określone w art. 4b.

2. Te wymogi i obowiązki mają zastosowanie niezależnie od tego, czy system sztucznej inteligencji ogólnego przeznaczenia jest wprowadzany do obrotu czy oddawany do użytku jako wstępnie wytrenowany model i czy użytkownik systemu sztucznej inteligencji ogólnego przeznaczenia ma przeprowadzić dalsze dostosowywanie tego modelu.

Artykuł 4b

Wymogi dotyczące systemów sztucznej inteligencji ogólnego przeznaczenia oraz obowiązki spoczywające na dostawcach takich systemów

1. Systemy sztucznej inteligencji ogólnego przeznaczenia, które mogą być wykorzystywane jako systemy sztucznej inteligencji wysokiego ryzyka lub jako komponenty systemów sztucznej inteligencji wysokiego ryzyka w rozumieniu art. 6, muszą spełniać wymogi ustanowione w tytule III rozdział 2 niniejszego rozporządzenia, począwszy od daty rozpoczęcia stosowania aktów wykonawczych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2, nie później niż 18 miesięcy po wejściu w życie niniejszego rozporządzenia. W tych aktach wykonawczych określa się i dostosowuje się spełnianie wymogów ustanowionych w tytule III rozdział 2 w odniesieniu do systemów sztucznej inteligencji ogólnego przeznaczenia w świetle ich cech, wykonalności technicznej, specyfiki łańcucha wartości sztucznej inteligencji i w świetle rozwoju rynku i rozwoju technologicznego. Przy spełnianiu tych wymogów uwzględnia się powszechnie uznany stan wiedzy technicznej.

2. Dostawcy systemów sztucznej inteligencji ogólnego przeznaczenia, o których mowa w ust. 1, wypełniają – od daty rozpoczęcia stosowania aktów wykonawczych, o których mowa w ust. 1 – obowiązki określone w art. 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 i 61.

3. W celu wypełniania obowiązków określonych w art. 16e dostawcy stosują procedurę oceny zgodności opierającą się na kontroli wewnętrznej, określoną w załączniku VI pkt 3 i 4.

4. Dostawcy takich systemów przechowują również dokumentację techniczną, o której mowa w art. 11, do dyspozycji właściwych organów krajowych – przez okres, który upływa dziesięć lat po wprowadzeniu systemu sztucznej inteligencji ogólnego przeznaczenia do obrotu w Unii lub oddaniu go do użytku w Unii.

PUBLIC

5. Dostawcy systemów sztucznej inteligencji ogólnego przeznaczenia współpracują z innymi dostawcami zamierzającymi oddać do użytku lub wprowadzić do obrotu w Unii takie systemy jako systemy sztucznej inteligencji wysokiego ryzyka lub jako komponenty tego rodzaju systemów oraz przekazują im niezbędne informacje, aby umożliwić takim innym dostawcom wypełnianie obowiązków wynikających z niniejszego rozporządzenia. Taka współpraca między dostawcami odbywa się z poszanowaniem, w stosownych przypadkach, praw własności intelektualnej oraz poufnych informacji handlowych lub tajemnic przedsiębiorstwa zgodnie z art. 70. W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia w odniesieniu do informacji, którymi mają dzielić się dostawcy systemów sztucznej inteligencji ogólnego przeznaczenia, Komisja może przyjmować akty wykonawcze zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

6. W ramach wypełniania wymogów i obowiązków, o których mowa w ust. 1, 2 i 3:

– wszelkie odniesienia do przeznaczenia należy rozumieć jako odniesienia do możliwego wykorzystania systemów sztucznej inteligencji ogólnego przeznaczenia jako systemów sztucznej inteligencji wysokiego ryzyka lub jako komponentów tego rodzaju systemów w rozumieniu art. 6;

– wszelkie odniesienia do wymogów dotyczących systemów sztucznej inteligencji wysokiego ryzyka w tytule III rozdział 2 należy rozumieć jako odniesienia wyłącznie do wymogów określonych w niniejszym artykule.

Artykuł 4c
Wyjątki od artykułu 4b

1. Artykuł 4b nie ma zastosowania, jeżeli dostawca wyraźnie wykluczył – w instrukcji obsługi lub w informacjach dołączonych do systemu sztucznej inteligencji ogólnego przeznaczenia – wszelkie zastosowania wysokiego ryzyka.

2. Dostawca dokonuje takiego wykluczenia w dobrej wierze, jednak nie można uznać go za uzasadnione, jeżeli dostawca ma wystarczające powody, by sądzić, że przedmiotowy system może być niewłaściwie wykorzystywany.

3. Jeżeli dostawca wykryje niewłaściwe wykorzystywanie na rynku lub zostanie o nim poinformowany, podejmuje wszelkie niezbędne i proporcjonalne środki w celu zapobieżenia takiemu dalszemu niewłaściwemu wykorzystywaniu, w szczególności biorąc pod uwagę skalę niewłaściwego wykorzystania i wagę związanego z nim ryzyka.

TYTUŁ II

ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

PUBLIC

Artykuł 5

1. Zakazuje się następujących praktyk w zakresie sztucznej inteligencji:

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

   b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który wykorzystuje dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną, w celu lub ze skutkiem istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, który powoduje lub istnieje uzasadnione prawdopodobieństwo, że spowoduje u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;

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

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

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

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

(i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw;

(ii) zapobiegania konkretnemu i poważnemu zagrożeniu infrastruktury krytycznej, zagrożeniu życia, zdrowia lub bezpieczeństwa fizycznego osób fizycznych lub zapobiegania atakom terrorystycznym;

(iii) lokalizacji lub identyfikacji osoby fizycznej do celów przeprowadzenia postępowania przygotowawczego, ścigania lub wykonywania kar w odniesieniu do przestępstw, o których mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW[32], podlegających w danym państwie członkowskim karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, lub w odniesieniu do innych określonych przestępstw podlegających w danym państwie członkowskim karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej pięć lat, zgodnie z prawem danego państwa członkowskiego.

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

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

[32] 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).

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

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

3. Jeżeli chodzi o ust. 1 lit. d) i ust. 2, każde wykorzystanie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa wymaga uzyskania uprzedniego zezwolenia udzielonego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego, w którym ma nastąpić wykorzystanie, wydanego na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego, o których mowa w ust. 4. W należycie uzasadnionych nagłych przypadkach można jednak rozpocząć wykorzystywanie systemu bez zezwolenia, pod warunkiem że o takie zezwolenie występuje się bez zbędnej zwłoki w trakcie wykorzystywania systemu sztucznej inteligencji, a w przypadku odmowy udzielenia takiego zezwolenia jego wykorzystywanie zostaje wstrzymane ze skutkiem natychmiastowym.

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

PUBLIC

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

TYTUŁ III

SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

ROZDZIAŁ 1

KLASYFIKACJA SYSTEMÓW SZTUCZNEJ INTELIGENCJI JAKO SYSTEMÓW WYSOKIEGO RYZYKA

Artykuł 6

Zasady klasyfikacji systemów sztucznej inteligencji wysokiego ryzyka

1. System sztucznej inteligencji, który sam w sobie stanowi produkt objęty unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II, uznawany jest za system wysokiego ryzyka, jeżeli musi zostać poddany ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia go do obrotu lub oddania go do użytku zgodnie ze wspomnianym prawodawstwem.

2. System sztucznej inteligencji przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego prawodawstwem, o którym mowa w ust. 1, uznawany jest za system wysokiego ryzyka, jeżeli musi zostać poddany ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia go do obrotu lub oddania go do użytku zgodnie z wyżej wymienionymi przepisami. Przepis ten ma zastosowanie bez względu na to, czy ten system sztucznej inteligencji wprowadza się do obrotu lub oddaje się go do użytku niezależnie od produktu.

3. Systemy sztucznej inteligencji, o których mowa w załączniku III, uznaje się za systemy sztucznej inteligencji wysokiego ryzyka, chyba że wynik działania systemu jest wyłącznie pomocniczy w odniesieniu do odpowiedniego działania lub decyzji, które należy podjąć, i w związku z tym system ten prawdopodobnie nie spowoduje istotnych zagrożeń dla zdrowia, bezpieczeństwa lub praw podstawowych.

W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia Komisja, nie później niż rok po jego wejściu w życie, przyjmuje akty wykonawcze określające okoliczności, w których wynik działania systemów sztucznej inteligencji wymienionych w załączniku III, byłby wyłącznie pomocniczy w odniesieniu do odpowiedniego działania lub decyzji, które należy podjąć. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 7

Zmiany w załączniku III

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

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

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

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

a) przeznaczenie systemu sztucznej inteligencji;

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

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

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

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

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

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

PUBLIC

h) zakres, w jakim obowiązujące przepisy Unii przewidują:

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

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

i) skalę i prawdopodobieństwo korzyści z wykorzystywania systemu sztucznej inteligencji płynących dla osób fizycznych, grup lub dla ogółu społeczeństwa.

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

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

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

ROZDZIAŁ 2

WYMOGI DOTYCZĄCE SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

Artykuł 8

Zgodność z wymogami

1. Systemy sztucznej inteligencji wysokiego ryzyka muszą spełniać wymogi ustanowione w niniejszym rozdziale, przy uwzględnieniu powszechnie uznanego stanu wiedzy technicznej.

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

Artykuł 9

System zarządzania ryzykiem

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

2. System zarządzania ryzykiem należy rozumieć jako ciągły, iteracyjny proces planowany i realizowany przez cały cykl życia systemu sztucznej inteligencji wysokiego ryzyka, wymagający regularnej, systematycznej aktualizacji. Obejmuje on następujące etapy:

   a) identyfikację i analizę znanych i dających się przewidzieć zagrożeń dla zdrowia, bezpieczeństwa i praw podstawowych, o najwyższym prawdopodobieństwie wystąpienia w świetle przeznaczenia systemu sztucznej inteligencji wysokiego ryzyka;

   b) [skreśla się]

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

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

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

PUBLIC

3. W ramach środków zarządzania ryzykiem, o których mowa w ust. 2 lit. d), należycie uwzględnia się skutki i możliwe interakcje wynikające z łącznego stosowania wymogów określonych w niniejszym rozdziale 2, z myślą o skuteczniejszym minimalizowaniu ryzyka przy jednoczesnym osiągnięciu odpowiedniej równowagi we wdrażaniu środków służących spełnieniu przedmiotowych wymogów.

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

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

   a) eliminację lub ograniczenie ryzyka, zidentyfikowanego i ocenionego zgodnie z ust. 2, w możliwie największym stopniu poprzez odpowiedni projekt systemu sztucznej inteligencji wysokiego ryzyka i proces jego opracowywania;

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

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

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

5. Systemy sztucznej inteligencji wysokiego ryzyka poddaje się testom w celu zapewnienia działania tych systemów zgodnie z ich przeznaczeniem oraz zapewnienia zgodności tych systemów z wymogami określonymi w niniejszym rozdziale.

6. Procedury testowe mogą obejmować testy w warunkach rzeczywistych zgodnie z art. 54a.

PUBLIC

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

8. W ramach systemu zarządzania ryzykiem opisanego w ust. 1–7 szczególną uwagę zwraca się na to, czy istnieje prawdopodobieństwo, że dostęp do systemu sztucznej inteligencji wysokiego ryzyka uzyskają osoby poniżej 18. roku życia lub że będzie on miał na nie wpływ.

9. W odniesieniu do dostawców systemów sztucznej inteligencji wysokiego ryzyka, którzy podlegają wymogom dotyczącym wewnętrznych procesów zarządzania ryzykiem na podstawie odpowiednich unijnych przepisów sektorowych, aspekty opisane w ust. 1–8 mogą być częścią procedur zarządzania ryzykiem ustanowionych zgodnie z tym prawem.

Artykuł 10

Dane i zarządzanie danymi

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

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

   a) odpowiednich decyzji projektowych;

   b) procesów gromadzenia danych;

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

PUBLIC

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

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

f) badania pod kątem ewentualnej tendencyjności, która może mieć wpływ na zdrowie i bezpieczeństwo osób fizycznych lub prowadzić do dyskryminacji zakazanej przez prawo Unii;

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

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

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

5. W zakresie, w jakim jest to ściśle niezbędne do celów zapewnienia monitorowania, wykrywania i korygowania tendencyjności systemów sztucznej inteligencji wysokiego ryzyka, dostawcy takich systemów mogą przetwarzać szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia (UE) 2016/679, art. 10 dyrektywy (UE) 2016/680 i art. 10 ust. 1 rozporządzenia (UE) 2018/1725, pod warunkiem stosowania odpowiednich zabezpieczeń gwarantujących ochronę podstawowych praw i wolności osób fizycznych, w tym środków technicznych ograniczających ponowne wykorzystanie tych danych i najnowocześniejszych środków służących zapewnieniu bezpieczeństwa i ochrony prywatności, takich jak pseudonimizacja lub – w przypadku gdy anonimizacja może znacząco wpłynąć na możliwość realizacji zakładanego celu – szyfrowanie.

PUBLIC

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

Artykuł 11

Dokumentacja techniczna

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

   Dokumentację techniczną sporządza się w taki sposób, aby wykazać, że system sztucznej inteligencji wysokiego ryzyka spełnia wymogi określone w niniejszym rozdziale, oraz aby dostarczyć właściwym organom krajowym i jednostkom notyfikowanym wszystkich informacji – w jasnej i kompleksowej formie – niezbędnych do oceny zgodności systemu sztucznej inteligencji z tymi wymogami. Zawiera ona co najmniej elementy określone w załączniku IV lub, w przypadku MŚP, w tym przedsiębiorstw typu start-up, wszelką równoważną dokumentację służącą tym samym celom, chyba że właściwy organ uzna ją za nieodpowiednią.

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

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

PUBLIC

Artykuł 12

Rejestrowanie zdarzeń

1. Systemy sztucznej inteligencji wysokiego ryzyka mają techniczne możliwości automatycznego rejestrowania zdarzeń („logi”) w trakcie cyklu życia systemu.

2. W celu zapewnienia, iż poziom identyfikowalności funkcjonowania systemu sztucznej inteligencji jest odpowiedni do przeznaczenia tego systemu, funkcja rejestracji zdarzeń zapewnia rejestrowanie zdarzeń istotnych dla:

   (i) identyfikacji sytuacji, które mogą skutkować tym, że system sztucznej inteligencji będzie stwarzał ryzyko w rozumieniu art. 65 ust. 1, lub które mogą prowadzić do wystąpienia istotnej zmiany;

   (ii) ułatwiania monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 61; oraz

   (iii) monitorowania działania systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w art. 29 ust. 4.

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

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

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

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

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

PUBLIC

Artykuł 13

Przejrzystość i udostępnianie informacji użytkownikom

1. Systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w sposób zapewniający wystarczającą przejrzystość ich działania, w celu osiągnięcia zgodności z odpowiednimi obowiązkami użytkownika i dostawcy, określonymi w rozdziale 3 niniejszego tytułu oraz umożliwienia użytkownikom właściwego zrozumienia i użytkowania systemu.

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

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

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

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

      (i) przeznaczenie systemu, łącznie z informacjami o szczególnym kontekście geograficznym, behawioralnym lub funkcjonalnym, w którym ma być wykorzystywany system sztucznej inteligencji wysokiego ryzyka;

      (ii) poziom dokładności, wraz z odnośnymi wskaźnikami, poziom solidności i cyberbezpieczeństwa, o których mowa w art. 15, względem których przetestowano system sztucznej inteligencji 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 sztucznej inteligencji wysokiego ryzyka zgodnie z jego przeznaczeniem, mogące powodować zagrożenia dla zdrowia i bezpieczeństwa lub praw podstawowych, o których mowa w art. 9 ust. 2;

(iv) w stosownych przypadkach, zachowania systemu w odniesieniu do osób lub grup osób, względem których ma on być wykorzystywany;

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

(vi) w stosownych przypadkach, opis oczekiwanego wyniku działania systemu.

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

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

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

f) opis mechanizmu zawartego w systemie sztucznej inteligencji, który umożliwia użytkownikom prawidłowe gromadzenie, przechowywanie i interpretowanie logów, tam gdzie ma to zastosowanie.

Artykuł 14

Nadzór ze strony człowieka

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

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

3. Nadzór ze strony człowieka zapewnia się za pośrednictwem jednego lub wszystkich z następujących rodzajów środków:

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

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

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

a) zrozumienie możliwości i ograniczeń systemu sztucznej inteligencji wysokiego ryzyka oraz należyte monitorowanie jego działania;

b) bycie stale świadomym potencjalnej tendencji do automatycznego polegania lub nadmiernego polegania na wyniku działania systemu sztucznej inteligencji wysokiego ryzyka (tzw. „automation bias”);

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

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

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

5. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1 lit. a), środki, o których mowa w ust. 3, muszą ponadto zapewniać, aby użytkownik nie podejmował żadnego działania ani decyzji na podstawie identyfikacji będącej wynikiem działania systemu, jeżeli nie zweryfikowały jej ani nie potwierdziły jej odrębnie co najmniej dwie osoby fizyczne. Wymóg odrębnej weryfikacji przez co najmniej dwie osoby fizyczne nie ma zastosowania do systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych do celów egzekwowania prawa, 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 sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w taki sposób, aby osiągały, z uwagi na ich przeznaczenie, odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz działały konsekwentnie pod tymi względami w całym cyklu życia.

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

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

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

   Systemy sztucznej inteligencji wysokiego ryzyka, które po wprowadzeniu na rynek lub oddaniu do użytku nadal się uczą, opracowuje się w taki sposób, aby w możliwie największym stopniu wyeliminować lub ograniczyć ryzyko potencjalnie tendencyjnych wyników działania wpływających na dane wejściowe w przyszłych operacjach („sprzężenie zwrotne").

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

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

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

ROZDZIAŁ 3

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

Artykuł 16

Obowiązki dostawców systemów sztucznej inteligencji wysokiego ryzyka

Dostawcy systemów sztucznej inteligencji wysokiego ryzyka:

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

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

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

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

d) w czasie, kiedy znajdują się one pod ich kontrolą, przechowują rejestry zdarzeń generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka, jak określono zgodnie z art. 20;

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

f) wypełniają obowiązki rejestracyjne, o których mowa w art. 51 ust. 1;

g) podejmują niezbędne działania naprawcze, o których mowa w art. 21, jeżeli system sztucznej inteligencji wysokiego ryzyka nie spełnia wymogów określonych w rozdziale 2 niniejszego tytułu;

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

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

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

Artykuł 17

Systemy zarządzania jakością

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2a. W odniesieniu do dostawców systemów sztucznej inteligencji wysokiego ryzyka, którzy podlegają obowiązkom dotyczącym systemów zarządzania jakością na podstawie odpowiednich unijnych przepisów sektorowych, aspekty opisane w ust. 1 mogą być częścią systemów zarządzania jakością zgodnie z tym prawem.

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

Artykuł 18

Prowadzenie dokumentacji

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

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

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

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

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

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

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

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

Artykuł 19

Ocena zgodności

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

2. [skreśla się]

PUBLIC

Artykuł 20

Automatycznie generowane rejestry zdarzeń

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka przechowują generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka rejestry zdarzeń, o których mowa w art. 12 ust. 1, o ile tego rodzaju rejestry znajdują się pod ich kontrolą na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa. Przechowują je przez okres co najmniej sześciu miesięcy, chyba że mające zastosowanie prawo unijne lub krajowe stanowi inaczej, w szczególności unijne prawo ochrony danych osobowych.

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

Artykuł 21

Działania naprawcze

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

Artykuł 22

Obowiązek informowania

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

Artykuł 23

Współpraca z właściwymi organami

Dostawcy systemów sztucznej inteligencji wysokiego ryzyka, na żądanie właściwego organu krajowego, przekazują temu organowi wszelkie informacje i dokumenty niezbędne do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, w języku łatwo zrozumiałym dla danego organu krajowego danego państwa członkowskiego. Na uzasadniony wniosek właściwego organu krajowego dostawcy zapewniają również temu organowi dostęp do generowanych automatycznie przez system sztucznej inteligencji 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 na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa.

Artykuł 23a

Warunki, na jakich inne osoby podlegają obowiązkom równoważnym obowiązkom dostawcy

1. Do celów niniejszego rozporządzenia za dostawcę nowego systemu sztucznej inteligencji wysokiego ryzyka uznaje się i obejmuje obowiązkami dostawcy na podstawie art. 16 każdą osobę fizyczną lub prawną, w dowolnym z poniższych przypadków:

    a) jeżeli umieszcza swoją nazwę lub znak towarowy w systemie sztucznej inteligencji 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) [skreśla się]

c) jeżeli wprowadza istotne zmiany w systemie sztucznej inteligencji wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku;

d) jeżeli zmienia przeznaczenie systemu sztucznej inteligencji nieobarczonego wysokim ryzykiem, który został już wprowadzony do obrotu lub oddany do użytku, w taki sposób, że zmodyfikowany system staje się systemem sztucznej inteligencji wysokiego ryzyka;

e) jeżeli wprowadza do obrotu lub oddaje do użytku system sztucznej inteligencji ogólnego przeznaczenia jako system sztucznej inteligencji wysokiego ryzyka lub jako element systemu sztucznej inteligencji wysokiego ryzyka.

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

3. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, które stanowią związane z bezpieczeństwem elementy produktów objętych zakresem stosowania aktów prawnych wymienionych w załączniku II sekcja A, producenta tych produktów uznaje się za dostawcę systemu sztucznej inteligencji wysokiego ryzyka i podlega on obowiązkom na podstawie w art. 16, zgodnie z jednym z następujących scenariuszy:

(i) system sztucznej inteligencji wysokiego ryzyka jest wprowadzany do obrotu wraz z produktem pod nazwą lub znakiem towarowym producenta produktu;

(ii) system sztucznej inteligencji wysokiego ryzyka jest oddawany do użytku pod nazwą lub znakiem towarowym producenta produktu po wprowadzeniu produktu do obrotu.

Artykuł 24

[skreśla się]

PUBLIC

Artykuł 25

Upoważnieni przedstawiciele

1. Przed wprowadzeniem swoich systemów na rynek Unii dostawcy mający siedzibę poza terytorium Unii są zobowiązani wyznaczyć – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego siedzibę w Unii.

2. Upoważniony przedstawiciel wykonuje zadania powierzone mu na mocy pełnomocnictwa udzielonego przez dostawcę. Do celów niniejszego rozporządzenia pełnomocnictwo uprawnia upoważnionego przedstawiciela do wykonywania jedynie następujących zadań:

-a) sprawdzenie, czy zostały sporządzone deklaracja zgodności UE i dokumentacja techniczna oraz czy została przeprowadzona przez dostawcę odpowiednia procedura oceny zgodności;

a) przechowywanie do dyspozycji właściwych organów krajowych i organów krajowych, o których mowa w art. 63 ust. 7, przez okres 10 lat od wprowadzenia do obrotu lub oddania do użytku systemu sztucznej inteligencji wysokiego ryzyka, dane kontaktowe dostawcy, przez którego dany upoważniony przedstawiciel został wyznaczony, kopię deklaracji zgodności UE, dokumentację techniczną oraz, w stosownych przypadkach, certyfikat wydany przez jednostkę notyfikowaną;

b) przekazywanie właściwemu organowi krajowemu na jego uzasadniony wniosek wszelkich informacji i dokumentów, w tym przechowywanych zgodnie z lit. b), niezbędnych do wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu, w tym zapewnienie temu organowi dostępu do generowanych automatycznie przez system sztucznej inteligencji 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 na podstawie ustaleń umownych z użytkownikiem lub z mocy prawa;

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

d) wypełnianie obowiązków rejestracyjnych, o których mowa w art. 51 ust. 1, oraz – przypadku gdy dostawca sam dokonuje rejestracji systemu, sprawdzenie, czy informacje, o których mowa w załączniku VIII część II pkt 1–11 są prawidłowe.

Upoważniony przedstawiciel wypowiada pełnomocnictwo, jeśli ma wystarczające powody sądzić, że dostawca działa w sposób naruszający jego obowiązki wynikające z niniejszego rozporządzenia. W takim przypadku o wypowiedzeniu pełnomocnictwa i jego przyczynach informuje on niezwłocznie również organ nadzoru rynku państwa członkowskiego, w którym ma siedzibę, a także, w stosownych przypadkach, odpowiednią jednostkę notyfikowaną.

Upoważniony przedstawiciel ponosi odpowiedzialność prawną za wadliwe systemy sztucznej inteligencji na takich samych zasadach jak dostawca i solidarnie z dostawcą w odniesieniu do jego potencjalnej odpowiedzialności na podstawie dyrektywy Rady 85/374/EWG.

Artykuł 26

Obowiązki importerów

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

   a) dostawca tego systemu sztucznej inteligencji przeprowadził stosowną procedurę oceny zgodności, o której mowa w art. 43;

   b) dostawca sporządził dokumentację techniczną zgodnie z załącznikiem IV;

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

   d) dostawca wyznaczył upoważnionego przedstawiciela, o którym mowa w art. 25.

2. W przypadku gdy importer ma wystarczające powody, aby uważać, że system sztucznej inteligencji wysokiego ryzyka jest niezgodny z niniejszym rozporządzeniem lub został sfałszowany lub sfałszowana została jego dokumentacja, nie wprowadza tego systemu do obrotu, dopóki nie zapewniona zostanie zgodność tego systemu sztucznej inteligencji z przepisami niniejszego rozporządzenia. Jeżeli system sztucznej inteligencji wysokiego ryzyka stwarza ryzyko w rozumieniu art. 65 ust. 1, importer informuje o tym dostawcę systemu sztucznej inteligencji, upoważnionych przedstawicieli oraz organy nadzoru rynku.

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

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

4a. Importerzy, przez okres, który upływa 10 lat po wprowadzeniu systemu sztucznej inteligencji do obrotu lub oddania go do użytku, przechowują kopię certyfikatu wydanego przez jednostkę notyfikowaną, w stosownych przypadkach, instrukcji obsługi oraz deklaracji zgodności UE.

5. Na uzasadnione żądanie właściwych organów krajowych importerzy przekazują im wszelkie niezbędne informacje i dokumentację, w tym przechowywane zgodnie z ust. 5, w celu wykazania zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w rozdziale 2 niniejszego tytułu, w języku łatwo zrozumiałym dla danego właściwego organu krajowego. W tym celu zapewniają również możliwość udostępnienia temu organowi dokumentacji technicznej.

5a. Importerzy współpracują z właściwymi organami krajowymi przy wszelkich działaniach podejmowanych przez te organy w związku z systemem sztucznej inteligencji, którego są importerami.

Artykuł 27

Obowiązki dystrybutorów

1. Przed wprowadzeniem systemu sztucznej inteligencji wysokiego ryzyka do obrotu dystrybutorzy upewniają się, że system sztucznej inteligencji wysokiego ryzyka został opatrzony wymaganym oznakowaniem zgodności CE, że załączono do niego kopię deklaracji zgodności UE i instrukcję obsługi oraz że dostawca oraz – w stosownych przypadkach – importer systemu wywiązali się z obowiązków określonych odpowiednio w art. 16 lit. b) i art. 26 ust. 3.

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

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

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

5. Na uzasadniony wniosek właściwego organu krajowego dystrybutorzy systemów sztucznej inteligencji wysokiego ryzyka przekazują temu organowi wszelkie informacje i dokumentację dotyczące jego działania, jak opisano w ust. 1–4.

5a. Dystrybutorzy współpracują z właściwymi organami krajowymi przy wszelkich działaniach podejmowanych przez te organy w związku z systemem sztucznej inteligencji, którego są dystrybutorami.

Artykuł 28

[skreśla się]

Artykuł 29

Obowiązki użytkowników systemów sztucznej inteligencji wysokiego ryzyka

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

1a. Użytkownicy powierzają sprawowanie nadzoru ze strony człowieka osobom fizycznym, które mają niezbędne kompetencje, ukończone szkolenia i uprawnienia.

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

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

PUBLIC

4. Użytkownicy wprowadzają sprawowanie nadzoru ze strony człowieka i monitorują działanie systemu sztucznej inteligencji wysokiego ryzyka w oparciu o instrukcję obsługi. Jeżeli użytkownicy mają powody przypuszczać, że użytkowanie systemu sztucznej inteligencji zgodnie z instrukcją obsługi może doprowadzić do powstania ryzyka w rozumieniu art. 65 ust. 1, informują o tym fakcie dostawcę lub dystrybutora i wstrzymują użytkowanie systemu. Użytkownicy zgłaszają również dostawcy lub dystrybutorowi wszelkie stwierdzone przez siebie poważne incydenty i zaprzestają użytkowania systemu sztucznej inteligencji. Jeżeli użytkownik nie jest w stanie skontaktować się z dostawcą, stosuje się odpowiednio przepisy art. 62. Obowiązek ten nie obejmuje wrażliwych danych operacyjnych użytkowników systemów sztucznej inteligencji będących organami ścigania.

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

5. Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka przechowują generowane automatycznie przez dany system sztucznej inteligencji 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. Przechowują je przez okres co najmniej sześciu miesięcy, chyba że mające zastosowanie prawo unijne lub krajowe stanowi inaczej, w szczególności unijne prawo ochrony danych osobowych.

Użytkownicy będący instytucjami finansowymi, które podlegają wymogom dotyczącym ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych, prowadzą rejestry zdarzeń jako część dokumentacji prowadzonej zgodnie z odpowiednimi unijnymi przepisami dotyczącymi usług finansowych.

5a. Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka będący publicznymi organami, agencjami lub jednostkami organizacyjnymi, z wyjątkiem organów ścigania, organów kontroli granicznej, organów imigracyjnych lub organów odpowiedzialnych za udzielanie azylu, spełniają obowiązki rejestracji, o których mowa w art. 51. Jeżeli stwierdzą, że system, z którego zamierzają korzystać, nie został zarejestrowany w bazie danych UE, o której mowa w art. 60, nie korzystają z tego systemu i informują o tym dostawcę lub dystrybutora.

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

6a. Użytkownicy współpracują z właściwymi organami krajowymi przy wszelkich działaniach podejmowanych przez te organy w związku z systemem sztucznej inteligencji, którego są użytkownikami.

PUBLIC

ROZDZIAŁ 4

ORGANY NOTYFIKUJĄCE I JEDNOSTKI NOTYFIKOWANE

Artykuł 30

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.

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

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

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

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

6. Organy notyfikujące zapewniają poufność gromadzonych informacji zgodnie z art. 70.

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

8. [skreśla się]

Artykuł 31

Wniosek jednostki oceniającej zgodność o notyfikację

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

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

PUBLIC

3. Jeżeli zainteresowana jednostka oceniająca zgodność nie jest w stanie przedstawić certyfikatu akredytacji, przekazuje organowi notyfikującemu wszystkie dowody w postaci dokumentów niezbędne do zweryfikowania, potwierdzenia i regularnego monitorowania przestrzegania przez tę jednostkę wymogów ustanowionych w art. 33. W odniesieniu do jednostek notyfikowanych wyznaczonych na podstawie wszelkiego innego unijnego prawodawstwa harmonizacyjnego w stosownych przypadkach dopuszcza się możliwość wykorzystania wszelkich dokumentów i certyfikatów dotyczącego takiego wyznaczenia w charakterze dowodów w toku procedury wyznaczania przeprowadzanej zgodnie z niniejszym rozporządzeniem. Jednostka notyfikowana aktualizuje dokumentację, o której mowa w ust. 2 i 3, gdy tylko wystąpią istotne zmiany, aby organowi odpowiedzialnemu za jednostki notyfikowane umożliwić monitorowanie i weryfikowanie ciągłej zgodności ze wszystkimi wymogami ustanowionymi w art. 33.

Artykuł 32

Procedura notyfikacyjna

1. Organy notyfikujące mogą dokonać notyfikacji tylko tych jednostek oceniających zgodność, które spełniają wymogi ustanowione w art. 33.

2. Organy notyfikujące notyfikują te jednostki Komisji i pozostałym państwom członkowskim za pomocą systemu notyfikacji elektronicznej, opracowanego i zarządzanego przez Komisję.

3. Notyfikacja, o której mowa w ust. 2, zawiera wyczerpujące, szczegółowe informacje na temat czynności z zakresu oceny zgodności, modułu lub modułów oceny zgodności i przedmiotowych systemów w sztucznej inteligencji oraz odpowiednie poświadczenie kompetencji. W przypadku gdy podstawą notyfikacji nie jest certyfikat akredytacji, o którym mowa w art. 31 ust. 2, organ notyfikujący przedkłada Komisji i pozostałym państwom członkowskim dowody w postaci dokumentów potwierdzające kompetencje jednostki oceniającej zgodność oraz wprowadzone ustalenia zapewniające regularne monitorowanie tej jednostki i dalsze spełnianie przez nią wymagań ustanowionych w art. 33.

4. Dana jednostka oceniająca zgodność może wykonywać działania jednostki notyfikowanej tylko wówczas, gdy Komisja lub pozostałe państwa członkowskie nie zgłosiły zastrzeżeń w terminie dwóch tygodni od notyfikacji przez organ notyfikujący, w przypadku gdy notyfikacja ta obejmuje certyfikat akredytacji, o którym mowa w art. 31 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. 31 ust. 3.

5. [skreśla się]

Artykuł 33

Wymogi dotyczące jednostek notyfikowanych

1. Jednostka notyfikowana jest ustanawiana zgodnie z prawem krajowym i ma osobowość prawną.

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

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

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

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

PUBLIC

6. Jednostki notyfikowane dysponują udokumentowanymi procedurami, które zapewniają zachowanie przez ich personel, komitety, jednostki zależne, podwykonawców oraz wszelkie stowarzyszone z nimi jednostki lub pracowników podmiotów zewnętrznych poufności – zgodnie z art. 70 – informacji, które znalazły się w ich posiadaniu w toku czynności z zakresu oceny zgodności, chyba że ujawnienie takich informacji jest wymagane na mocy obowiązującego prawa. Personel jednostek notyfikowanych pozostaje związany tajemnicą zawodową w kwestii wszystkich informacji pozyskiwanych w toku wykonywania zadań powierzonych mu zgodnie z niniejszym rozporządzeniem, z wyjątkiem działań podejmowanych w odniesieniu do organów notyfikujących państwa członkowskiego, w którym wykonuje on te zadania.

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

8. Jednostki notyfikowane zawierają odpowiednie umowy ubezpieczenia od odpowiedzialności cywilnej w odniesieniu do podejmowanych przez siebie czynności z zakresu oceny zgodności, chyba że 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.

9. Jednostki notyfikowane posiadają zdolność wykonywania wszystkich zadań powierzonych im na podstawie niniejszego rozporządzenia z zachowaniem najwyższego poziomu uczciwości zawodowej i wymaganych kompetencji w danej dziedzinie, niezależnie od tego, czy zadania te są wykonywane przez nie samodzielnie, czy też w ich imieniu i na ich odpowiedzialność.

10. Jednostki notyfikowane dysponują wystarczającymi kompetencjami wewnętrznymi, aby należycie oceniać zadania wykonywane w ich imieniu przez podmioty zewnętrzne. Jednostka notyfikowana zawsze zapewnia stałą dostępność odpowiedniej liczby pracowników administracyjnych, technicznych i naukowych dysponujących doświadczeniem i wiedzą w zakresie stosowania odpowiednich technologii sztucznej inteligencji, danych i metod przetwarzania danych oraz w zakresie wymogów ustanowionych w rozdziale 2 niniejszego tytułu.

PUBLIC

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

12. [skreśla się]

PUBLIC

Artykuł 33a

Domniemanie zgodności z wymogami dotyczącymi jednostek notyfikowanych

W przypadku gdy jednostka oceniająca zgodność wykaże swoją zgodność z kryteriami ustanowionymi w odpowiednich normach zharmonizowanych lub części tych norm, do których odniesienia opublikowano w Dzienniku Urzędowym Unii Europejskiej, zakłada się, że spełnia ona wymogi ustanowione w rozdziale 33 w zakresie, w jakim mające zastosowanie normy zharmonizowane obejmują te wymogi.

Artykuł 34

Jednostki zależne i podwykonawcy jednostek notyfikowanych

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

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

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

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

Artykuł 34a

Obowiązki operacyjne jednostek notyfikowanych

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

2. Jednostki notyfikowane wykonują powierzone im zadania, unikając przy tym niekoniecznych obciążeń dla dostawców oraz uwzględniając rozmiar przedsiębiorstwa, sektora, w którym prowadzi ono działalność, jego struktury oraz stopnia złożoności danego systemu sztucznej inteligencji wysokiego ryzyka. Czyniąc to, jednostka notyfikowana przestrzega jednak stopnia rygorystyczności i poziomu ochrony wymaganych do celów zgodności danego systemu sztucznej inteligencji wysokiego ryzyka z wymogami niniejszego rozporządzenia.

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

Artykuł 35

Numery identyfikacyjne i wykazy jednostek notyfikowanych wyznaczonych zgodnie z niniejszym rozporządzeniem

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

PUBLIC

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

Artykuł 36

Zmiany w notyfikacjach

1. Organ notyfikujący powiadamia Komisję i pozostałe państwa członkowskie za pomocą systemu notyfikacji elektronicznej, o którym mowa w art. 32 ust. 2, o wszelkich istotnych zmianach w notyfikacji danej jednostki notyfikowanej.

2. Procedury opisane w art. 31 i 32 mają zastosowanie do rozszerzenia zakresu notyfikacji. W przypadku zmian w notyfikacji innych niż rozszerzenie jej zakresu stosuje się procedury ustanowione w ustępach poniżej.

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

PUBLIC

3. W przypadku gdy organ notyfikujący ma wystarczające powody, by uznać, że jednostka notyfikowana przestała spełniać wymogi ustanowione w art. 33 lub nie wypełnia swoich obowiązków, organ notyfikujący – pod warunkiem że jednostka notyfikowana miała możliwość przedstawienia swojej opinii – odpowiednio ogranicza, zawiesza lub cofa notyfikację, w zależności od wagi niespełnienia tych wymogów lub niewypełnienia obowiązków. Organ notyfikujący niezwłocznie informuje o tym fakcie odpowiednio Komisję i pozostałe państwa członkowskie.

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

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

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

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

   b) przedkłada Komisji i pozostałym państwom członkowskim sprawozdanie ze swoich ustaleń w ciągu trzech miesięcy od notyfikowania zmian w notyfikacji;

   c) zwraca się do jednostki notyfikowanej, by w celu zapewnienia zgodności systemów sztucznej inteligencji 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;

PUBLIC

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

7. Z wyjątkiem certyfikatów nienależnie wydanych oraz w przypadkach, w których zawieszono lub ograniczono notyfikację, certyfikaty pozostają ważne w następujących okolicznościach:

a) organ notyfikujący potwierdził, w terminie jednego miesiąca od zawieszenia lub ograniczenia, że w odniesieniu do certyfikatów, których dotyczy to zawieszenie lub ograniczenie, nie występuje zagrożenie zdrowia, bezpieczeństwa lub praw podstawowych i określił przewidywany czas i działania służące 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 ustala, czy dana jednostka notyfikowana jest zdolna do dalszego monitorowania i bycia odpowiedzialną za istniejące certyfikaty wydane na okres zawieszenia lub ograniczenia. W przypadku gdy organ odpowiedzialny za jednostki notyfikowane ustali, że jednostka notyfikowana nie posiada zdolności do obsługi wydanych certyfikatów, dostawca – w terminie trzech miesięcy od zawieszenia lub ograniczenia – przekazuje właściwemu organowi krajowemu w państwie członkowskim, w którym dostawca systemu objętego certyfikatem ma zarejestrowane miejsce prowadzenia działalności, potwierdzenie na piśmie, że inna wykwalifikowana jednostka notyfikowana tymczasowo przejmuje funkcje jednostki notyfikowanej w zakresie monitorowania i pozostanie ona odpowiedzialna za te certyfikaty w okresie zawieszenia lub ograniczenia.

8. Z wyjątkiem certyfikatów nienależnie wydanych oraz w przypadkach, w których zawieszono lub ograniczono wyznaczenie, certyfikaty pozostają ważne przez okres dziewięciu miesięcy w następujących okolicznościach:

a) w przypadku gdy właściwy organ krajowy w państwie członkowskim, w którym dostawca systemu sztucznej inteligencji objętego certyfikatem ma zarejestrowane miejsce prowadzenia działalności, potwierdził, że nie występuje zagrożenie zdrowia, bezpieczeństwa lub praw podstawowych związane z danym systemem; oraz

b) inna jednostka notyfikowana potwierdziła na piśmie, że przejmie bezpośrednią odpowiedzialność za te systemy i zakończy ich ocenę w terminie dwunastu miesięcy od cofnięcia wyznaczenia.

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

Właściwy organ krajowy lub jednostka notyfikowana przejmująca funkcje jednostki notyfikowanej, której notyfikacja została zmieniona, niezwłocznie powiadamiają o tym Komisję, pozostałe państwa członkowskie i pozostałe jednostki notyfikowane.

Artykuł 37

Kwestionowanie kompetencji jednostek notyfikowanych

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

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

3. Komisja zapewnia zgodnie z art. 70 poufność wszystkich informacji poufnych uzyskanych w toku postępowań wyjaśniających prowadzonych zgodnie z niniejszym artykułem.

4. W przypadku gdy Komisja stwierdzi, że jednostka notyfikowana nie spełnia lub przestała spełniać wymogi ustanowione w art. 33, informuje organ notyfikujący o przyczynach takiego stwierdzenia i zwraca się do niego o wdrożenie koniecznych środków naprawczych, obejmujących, w razie potrzeby, zawieszenie, ograniczenie lub cofnięcie wyznaczenia. W przypadku niewprowadzenia przez organ notyfikujący koniecznych środków naprawczych Komisja może w drodze aktów wykonawczych zawiesić, ograniczyć lub cofnąć notyfikację. Wspomniany akt wykonawczy przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Artykuł 38

Koordynacja jednostek notyfikowanych

1. Komisja zapewnia – w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka – wprowadzenie i właściwy przebieg odpowiedniej koordynacji i współpracy jednostek notyfikowanych prowadzących działalność w zakresie procedur oceny zgodności na mocy niniejszego rozporządzenia – w formie sektorowej grupy jednostek notyfikowanych.

2. Organ notyfikujący zapewnia, aby notyfikowane przez niego jednostki uczestniczyły w pracach tej grupy bezpośrednio lub za pośrednictwem wyznaczonych przedstawicieli.

Artykuł 39

Jednostki oceniające zgodność z państw trzecich

Jednostki oceniające zgodność ustanowione na mocy prawa państwa trzeciego, z którym Unia zawarła umowę, mogą być upoważnione do prowadzenia działalności właściwej dla jednostek notyfikowanych zgodnie z niniejszym rozporządzeniem, z zastrzeżeniem spełniania przez nie wymogów art. 33.

PUBLIC

ROZDZIAŁ 5

NORMY, OCENA ZGODNOŚCI, CERTYFIKATY, REJESTRACJA

Artykuł 40

Normy zharmonizowane

1. Systemy sztucznej inteligencji wysokiego ryzyka lub systemy sztucznej inteligencji ogólnego przeznaczenia spełniające normy zharmonizowane lub części tych norm, do których odniesienia opublikowano w Dzienniku Urzędowym Unii Europejskiej, uznaje się za spełniające wymogi określone w rozdziale 2 niniejszego tytułu lub, w stosownych przypadkach, wymogi określone w art. 4a i 4b, w zakresie, w jakim wspomniane normy obejmują te wymogi.

2. Kierując wniosek o normalizację do europejskich organizacji normalizacyjnych zgodnie z art. 10 rozporządzenia nr 1025/2012, Komisja stwierdza, że normy są spójne, jasne i opracowane w taki sposób, aby służyły osiągnięciu w szczególności następujących celów:

   a) zapewnienie, aby systemy sztucznej inteligencji wprowadzane do obrotu lub oddawane do użytku w Unii były bezpieczne i zgodne z wartościami Unii oraz wzmacniały otwartą strategiczną autonomię Unii;

   b) promowanie inwestycji i innowacji w dziedzinie sztucznej inteligencji, w tym poprzez zwiększenie pewności prawa, a także konkurencyjności i wzrostu rynku Unii;

   c) wzmocnienie zarządzania z udziałem wielu zainteresowanych stron reprezentujących wszystkie odpowiednie zainteresowane strony europejskie (np. przemysł, MŚP, społeczeństwo obywatelskie, badaczy);

   d) przyczynianie się do zacieśnienia globalnej współpracy w zakresie normalizacji w dziedzinie sztucznej inteligencji, spójnej z wartościami i interesami Unii.

   Komisja zwraca się do europejskich organizacji normalizacyjnych o przedstawienie dowodów, że dokładają wszelkich starań, aby osiągnąć powyższe cele.

PUBLIC

Artykuł 41

Wspólne specyfikacje

1. Komisja jest uprawniona do przyjmowania – po konsultacji z Radą ds. Sztucznej Inteligencji, o której mowa w art. 56 – aktów wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2, ustanawiających wspólne specyfikacje techniczne w odniesieniu do wymogów określonych w rozdziale 2 niniejszego tytułu lub, w stosownych przypadkach, zgodnie z wymogami określonymi w art. 4a i 4b, przy spełnieniu następujących warunków:

   a) w Dzienniku Urzędowym Unii Europejskiej nie opublikowano odniesienia zgodnie z rozporządzeniem (UE) nr 1025/2012 do norm zharmonizowanych obejmujących określone zasadnicze zastrzeżenia dotyczące bezpieczeństwa lub poszanowania praw podstawowych,

   b) Komisja wystąpiła zgodnie z art. 10 ust. 1 rozporządzenia 1025/2012 do jednej lub kilku europejskich organizacji normalizacyjnych z wnioskiem o opracowanie normy zharmonizowanej w odniesieniu do wymogów określonych w rozdziale 2 niniejszego tytułu;

   c) wniosek, o którym mowa w lit. b), nie został przyjęty przez żadną z europejskich organizacji normalizacyjnych lub normy zharmonizowane dotyczące tego wniosku nie zostały przygotowane w terminie wyznaczonym zgodnie z art. 10 ust. 1 rozporządzenia 1025/2012 lub normy te nie spełniają założeń tego wniosku.

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

2. Na wczesnym etapie przygotowywania projektu aktu wykonawczego ustanawiającego wspólną specyfikację Komisja realizuje cele, o których mowa w art. 40 ust. 2, i gromadzi opinie odpowiednich organów lub grup ekspertów ustanowionych na podstawie odpowiednich przepisów sektorowych Unii. Na podstawie tych konsultacji Komisja przygotowuje projekt aktu wykonawczego.

PUBLIC

3. Systemy sztucznej inteligencji wysokiego ryzyka lub systemy sztucznej inteligencji ogólnego przeznaczenia zgodne ze wspólnymi specyfikacjami, o których mowa w ust. 1, uznaje się za spełniające wymogi określone w rozdziale 2 niniejszego tytułu lub, w stosownych przypadkach, z wymogami określonymi w art. 4a i 4b, w zakresie, w jakim te wspólne specyfikacje obejmują te wymogi.

4. Kiedy odniesienia do normy zharmonizowanej są publikowane w Dzienniku Urzędowym Unii Europejskiej, akty wykonawcze, o których mowa w ust. 1, obejmujące wymogi określone w rozdziale 2 niniejszego tytułu lub wymogi określone w art. 4a i 4b zostają w stosownych przypadkach uchylone.

5. Kiedy państwo członkowskie uzna, że wspólna specyfikacja nie do końca spełnia wymogi określone w rozdziale 2 niniejszego tytułu lub – stosownie do przypadku – wymogi określone w art. 4a i 4b, informuje o tym Komisję wraz ze szczegółowym wyjaśnieniem, a Komisja ocenia te informacje i w stosownych przypadkach zmienia akt wykonawczy ustanawiający przedmiotową wspólną specyfikację.

Artykuł 42

Domniemanie zgodności z określonymi wymogami

1. Systemy sztucznej inteligencji wysokiego ryzyka, które zostały wytrenowane i przetestowane przy użyciu danych odzwierciedlających określone środowisko geograficzne, behawioralne i funkcjonalne, w którym planuje się z nich korzystać, uznaje się za spełniające odpowiednie wymogi określone w art. 10 ust. 4.

PUBLIC

2. Systemy sztucznej inteligencji wysokiego ryzyka lub systemy sztucznej inteligencji ogólnego przeznaczenia, które uzyskały certyfikację lub w odniesieniu do których wydano deklarację zgodności w ramach programu certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881[33] i do których odniesienia opublikowano w Dzienniku Urzędowym Unii Europejskiej, uznaje się za spełniające wymogi w zakresie cyberbezpieczeństwa ustanowione w art. 15 niniejszego rozporządzenia w zakresie, w jakim certyfikat cyberbezpieczeństwa lub deklaracja zgodności, lub ich części obejmują te wymogi.

Artykuł 43

Ocena zgodności

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

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

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

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

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

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

2. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2–8, oraz systemów sztucznej inteligencji ogólnego przeznaczenia, o których mowa w tytule 1a, 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 sztucznej inteligencji wysokiego ryzyka, do których zastosowanie mają akty prawne wymienione w załączniku II sekcja A, dostawca przeprowadza odpowiednią ocenę zgodności wymaganą na podstawie tych aktów prawnych. W odniesieniu do tego rodzaju systemów sztucznej inteligencji wysokiego ryzyka zastosowanie mają wymogi ustanowione w rozdziale 2 niniejszego tytułu i stanowią one jeden z elementów tej oceny. W takim przypadku zastosowanie mają również przepisy załącznika VII pkt 4.3, pkt 4.4, pkt 4.5 i pkt 4.6 akapit piąty.

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

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

4. [skreśla się]

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73, aby zaktualizować załączniki VI i VII z uwagi na postęp techniczny.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych, aby zmienić przepisy ust. 1 i 2 w celu objęcia systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2–8, procedurą oceny zgodności, o której mowa w załączniku VII, lub elementami tej procedury. Komisja przyjmuje takie akty delegowane, biorąc pod uwagę skuteczność procedury oceny zgodności opierającej się na kontroli wewnętrznej, o której mowa w załączniku VI, w zapobieganiu zagrożeniom dla zdrowia i bezpieczeństwa oraz ochrony praw podstawowych stwarzanym przez takie systemy lub minimalizowaniu tych zagrożeń, a także uwzględniając dostępność odpowiednich zdolności i zasobów wśród jednostek notyfikowanych.

Artykuł 44

Certyfikaty

1. Certyfikaty 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. Na wniosek dostawcy ważność certyfikatu można przedłużyć na kolejne okresy, które nie mogą każdorazowo przekraczać pięciu lat, w oparciu o wyniki ponownej oceny przeprowadzonej zgodnie z mającymi zastosowanie procedurami oceny zgodności. Wszelkie uzupełnienia do certyfikatu pozostają ważne przez okres ważności tego certyfikatu.

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

PUBLIC

Artykuł 45

Odwołanie od decyzji jednostek notyfikowanych

Dostępna jest procedura odwoławcza od decyzji jednostek notyfikowanych.

Artykuł 46

Obowiązki jednostek notyfikowanych w zakresie informowania

1. Jednostki notyfikowane informują organ notyfikujący:

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

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

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

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

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

2. Każda jednostka notyfikowana informuje pozostałe jednostki notyfikowane:

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

PUBLIC

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

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

4. Obowiązki, o których mowa w ust. 1–3, są wypełniane zgodnie z art. 70.

Artykuł 47

Odstępstwo od procedury oceny zgodności

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

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

2. Zezwolenie, o którym mowa w ust. 1, wydaje się wyłącznie wówczas, gdy organ nadzoru rynku stwierdzi, że system sztucznej inteligencji wysokiego ryzyka spełnia wymogi ustanowione w rozdziale 2 niniejszego tytułu. Organ nadzoru rynku informuje Komisję i pozostałe państwa członkowskie o wszelkich zezwoleniach wydanych zgodnie z ust. 1. Obowiązek ten nie obejmuje wrażliwych danych operacyjnych dotyczących działalności organów ścigania.

3. [skreśla się]

4. [skreśla się]

5. [skreśla się]

6. Do systemów sztucznej inteligencji wysokiego ryzyka związanych z produktami objętymi unijnym prawodawstwem harmonizacyjnym, o którym mowa w załączniku II sekcja A, zastosowanie mają wyłącznie odstępstwa od procedur oceny zgodności ustanowione w tym prawodawstwie.

Artykuł 48

Deklaracja zgodności UE

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

2. W deklaracji zgodności UE potwierdza się, że dany system sztucznej inteligencji wysokiego ryzyka spełnia wymogi ustanowione w rozdziale 2 niniejszego tytułu. Deklaracja zgodności UE zawiera informacje przedstawione w załączniku V i musi zostać przetłumaczona na język łatwo zrozumiały dla właściwych organów krajowych państw członkowskich, w których udostępniany jest dany system sztucznej inteligencji wysokiego ryzyka.

PUBLIC

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

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

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

Artykuł 49

Oznakowanie zgodności CE

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

2. Oznakowanie CE umieszcza się na systemie sztucznej inteligencji wysokiego ryzyka w sposób widoczny, czytelny i trwały. Jeżeli z uwagi na charakter systemu sztucznej inteligencji wysokiego ryzyka oznakowanie systemu w powyższy sposób nie jest możliwe lub uzasadnione, oznakowanie to umieszcza się na opakowaniu lub – w stosownych przypadkach – w dokumentacji towarzyszącej systemowi.

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

Artykuł 50

[skreśla się]

Artykuł 51

Rejestracja odpowiednich operatorów i systemów sztucznej inteligencji wysokiego ryzyka umieszczonych w załączniku III

1. Przed wprowadzeniem do obrotu lub oddaniem do użytku systemu sztucznej inteligencji wysokiego ryzyka wymienionego w załączniku III, z wyjątkiem systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7 w obszarach egzekwowania prawa, zarządzania migracją, azylem i kontrolą graniczną oraz z wyjątkiem systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2, dostawca oraz, w stosownych przypadkach, upoważniony przedstawiciel rejestrują się w unijnej bazie danych, o której mowa w art. 60. Dostawca lub, w stosownych przypadkach, upoważniony przedstawiciel również rejestrują swoje systemy w tej bazie danych.

2. Przed zastosowaniem systemu sztucznej inteligencji wysokiego ryzyka wymienionego w załączniku III użytkownicy systemów sztucznej inteligencji wysokiego ryzyka będący publicznymi organami, agencjami lub jednostkami organizacyjnymi, lub podmioty działające w ich imieniu, rejestrują się w unijnej bazie danych, o której mowa w art. 60, i wybierają system, z którego zamierzają skorzystać.

   Obowiązki ustanowione w poprzednim akapicie nie mają zastosowania do organów ścigania, agencji lub jednostek organizacyjnych zajmujących się zarządzaniem kontrolą graniczną, migracją lub azylem oraz organów, agencji lub jednostek organizacyjnych wykorzystujących systemy sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2, jak również do podmiotów występujących w ich imieniu.

PUBLIC

TYTUŁ IV

OBOWIĄZKI W ZAKRESIE PRZEJRZYSTOŚCI DLA DOSTAWCÓW I UŻYTKOWNIKÓW OKREŚLONYCH SYSTEMÓW SZTUCZNEJ INTELIGENCJI

PUBLIC

Artykuł 52

Obowiązki w zakresie przejrzystości dla dostawców i użytkowników określonych systemów sztucznej inteligencji

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

2. Użytkownicy systemów kategoryzacji biometrycznej informują osoby fizyczne, wobec których systemy te są stosowane, o fakcie ich stosowania. Obowiązek ten nie ma zastosowania do systemów sztucznej inteligencji wykorzystywanych do kategoryzacji biometrycznej zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom i prowadzenia postępowań przygotowawczych w związku z przestępstwami, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.

2a. Użytkownicy systemów rozpoznawania emocji informują osoby fizyczne, wobec których systemy te są stosowane, o fakcie ich stosowania. Obowiązek ten nie ma zastosowania do systemów sztucznej inteligencji wykorzystywanych do rozpoznawania emocji zatwierdzonych z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia postępowań przygotowawczych w związku z przestępstwami, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.

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

Przepisy akapitu pierwszego nie mają jednak zastosowania w przypadku, gdy korzystanie z takich rozwiązań zatwierdzono z mocy prawa do celów wykrywania przestępstw, przeciwdziałania przestępstwom, prowadzenia postępowań przygotowawczych w związku z przestępstwami i ścigania ich sprawców lub w przypadku, gdy treści te stanowią część dzieła lub programu mającego wyraźnie charakter twórczy, satyryczny, artystyczny lub fikcyjny, z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.

3a. Informacje, o których mowa w ust. 1–3, są przekazywane osobom fizycznym w jasny i wyraźny sposób, najpóźniej w momencie pierwszej interakcji lub kontaktu.

4. Przepisy ust. 1, 2, 2a, 3 oraz 3a pozostają bez wpływu na wymogi i obowiązki ustanowione w tytule III niniejszego rozporządzenia i pozostają bez uszczerbku dla innych, określonych w prawie Unii lub prawie krajowym, obowiązków w zakresie przejrzystości dla użytkowników systemów sztucznej inteligencji.

TYTUŁ V

ŚRODKI WSPIERAJĄCE INNOWACYJNOŚĆ

Artykuł 53

Piaskownice regulacyjne w zakresie sztucznej inteligencji

-1a. Właściwe organy krajowe mogą ustanowić piaskownice regulacyjne w zakresie sztucznej inteligencji na potrzeby opracowywania, trenowania, testowania i walidowania innowacyjnych systemów sztucznej inteligencji pod bezpośrednim nadzorem i kierunkiem właściwego organu krajowego i przy jego wsparciu, zanim systemy te zostaną wprowadzone do obrotu lub oddane do użytku. Takie piaskownice regulacyjne mogą obejmować testy w warunkach rzeczywistych nadzorowane przez właściwe organy krajowe.

-1b. [skreśla się]

-1c W stosownych przypadkach właściwe organy krajowe współpracują z innymi odpowiednimi organami i mogą zezwolić na zaangażowanie innych podmiotów z ekosystemu sztucznej inteligencji.

-1d. Niniejszy artykuł nie ma wpływu na inne piaskownice regulacyjne ustanowione na mocy prawa krajowego lub prawa Unii, w tym w przypadkach gdy produkty lub usługi, które są w nich testowane, są powiązane z wykorzystaniem innowacyjnych systemów sztucznej inteligencji. Państwa członkowskie zapewniają odpowiedni poziom współpracy między organami nadzorującymi te inne piaskownice a właściwymi organami krajowymi.

1. [skreśla się]

1a. [skreśla się]

1b. Ustanowienie piaskownic regulacyjnych w zakresie sztucznej inteligencji na podstawie niniejszego rozporządzenia ma na celu przyczynienie się do osiągnięcia co najmniej jednego z następujących celów:

a) wzmacnianie innowacyjności i konkurencyjności oraz ułatwianie rozwoju ekosystemu sztucznej inteligencji;
b) ułatwianie i przyspieszanie dostępu do unijnego rynku dla systemów sztucznej inteligencji, w szczególności gdy są one oferowane przez małe i średnie przedsiębiorstwa (MŚP), w tym przedsiębiorstwa typu start-up;
c) zwiększenie pewności prawa i przyczynienie się do wymiany najlepszych praktyk poprzez współpracę z organami zaangażowanymi w piaskownicę regulacyjną w zakresie sztucznej inteligencji w celu zapewnienia w przyszłości zgodności z niniejszym rozporządzeniem oraz, w stosownych przypadkach, z innymi przepisami Unii i państw członkowskich;
d) wniesienie wkładu w oparte na dowodach uczenie się działań regulacyjnych.

2. [skreśla się]

2a. Dostęp do piaskownic regulacyjnych w zakresie sztucznej inteligencji jest otwarty dla każdego dostawcy lub potencjalnego dostawcy systemu sztucznej inteligencji spełniającego kryteria kwalifikowalności i wyboru, o których mowa w ust. 6 lit. a), wybranego przez właściwe organy krajowe w wyniku procedury wyboru, o której mowa w ust. 6 lit. b). Dostawcy lub potencjalni dostawcy mogą również składać wnioski we współpracy z użytkownikami lub wszelkimi innymi odpowiednimi osobami trzecimi.

Uczestnictwo w piaskownicy regulacyjnej w zakresie sztucznej inteligencji jest ograniczone do okresu, który odpowiada złożoności i skali projektu. Okres ten może zostać przedłużony przez właściwy organ krajowy.

Uczestnictwo w piaskownicy regulacyjnej w zakresie sztucznej inteligencji opiera się na szczegółowym planie, o którym mowa w ust. 6 niniejszego artykułu, uzgadnianym między uczestnikiem (uczestnikami) i właściwym organem krajowym (właściwymi organami krajowymi), stosownie do przypadku.

3. Uczestnictwo w piaskownicach regulacyjnych w zakresie sztucznej inteligencji pozostaje bez wpływu na uprawnienia w zakresie nadzoru i stosowania środków naprawczych przynależne organom nadzorującym te piaskownice. Organy te wykonują swoje uprawnienia nadzorcze w sposób elastyczny w granicach określonych w odpowiednich przepisach, wykorzystując swoje uprawnienia dyskrecjonalne przy stosowaniu przepisów prawnych do konkretnego projektu piaskownicy w zakresie sztucznej inteligencji, w celu wspierania innowacji w dziedzinie sztucznej inteligencji w Unii.

O ile uczestnik lub uczestnicy przestrzegają planu opracowanego dla danej piaskownicy oraz warunków ich uczestnictwa, o których mowa w ust. 6 lit. c), oraz stosują się w dobrej wierze do wytycznych wydawanych przez organy, organy nie nakładają administracyjnych kar pieniężnych za naruszenie przepisów Unii lub państw członkowskich mających zastosowanie do systemu sztucznej inteligencji nadzorowanego w piaskownicy, w tym przepisów niniejszego rozporządzenia.

4. Uczestnicy pozostają odpowiedzialni, na mocy mających zastosowanie przepisów Unii i przepisów państw członkowskich dotyczących odpowiedzialności, za wszelkie szkody spowodowane w trakcie ich uczestnictwa w piaskownicy regulacyjnej w zakresie sztucznej inteligencji.

PUBLIC

4a. Na wniosek dostawcy lub potencjalnego dostawcy systemu sztucznej inteligencji właściwy organ krajowy przygotowuje, w stosownych przypadkach, pisemny dowód działań przeprowadzonych z powodzeniem w ramach piaskownicy. Właściwy organ krajowy przygotowuje również sprawozdanie na wyjście zawierające szczegółowe informacje na temat działań przeprowadzonych w ramach piaskownicy oraz powiązanych wyników i efektów uczenia się. Taki pisemny dowód oraz sprawozdanie na wyjście mogą być uwzględniane przez organy nadzoru rynku lub jednostki notyfikowane, stosownie do przypadku, w kontekście procedur oceny zgodności lub kontroli w ramach nadzoru rynku.

Z zastrzeżeniem przepisów dotyczących poufności określonych w art. 70 i za zgodą uczestników piaskownicy Komisja Europejska i Rada ds. Sztucznej Inteligencji są upoważnione, by uzyskać dostęp do sprawozdań na wyjście i w stosownych przypadkach uwzględniają je przy wykonywaniu swoich zadań na mocy niniejszego rozporządzenia. Jeżeli zarówno uczestnik, jak i właściwy organ krajowy wyraźnie wyrażą na to zgodę, sprawozdanie na wyjście może zostać podane do wiadomości publicznej za pośrednictwem jednolitej platformy informacyjnej, o której mowa w art. 55 ust. 3 lit. b).

4b. Piaskownice regulacyjne w zakresie sztucznej inteligencji opracowuje się i wdraża w taki sposób, by w stosownych przypadkach ułatwiały współpracę transgraniczną między właściwymi organami krajowymi.

5. Właściwe organy krajowe podają do wiadomości publicznej dostępne sprawozdania roczne z wdrażania piaskownic regulacyjnych w zakresie sztucznej inteligencji, obejmujące dobre praktyki, wyciągnięte wnioski, zalecenia dotyczące tworzenia piaskownic regulacyjnych i – w stosownych przypadkach – zalecenia dotyczące objętego nadzorem w ramach piaskownicy stosowania niniejszego rozporządzenia i innych przepisów Unii. Te sprawozdania roczne przedkłada się Radzie ds. Sztucznej Inteligencji, która podaje do wiadomości publicznej podsumowanie wszystkich dobrych praktyk, wyciągniętych wniosków i zaleceń. Obowiązek publicznego udostępniania sprawozdań rocznych nie obejmuje szczególnie chronionych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych. Komisja i Rada ds. Sztucznej Inteligencji w stosownych przypadkach uwzględniają sprawozdania roczne przy wykonywaniu swoich zadań na podstawie niniejszego rozporządzenia.

5b. Komisja zapewnia, aby informacje o piaskownicach regulacyjnych w zakresie sztucznej inteligencji, w tym o piaskownicach ustanowionych na mocy niniejszego artykułu, były dostępne za pośrednictwem jednolitej platformy informacyjnej, o której mowa w art. 55 ust. 3 lit. b).

6. Zasady i warunki ustanawiania i prowadzenia piaskownic regulacyjnych w zakresie sztucznej inteligencji na podstawie niniejszego rozporządzenia przyjmuje się w drodze aktów wykonawczych zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Te zasady i warunki w możliwie największym stopniu wspierają elastyczność właściwych organów krajowych w zakresie ustanawiania i prowadzenia piaskownic regulacyjnych w zakresie sztucznej inteligencji, sprzyjają innowacjom i uczeniu się działań regulacyjnych, a w szczególności uwzględniają szczególne uwarunkowania i zdolności uczestniczących MŚP, w tym przedsiębiorstw typu start-up.

Przedmiotowe akty wykonawcze określają wspólne główne zasady dotyczące następujących kwestii:

a) kwalifikowalności i wyboru do udziału w piaskownicy regulacyjnej w zakresie sztucznej inteligencji;
b) procedury składania wniosków, uczestnictwa, monitorowania, wychodzenia z piaskownicy regulacyjnej w zakresie sztucznej inteligencji i jej zakończenia, w tym planu opracowywanego dla piaskownicy i sprawozdania na wyjście;
c) warunków mających zastosowanie do uczestników.

7. Jeżeli właściwe organy krajowe rozważają udzielenie zezwolenia na przeprowadzenie testów w warunkach rzeczywistych nadzorowanych w ramach piaskownicy w zakresie sztucznej inteligencji ustanowionej 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 54

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

1. W piaskownicy regulacyjnej w zakresie sztucznej inteligencji dane osobowe zgromadzone zgodnie z prawem w innych celach można przetwarzać na potrzeby opracowywania, testowania i trenowania innowacyjnych systemów sztucznej inteligencji w ramach piaskownicy na następujących łącznych warunkach:

   a) innowacyjne systemy sztucznej inteligencji opracowuje się w celu zapewnienia ochrony ważnego interesu publicznego – przez organ publiczny lub inną osobę fizyczną lub prawną podlegającą prawu publicznemu lub prawu prywatnemu – w co najmniej jednym z poniższych obszarów:

      (i) [skreśla się]

      (ii) bezpieczeństwo i zdrowie publiczne, w tym profilaktyka, kontrola i leczenie chorób oraz poprawa systemów opieki zdrowotnej;

      (iii) ochrona i poprawa jakości środowiska, w tym transformacja ekologiczna, łagodzenie zmiany klimatu i przystosowywanie się do niej;

      (iv) zrównoważoność energetyczna, transport i mobilność;

      (v) wydajność i jakość administracji publicznej i usług publicznych;

      (vi) cyberbezpieczeństwo i odporność infrastruktury krytycznej.

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

c) ustanowiono skuteczne mechanizmy monitorowania pozwalające zidentyfikować wszelkie poważne zagrożenia dla praw i wolności osób, których dane dotyczą, określone w art. 35 rozporządzenia (UE) 2016/679 i art. 39 rozporządzenia (UE) 2018/1725, jakie mogą wystąpić w trakcie przeprowadzania eksperymentów w ramach piaskownicy, a także mechanizm reagowania zapewniający możliwość szybkiego zaradzenia tym zagrożeniom oraz – w stosownych przypadkach – wstrzymania przetwarzania;

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

e) wszelkie przetwarzane dane osobowe nie mogą być przenoszone, przekazywane ani w żaden inny sposób udostępniane osobom trzecim, które nie są uczestnikami piaskownicy, chyba że takie ujawnienie odbywa się zgodnie z rozporządzeniem (UE) 2016/679 lub, w stosownych przypadkach, z rozporządzeniem 2018/725, i wszyscy uczestnicy wyrazili na nie zgodę;

f) wszelkie przetwarzanie danych osobowych w kontekście piaskownicy nie wpływa na stosowanie praw osób, których dane dotyczą, przewidzianych w prawie Unii dotyczącym ochrony danych osobowych, w szczególności w art. 22 rozporządzenia (UE) 2016/679 i art. 24 rozporządzenia (UE) 2018/1725;

g) wszelkie dane osobowe przetwarzane w kontekście piaskownicy chroni się za pomocą odpowiednich środków technicznych i organizacyjnych oraz usuwa się po zakończeniu uczestnictwa w piaskownicy lub po upływie okresu przechowywania danych osobowych;

h) logi ewidencjonujące przetwarzanie danych osobowych w kontekście piaskownicy przechowuje się przez cały czas uczestnictwa w piaskownicy, chyba że prawo Unii lub prawo krajowe stanowią inaczej;

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

j) krótkie podsumowanie projektu w zakresie sztucznej inteligencji opracowanego w ramach piaskownicy, jego celów i oczekiwanych rezultatów opublikowano na stronie internetowej właściwych organów. Obowiązek ten nie obejmuje szczególnie chronionych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych.

1a. Do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania przestępstw lub egzekwowania sankcji karnych, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom pod nadzorem organów ścigania i na ich odpowiedzialność, przetwarzanie danych osobowych w piaskownicach regulacyjnych w zakresie sztucznej inteligencji prowadzone jest w oparciu o konkretne przepisy państw członkowskich lub przepisy Unii i podlega tym samym łącznym warunkom, o których mowa w ust. 1.

2. Ust. 1 pozostaje bez uszczerbku dla przepisów prawa Unii lub państw członkowskich określających podstawy przetwarzania danych osobowych niezbędnego do celów opracowywania, testowania i trenowania innowacyjnych systemów sztucznej inteligencji lub dla jakiejkolwiek innej podstawy prawnej, zgodnie z prawem Unii dotyczącym ochrony danych osobowych.

Artykuł 54a

Testy systemów sztucznej inteligencji wysokiego ryzyka w warunkach rzeczywistych poza piaskownicami regulacyjnymi w zakresie sztucznej inteligencji

1. Testy systemów sztucznej inteligencji w warunkach rzeczywistych prowadzone poza piaskownicami regulacyjnymi w zakresie sztucznej inteligencji mogą być przeprowadzane przed dostawców lub potencjalnych dostawców systemów sztucznej inteligencji wysokiego ryzyka, wymienionych w załączniku III, zgodnie z przepisami niniejszego artykułu i planem testów w warunkach rzeczywistych, o którym mowa w niniejszym artykule.

Szczegółowe elementy planu testów w warunkach rzeczywistych określa się w aktach wykonawczych przyjmowanych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 74 ust. 2.

Przepis ten pozostaje bez uszczerbku dla przepisów Unii lub przepisów państw członkowskich dotyczących testów w warunkach rzeczywistych systemów sztucznej inteligencji wysokiego ryzyka związanych z produktami objętymi prawodawstwem wymienionym w załączniku II.

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

3. Testy w warunkach rzeczywistych systemów sztucznej inteligencji wysokiego ryzyka na podstawie niniejszego artykułu pozostają bez uszczerbku dla oceny etycznej, która może być wymagana na mocy prawa krajowego lub prawa Unii.

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 lub państwach członkowskich, w których mają być przeprowadzane te testy;

b) organ nadzoru rynku w państwie członkowskim lub państwach członkowskich, w których mają być przeprowadzone testy w warunkach rzeczywistych, nie zgłosił sprzeciwu wobec tych testów w ciągu 30 dni od przedłożenia planu testów;

c) dostawca lub potencjalny dostawca – z wyjątkiem dostawców systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7 w obszarach egzekwowania prawa, zarządzania migracją, azylem i kontrolą graniczną, oraz systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 2 – zarejestrował testy w warunkach rzeczywistych w unijnej bazie danych, o której mowa w art. 60 ust. 5a, pod ogólnounijnym niepowtarzalnym numerem identyfikacyjnym, podając informacje określone w załączniku VIIIa;

d) dostawca lub potencjalny dostawca przeprowadzający testy w warunkach rzeczywistych ma siedzibę w Unii lub wyznaczył przedstawiciela prawnego do celów przeprowadzania testów w warunkach rzeczywistych, który ma siedzibę w Unii;

e) dane gromadzone i przetwarzane do celów testów w warunkach rzeczywistych nie są przekazywane do państw spoza Unii, chyba że w ramach tego przekazywania i przetwarzania zapewnione są zabezpieczenia równoważne zabezpieczeniom przewidzianym w prawie Unii;

f) testy w warunkach rzeczywistych nie trwają dłużej niż jest to konieczne do osiągnięcia ich celów, a w żadnym razie nie dłużej niż 12 miesięcy;

g) osoby należące do słabszych grup społecznych ze względu na wiek, niepełnosprawność fizyczną lub umysłową są odpowiednio chronione;

h) [skreśla się]

i) w przypadku gdy dostawca lub potencjalny dostawca organizuje testy w warunkach rzeczywistych we współpracy z co najmniej jednym potencjalnym użytkownikiem, ten ostatni został poinformowany o wszystkich aspektach testów, które są istotne dla jego decyzji o uczestnictwie, oraz otrzymał odpowiednie instrukcje dotyczące sposobu korzystania z systemu sztucznej inteligencji, o których mowa w art. 13; dostawca lub przyszły dostawca oraz użytkownik lub użytkownicy zawierają umowę określającą ich role i obowiązki w celu zapewnienia zgodności z przepisami dotyczącymi testów w warunkach rzeczywistych na mocy niniejszego rozporządzenia i z innymi mającymi zastosowanie przepisami Unii i przepisami państw członkowskich;

j) podmioty testów w warunkach rzeczywistych wyraziły świadomą zgodę zgodnie z art. 54b lub – w przypadku organów ścigania – gdy uzyskanie świadomej zgody uniemożliwiłoby testy systemu sztucznej inteligencji, same testy w warunkach rzeczywistych oraz ich wynik nie mogą mieć negatywnego wpływu na podmiot testów;

k) testy w warunkach rzeczywistych są skutecznie nadzorowane przez dostawcę lub potencjalnego dostawcę i użytkownika (użytkowników) przy udziale osób posiadających odpowiednie kwalifikacje w danej dziedzinie oraz zdolności, przygotowanie szkoleniowe i uprawnienia niezbędne do wykonywania ich zadań;

l) przewidywania, zalecenia lub decyzje systemu sztucznej inteligencji można skutecznie odwrócić lub zignorować.

PUBLIC

5. Każdy podmiot testów w warunkach rzeczywistych, lub, w stosownych przypadkach, jego wyznaczony zgodnie z prawem przedstawiciel może – bez konsekwencji dla tego podmiotu i bez konieczności przedstawiania jakiegokolwiek uzasadnienia – wycofać się z testów w dowolnym momencie poprzez odwołanie swojej świadomej zgody. Wycofanie świadomej zgody nie ma wpływu na działania już przeprowadzone ani na wykorzystanie danych uzyskanych na podstawie świadomej zgody przed jej wycofaniem.

6. Każdy poważny incydent stwierdzony w trakcie testów w warunkach rzeczywistych zgłasza się krajowemu organowi nadzoru rynku zgodnie z art. 62 niniejszego rozporządzenia. Dostawca lub potencjalny dostawca przyjmuje natychmiastowe środki zaradcze lub, w przypadku gdy jest to niemożliwe, zawiesza testy w warunkach rzeczywistych do czasu zaradzenia incydentowi lub kończy testy w inny sposób. Dostawca lub potencjalny dostawca ustanawia procedurę niezwłocznego wycofania systemu sztucznej inteligencji od użytkowników po takim zakończeniu testów w warunkach rzeczywistych.

7. Dostawcy lub potencjalni dostawcy powiadamiają krajowy organ nadzoru rynku w państwie członkowskim lub państwach członkowskich, w których miały być prowadzone testy w warunkach rzeczywistych, o zawieszeniu lub zakończeniu tych testów i o ostatecznych wynikach.

8. Dostawcy lub potencjalni dostawcy są odpowiedzialni, na mocy mających zastosowanie przepisów Unii i przepisów państw członkowskich dotyczących odpowiedzialności, za wszelkie szkody spowodowane w trakcie ich uczestnictwa w testach w warunkach rzeczywistych.

Artykuł 54b

Świadoma zgoda na uczestnictwo w testach w warunkach rzeczywistych poza piaskownicami regulacyjnymi w zakresie sztucznej inteligencji

1. Do celów testów w warunkach rzeczywistych prowadzonych na podstawie art. 54a wydana zostać musi przez podmiot testów dobrowolna świadoma zgoda – przed jego udziałem w takich testach i po należytym poinformowaniu go w sposób zwięzły, jasny, adekwatny i zrozumiały o:

(i) charakterze i celach testów w warunkach rzeczywistych oraz ewentualnych niedogodnościach, które mogą być związane z udziałem w tych testach;

(ii) warunkach na jakich mają być prowadzone testy w warunkach rzeczywistych, w tym o przewidywanym czasie trwania uczestnictwa w testach;

(iii) prawach podmiotu testów i gwarancjach dotyczących udziału w testach, w szczególności o prawie do odmowy udziału w testach oraz o prawie do wycofania się z testów w warunkach rzeczywistych – w dowolnym momencie bez konsekwencji dla podmiotu testów i bez konieczności przedstawiania jakiegokolwiek uzasadnienia;

(iv) sposobach zwracania się o odwrócenie lub zignorowanie przewidywań, zaleceń lub decyzji wydanych przez system sztucznej inteligencji;

(v) ogólnounijnym niepowtarzalnym numerze identyfikacyjnym testów w warunkach rzeczywistych nadanym zgodnie z art. 54a ust. 4c i o danych kontaktowych dostawcy lub jego przedstawiciela prawnego, od których można uzyskać dalsze informacje.

2. Świadoma zgoda jest opatrzona datą i udokumentowana, a pomiot testów lub jego przedstawiciel prawny otrzymują jej kopię.

Artykuł 55

Środki wsparcia dla operatorów, w szczególności MŚP, w tym przedsiębiorstw typu start-up

1. Państwa członkowskie podejmują następujące działania:

a) zapewniają MŚP, w tym przedsiębiorstwom typu start-up, dostęp do piaskownic regulacyjnych w zakresie sztucznej inteligencji na zasadzie pierwszeństwa, o ile spełniają oni kryteria kwalifikowalności i wyboru;

b) organizują specjalne wydarzenia informacyjne i szkoleniowe poświęcone stosowaniu przepisów niniejszego rozporządzenia dostosowane do potrzeb MŚP, w tym przedsiębiorstw typu start-up, i w stosownych przypadkach lokalnych organów publicznych;

c) w stosownych przypadkach ustanawiają specjalny kanał komunikacji z MŚP, w tym przedsiębiorstwami typu start-up, i, stosownie do sytuacji, z lokalnymi organami publicznymi – w celu zapewnienia poradnictwa i udzielania odpowiedzi na zapytania dotyczące wdrażania niniejszego rozporządzenia, w tym w zakresie udziału w piaskownicach regulacyjnych w zakresie sztucznej inteligencji.

2. Przy ustalaniu wysokości opłat z tytułu oceny zgodności przeprowadzanej zgodnie z art. 43 bierze się pod uwagę szczególne interesy i potrzeby MŚP, w tym przedsiębiorstw typu start-up, obniżając te opłaty proporcjonalnie do wielkości tych przedsiębiorstw, wielkości rynku i innych odpowiednich wskaźników.

3. Komisja podejmuje następujące działania:

a) na wniosek Rady ds. Sztucznej Inteligencji zapewnia ustandaryzowane wzorce dokumentacji dla obszarów objętych niniejszym rozporządzeniem;

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 sztucznej inteligencji.

Artykuł 55a

Odstępstwa w sytuacjach szczególnych

1. Obowiązki określone w art. 17 niniejszego rozporządzenia nie mają zastosowania do mikroprzedsiębiorstw zdefiniowanych w art. 2 ust. 3 załącznika do zalecenia Komisji 2003/361/WE dotyczącego definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, o ile przedsiębiorstwa te nie mają przedsiębiorstw partnerskich ani przedsiębiorstw powiązanych zdefiniowanych w art. 3 wspomnianego załącznika.

2. Ustępu 1 nie należy interpretować jako zwalniającego tych operatorów z wszelkich innych wymogów i obowiązków określonych w niniejszym rozporządzeniu, w tym tych ustanowionych w art. 9, 61 i 62.

3. Wymogi i obowiązki dotyczące systemów sztucznej inteligencji ogólnego przeznaczenia określone w art. 4b nie mają zastosowania do mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, pod warunkiem że przedsiębiorstwa te nie mają przedsiębiorstw partnerskich ani przedsiębiorstw powiązanych zdefiniowanych w art. 3 załącznika do zalecenia Komisji 2003/361/WE dotyczącego definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

PUBLIC

TYTUŁ VI

ZARZĄDZANIE

ROZDZIAŁ 1

EUROPEJSKA RADA DS. SZTUCZNEJ INTELIGENCJI

Artykuł 56

Ustanowienie i struktura Europejskiej Rady ds. Sztucznej Inteligencji

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

2. W skład Rady wchodzi po jednym przedstawicielu z każdego państwa członkowskiego. Europejski Inspektor Ochrony Danych uczestniczy w charakterze obserwatora.
W posiedzeniach Rady ds. Sztucznej Inteligencji uczestniczy również Komisja bez prawa głosu.

   Do udziału w posiedzeniach Rada może zapraszać w poszczególnych przypadkach inne krajowe i unijne organy, jednostki organizacyjne lub ekspertów, w przypadku gdy omawiane kwestie są dla nich istotne.

2a. Każdy przedstawiciel jest wyznaczany przez swoje państwo członkowskie na okres trzech lat, z możliwością jednokrotnego przedłużenia.

2aa. Państwa członkowskie zapewniają, by ich przedstawiciele w Radzie:

   (i) mieli w swoim państwie członkowskim odpowiednie kompetencje i uprawnienia, tak aby aktywnie przyczyniać się do realizacji zadań Rady, o których mowa w art. 58;

   (ii) zostali wyznaczeni w charakterze pojedynczego punktu kontaktowego z Radą lub, w stosownych przypadkach, przy uwzględnieniu potrzeb państw członkowskich, jako pojedynczy punkt kontaktowy dla zainteresowanych stron;

PUBLIC

(iii) byli uprawnieni do ułatwiania zapewniania 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 – poprzez gromadzenie odpowiednich danych i informacji.

3. Wyznaczeni przedstawiciele państw członkowskich przyjmują regulamin wewnętrzny Rady większością dwóch trzecich głosów.

W regulaminie wewnętrznym ustanawia się w szczególności procedury wyboru, czas trwania mandatu i specyfikację zadań przewodniczącego, zasady głosowania oraz organizację działalności Rady i jej podgrup.

Rada ustanawia stałą podgrupę służącą jako platforma dla zainteresowanych stron w celu doradzania Radzie we wszystkich kwestiach związanych z wdrażaniem niniejszego rozporządzenia, w tym przygotowania aktów wykonawczych i delegowanych. W tym celu do udziału w tej podgrupie zaprasza się organizacje reprezentujące interesy dostawców i użytkowników systemów sztucznej inteligencji, w tym MŚP i przedsiębiorstwa typu start-up, a także organizacje społeczeństwa obywatelskiego, przedstawicieli osób, na które te systemy mogą mieć wpływ, naukowców, organizacji normalizacyjnych, jednostek notyfikowanych, laboratoriów oraz ośrodków testowo-doświadczalnych. Rada ustanawia 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.

W stosownych przypadkach Rada może również tworzyć inne stałe lub tymczasowe podgrupy na potrzeby zbadania konkretnych kwestii. W stosownych przypadkach zainteresowane strony, o których mowa w poprzednim akapicie, mogą zostać zaproszone do udziału w takich podgrupach lub na konkretne posiedzenia tych podgrup w charakterze obserwatorów.

3a. Rada jest zorganizowana i zarządzana w sposób gwarantujący niezależność, obiektywizm i bezstronność podejmowanych przez nią działań.

PUBLIC

4. Przewodniczącym Rady jest jeden z przedstawicieli państw członkowskich. Na żądanie przewodniczącego Komisja zwołuje posiedzenia i przygotowuje porządek obrad zgodnie z zadaniami Rady określonymi w niniejszym rozporządzeniu oraz z jej regulaminem wewnętrznym. Komisja udziela administracyjnego i analitycznego wsparcia na potrzeby działań Rady podejmowanych na podstawie niniejszego rozporządzenia.

Artykuł 57

[skreśla się]

Artykuł 58

Zadania Rady

Rada ds. Sztucznej Inteligencji doradza Komisji i państwom członkowskim oraz udziela im wsparcia w celu ułatwienia spójnego i skutecznego stosowania niniejszego rozporządzenia. W tym celu Rada może w szczególności:

a) gromadzić fachową wiedzę techniczną i regulacyjną oraz najlepsze praktyki i udostępniać je państwom członkowskim;

b) przyczyniać się do harmonizacji praktyk administracyjnych w państwach członkowskich, w tym w odniesieniu do odstępstwa od procedur oceny zgodności, o którym mowa w art. 47, funkcjonowania piaskownic regulacyjnych oraz testów w warunkach rzeczywistych, o których mowa w art. 53, 54 i 54a;

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

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

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

PUBLIC

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

d) doradzać Komisji w zakresie potencjalnej konieczności zmiany załącznika III zgodnie z art. 4 i 7, przy uwzględnieniu odpowiednich dostępnych dowodów i rozwoju technologii,

e) doradzać Komisji w trakcie przygotowywania aktu delegowanego lub wykonawczego zgodnie z niniejszym rozporządzeniem,

f) współpracować, w stosownych przypadkach, z odpowiednimi organami, grupami ekspertów i sieciami UE, w szczególności w dziedzinie bezpieczeństwa produktów, cyberbezpieczeństwa, konkurencyjności, usług cyfrowych i medialnych, usług finansowych, kryptowalut, ochrony konsumentów, ochrony danych oraz ochrony praw podstawowych;

g) wnosić wkład i służyć Komisji odpowiednim doradztwem przy opracowywaniu przez nią wskazówek, o których mowa w art. 58a, lub zwracać się o opracowanie takich wskazówek;

h) wspierać prace organów nadzoru rynku oraz – we współpracy z zainteresowanymi organami rynku i za ich zgodą – promować i wspierać transgraniczne postępowania wyjaśniające w zakresie nadzoru rynku, w tym w odniesieniu do nowych zagrożeń o charakterze systemowym, które mogą pojawić się w związku z systemami sztucznej inteligencji;

i) uczestniczyć w ocenie potrzeb szkoleniowych personelu państw członkowskich uczestniczącego we wdrażaniu niniejszego rozporządzenia;

j) doradzać Komisji w odniesieniu do międzynarodowych kwestii dotyczących sztucznej inteligencji.

PUBLIC

ROZDZIAŁ 1A

WYTYCZNE KOMISJI

Artykuł 58a

Wytyczne Komisji w sprawie wdrożenia niniejszego rozporządzenia

1. Na wniosek państw członkowskich lub Rady ds. Sztucznej Inteligencji – lub z własnej inicjatywy – Komisja wydaje wytyczne dotyczące praktycznego wdrażania niniejszego rozporządzenia, odnoszące się w szczególności do:

   (i) stosowania wymogów, o których mowa w art. 8–15;

   (ii) zakazanych praktyk, o których mowa w art. 5;

   (iii) praktycznego wdrażania przepisów dotyczących istotnych zmian;

   (iv) praktycznego wdrażania jednolitych warunków, o których mowa w art. 6 ust. 3, z uwzględnieniem przykładów dotyczących systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III;

   (v) praktycznego wdrażania obowiązków w zakresie przejrzystości ustanowionych w art. 52;

   (vi) zależności między niniejszym rozporządzeniem a innym odpowiednim prawodawstwem Unii, w tym w odniesieniu do spójności w ich egzekwowaniu.

Przy wydawaniu takich wytycznych Komisja zwraca szczególną uwagę na potrzeby MŚP, w tym przedsiębiorstw typu start-up, lokalnych organów publicznych i sektorów, na które niniejsze rozporządzenie będzie miało najprawdopodobniej największy wpływ.

PUBLIC

ROZDZIAŁ 2

WŁAŚCIWE ORGANY KRAJOWE

Artykuł 59

Wyznaczanie właściwych organów krajowych

1. [skreśla się]

2. 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 organizuje się w sposób gwarantujący obiektywizm i bezstronność podejmowanych przez nie działań i wykonywanych przez nie zadań. Takie działania i zadania mogą być wykonywane przez jeden lub kilka wyznaczonych organów zgodnie z potrzebami organizacyjnymi państwa członkowskiego, pod warunkiem poszanowania tych zasad.

3. Państwa członkowskie informują Komisję o ich wyznaczeniu lub wyznaczeniach.

4. Państwa członkowskie zapewniają, aby właściwe organy krajowe dysponowały odpowiednimi zasobami finansowymi, wyposażeniem technicznym oraz dobrze wykwalifikowanymi zasobami ludzkimi umożliwiającymi im efektywne wykonywanie zadań powierzonych im na podstawie niniejszego rozporządzenia.

5. Do dnia *[rok po wejściu w życie niniejszego rozporządzenia]*, a następnie sześć miesięcy przed terminem, o którym mowa w art. 84 ust. 2, państwa członkowskie poinformują Komisję o stanie zasobów finansowych, wyposażenia technicznego i zasobów ludzkich właściwych organów krajowych wraz z oceną ich adekwatności. Komisja przekazuje te informacje Radzie w celu ich omówienia i ewentualnego wydania zaleceń.

6. Komisja ułatwia wymianę doświadczeń między właściwymi organami krajowymi.

PUBLIC

7. Właściwe organy krajowe mogą zapewniać doradztwo w zakresie wdrażania niniejszego rozporządzenia, z uwzględnieniem dostosowania do potrzeb dostawców będących MŚP, w tym przedsiębiorstw typu start-up. Jeżeli właściwe organy krajowe zamierzają udzielić wytycznych i porad dotyczących systemu sztucznej inteligencji w dziedzinach objętych innymi przepisami Unii, są zobowiązane – w stosownych przypadkach – do każdorazowego zasięgnięcia opinii właściwych organów krajowych wyznaczonych na podstawie tych przepisów Unii. Państwa członkowskie mogą również utworzyć jeden centralny punkt kontaktowy na potrzeby wymiany informacji z operatorami.

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

TYTUŁ VII

UNIJNA BAZA DANYCH SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA UMIESZCZONYCH W ZAŁĄCZNIKU III

Artykuł 60

Unijna baza danych systemów sztucznej inteligencji wysokiego ryzyka umieszczonych w załączniku III

1. Komisja – we współpracy z państwami członkowskimi – tworzy i prowadzi unijną bazę danych zawierającą informacje, o których mowa w ust. 2, dotyczące odpowiednich operatorów i systemów sztucznej inteligencji wysokiego ryzyka umieszczonych w załączniku III podlegających rejestracji zgodnie z art. 51 i 54a. Przy ustalaniu funkcjonalnych specyfikacji takiej bazy danych Komisja konsultuje się z Radą ds. Sztucznej Inteligencji.

PUBLIC

2. Dane wymienione w załączniku VIII część I są wprowadzane do unijnej bazy danych UE – odpowiednio – przez dostawców, upoważnionych przedstawicieli i odpowiednich użytkowników, po ich rejestracji. Dane wymienione w załączniku VIII część II pkt 1–11 są wprowadzane do unijnej bazy danych UE przez dostawców lub – w stosownych przypadkach – przez upoważnionego przedstawiciela, zgodnie z art. 51. Dane, o których mowa w załączniku VIII część II pkt 12, są generowane automatycznie w bazie danych na podstawie informacji podanych przez odpowiednich użytkowników zgodnie z art. 51 ust. 2. Dane wymienione w załączniku VIIIa są wprowadzane do bazy danych przez potencjalnych dostawców lub dostawców zgodnie z art. 54a.

3. [skreśla się]

4. Unijna baza danych nie zawiera danych osobowych, z wyjątkiem informacji wymienionych w załączniku VIII, i pozostaje bez uszczerbku dla art. 70.

5. Komisja pełni funkcję administratora unijnej bazy danych. Zapewnia dostawcom, potencjalnym dostawcom oraz użytkownikom odpowiednie wsparcie techniczne i administracyjne.

5a. Informacje zawarte w unijnej bazie danych zarejestrowane zgodnie z art. 51 są publicznie dostępne. Informacje zarejestrowane zgodnie z art. 54a są dostępne wyłącznie dla organów nadzoru rynku i dla Komisji, chyba że potencjalny dostawca lub dostawca wyrazili zgodę na udostępnienie tych informacji również opinii publicznej.

PUBLIC

TYTUŁ VIII

MONITOROWANIE PO WPROWADZENIU DO OBROTU, WYMIANA INFORMACJI, NADZÓR RYNKU

ROZDZIAŁ 1

MONITOROWANIE PO WPROWADZENIU DO OBROTU

Artykuł 61

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

1. Dostawcy ustanawiają i dokumentują – w sposób proporcjonalny do ryzyka związanego ze stosowaniem danego systemu sztucznej inteligencji wysokiego ryzyka – system monitorowania po wprowadzeniu do obrotu.

2. W celu umożliwienia dostawcy dokonania oceny zgodności systemów sztucznej inteligencji z wymogami określonymi w tytule III rozdział 2 w całym cyklu życia tych systemów, w systemie monitorowania po wprowadzeniu do obrotu są gromadzone, dokumentowane i analizowane odnośne dane, które mogą być dostarczane przez użytkowników lub które mogą być zbierane z innych źródeł, dotyczące działania systemów sztucznej inteligencji wysokiego ryzyka. Obowiązek ten nie obejmuje szczególnie chronionych danych operacyjnych użytkowników systemów sztucznej inteligencji będących organami ścigania.

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

PUBLIC

4. W odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka objętych przepisami aktów prawnych, o których mowa w załączniku II sekcja A, w przypadku gdy zgodnie z tymi przepisami ustanowiono już system i plan monitorowania po wprowadzeniu do obrotu, dokumentację dotyczącą monitorowania po wprowadzeniu do obrotu przygotowaną na podstawie tego prawodawstwa uznaje się za wystarczającą, pod warunkiem że stosowany jest wzór, o którym mowa w ust. 3.

Akapit pierwszy ma również zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5, wprowadzonych do obrotu lub oddanych do użytku przez instytucje finansowe objęte wymogami dotyczącymi ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych.

ROZDZIAŁ 2

WYMIANA INFORMACJI NA TEMAT POWAŻNYCH INCYDENTÓW

Artykuł 62

Zgłaszanie poważnych incydentów

1. Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzonych do obrotu na rynku unijnym zgłaszają wszelkie poważne incydenty organom nadzoru rynku tego państwa członkowskiego, w którym wystąpił dany incydent.

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

2. Po otrzymaniu zgłoszenia dotyczącego poważnego incydentu, o którym mowa w art. 3 ust. 44 lit. c), odpowiedni organ nadzoru rynku informuje o tym fakcie krajowe organy publiczne lub organy, o których mowa w art. 64 ust. 3. Komisja opracowuje specjalne wytyczne ułatwiające zapewnienie zgodności z obowiązkami określonymi w ust. 1. Wytyczne wydaje się najpóźniej w terminie 12 miesięcy od dnia wejścia niniejszego rozporządzenia w życie.

3. W przypadku systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 5, wprowadzanych do obrotu lub oddawanych do użytku przez dostawców będących instytucjami finansowymi objętymi wymogami dotyczącymi ich systemu zarządzania wewnętrznego, uzgodnień lub procedur na podstawie unijnych przepisów dotyczących usług finansowych, zgłaszanie poważnych incydentów ogranicza się do incydentów, o których mowa w art. 3 ust. 44 lit. c).

4. W przypadku systemów sztucznej inteligencji wysokiego ryzyka będących związanymi z bezpieczeństwem elementami wyrobów podlegających przepisom rozporządzenia (UE) 2017/745 i rozporządzenia (UE) 2017/746 lub które same są takimi wyrobami, zgłaszanie poważnych incydentów ogranicza się do incydentów, o których mowa w art. 3 ust. 44 lit, c), i jest dokonywane do właściwego organu krajowego wybranego do tego celu przez państwo członkowskie, w którym wystąpił dany incydent.

ROZDZIAŁ 3

EGZEKWOWANIE PRZEPISÓW

Artykuł 63

Nadzór rynku i kontrola systemów sztucznej inteligencji na rynku Unii

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

   a) wszelkie odniesienia do podmiotu gospodarczego w rozporządzeniu (UE) 2019/1020 rozumie się jako obejmujące wszystkich operatorów zidentyfikowanych w art. 2 niniejszego rozporządzenia;

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

2. W ramach ich obowiązków dotyczących informowania na podstawie art. 34 ust. 4 rozporządzenia (UE) 2019/1020 organy nadzoru rynku informują Komisję o rezultatach odpowiednich działań z zakresu nadzoru rynku na podstawie niniejszego rozporządzenia.

3. W przypadku systemów sztucznej inteligencji wysokiego ryzyka powiązanych z produktami, do których zastosowanie mają przepisy aktów prawnych wymienionych w załączniku II sekcja A, za organ nadzoru rynku do celów niniejszego rozporządzenia uznaje się organ odpowiedzialny za podejmowanie działań w zakresie nadzoru rynku wyznaczony na podstawie tych aktów prawnych, lub – w uzasadnionych okolicznościach i pod warunkiem zapewnienia koordynacji – inny odpowiedni organ wskazany przez dane państwo członkowskie.

   Procedury, o których mowa w art. 65, 66, 67 i 68 niniejszego rozporządzenia, nie mają zastosowania do systemów sztucznej inteligencji związanych z produktami, do których mają zastosowanie akty prawne wymienione w załączniku II sekcja A, jeżeli te akty prawne przewidują już procedury o takim samym celu. W takim przypadku zastosowanie mają te procedury sektorowe.

4. W przypadku systemów sztucznej inteligencji wysokiego ryzyka wprowadzanych do obrotu, oddawanych do użytku lub wykorzystywanych przez instytucje finansowe podlegające unijnym przepisomi dotyczącym usług finansowych organem nadzoru rynku do celów niniejszego rozporządzenia jest odpowiedni organ krajowy odpowiedzialny na mocy tego prawodawstwa za nadzór finansowy nad tymi instytucjami, w zakresie, w jakim wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie danego systemu sztucznej inteligencji jest bezpośrednio związane ze świadczeniem tych usług finansowych.

   W drodze odstępstwa od poprzedniego akapitu w uzasadnionych okolicznościach i pod warunkiem zapewnienia koordynacji państwo członkowskie może do celów niniejszego rozporządzenia wskazać inny odpowiedni organ jako organ nadzoru rynku.

   Krajowe organy nadzoru rynku nadzorujące instytucje kredytowe uregulowane na podstawie dyrektywy 2013/36/UE, które to organy uczestniczą w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem Rady nr 1024/2013, powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zidentyfikowane w trakcie prowadzonych przez nie działań z zakresu nadzoru rynku, które potencjalnie mogą mieć znaczenie dla Europejskiego Banku Centralnego z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego.

5. W odniesieniu do wymienionych w ust. 1 lit. a) systemów sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim systemy te są wykorzystywane do celów egzekwowania prawa, zgodnie z pkt 6, 7 i 8 załącznika III, państwa członkowskie wyznaczają jako organy nadzoru rynku do celów niniejszego rozporządzenia albo krajowe organy nadzorujące działania organów ścigania, organów kontroli granicznej, organów imigracyjnych, organów odpowiedzialnych za udzielanie azylu lub organów wymiaru sprawiedliwości albo właściwe organy nadzorcze ds. ochrony danych na podstawie dyrektywy (UE) 2016/680 lub rozporządzenia 2016/679. Działania w zakresie nadzoru rynku nie mogą w żaden sposób wpływać na niezależność organów wymiaru sprawiedliwości, ani w żaden inny sposób zakłócać ich działań w ramach sprawowania przez nie wymiaru sprawiedliwości.

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

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

8. Bez uszczerbku dla uprawnień przewidzianych na podstawie rozporządzenia (UE) 2019/1020 oraz w stosownych przypadkach i w zakresie ograniczonym do tego, co jest niezbędne do wykonywania ich zadań, dostawca zapewnia organom nadzoru rynku pełny dostęp do dokumentacji, a także do zbiorów danych treningowych, walidacyjnych i testowych wykorzystywanych do tworzenia systemu sztucznej inteligencji 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.

9. Organom nadzoru rynku udziela się dostępu do kodu źródłowego systemu sztucznej inteligencji wysokiego ryzyka na ich uzasadniony wniosek i wyłącznie wtedy, gdy spełnione są łącznie następujące warunki:

a) dostęp do kodu źródłowego jest niezbędny do oceny zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w tytule III rozdział 2; oraz

b) zostały wyczerpane lub okazały się niewystarczające procedury testowania/audytu i weryfikacji w oparciu o dane i dokumentację dostarczone przez dostawcę.

10. Wszelkie informacje i dokumenty uzyskane na podstawie niniejszego artykułu przez organy nadzoru rynku traktuje się zgodnie z obowiązkami dotyczącymi poufności określonymi w art. 70.

11. Skargi do właściwego organu nadzoru rynku mogą być wnoszone przez każdą osobę fizyczną lub prawną, która ma podstawy, by sądzić, że doszło do naruszenia przepisów niniejszego rozporządzenia.

Zgodnie z art. 11 ust. 3 lit. e) i art. 11 ust. 7 lit. a) rozporządzenia (UE) 2019/1020 skargi uwzględnia się do celów prowadzenia działań w zakresie nadzoru rynku i rozpatruje zgodnie ze specjalnymi procedurami ustanowionymi w związku z tym przez organy nadzoru rynku.

Artykuł 63a

Nadzór organów nadzoru rynku nad testami w warunkach rzeczywistych

1. Organy nadzoru rynku mają kompetencje i uprawnienia do zapewnienia, by testy w warunkach rzeczywistych odbywały się zgodnie z niniejszym rozporządzeniem.

2. W przypadku testów w warunkach rzeczywistych prowadzonych na systemach sztucznej inteligencji nadzorowanych w ramach piaskownicy regulacyjnej w zakresie sztucznej inteligencji na podstawie art. 54 organy nadzoru rynku weryfikują zgodność z przepisami art. 54a w ramach swojej roli nadzorczej w odniesieniu do piaskownicy regulacyjnej w zakresie sztucznej inteligencji. Na zasadzie odstępstwa od warunków określonych w art. 54a ust. 4 lit. f) i g) organy te mogą, w stosownych przypadkach, zezwolić na prowadzenie przez dostawcę lub potencjalnego dostawcę testów w warunkach rzeczywistych.

PUBLIC

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 spełnione warunki określone w art. 54a i 54b, może na swoim terytorium podjąć w stosownych przypadkach którąkolwiek z następujących decyzji:

a) zawiesić lub zakończyć testy w warunkach rzeczywistych;

b) zobowiązać dostawcę lub potencjalnego dostawcę i użytkownika (użytkowników) do zmiany któregokolwiek aspektu testów w warunkach rzeczywistych.

4. W przypadku gdy organ nadzoru rynku podjął decyzję, o której mowa w ust. 3 niniejszego artykułu, lub zgłosił sprzeciw w rozumieniu art. 54a ust. 4 lit. b), w decyzji lub sprzeciwie podaje się ich uzasadnienie oraz sposoby i warunki, na jakich dostawca lub potencjalny dostawca mogą zaskarżyć tę decyzję lub sprzeciw.

5. Tam, gdzie ma to zastosowanie, w przypadku gdy organ nadzoru rynku podjął decyzję, o której mowa w ust. 3 niniejszego artykułu, informuje o powodach takiej decyzji organy nadzoru rynku pozostałych państw członkowskich, w których dany system sztucznej inteligencji był testowany zgodnie z planem testów.

Artykuł 64

Uprawnienia organów ochrony praw podstawowych

1. [skreśla się]

2. [skreśla się]

PUBLIC

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

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

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

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

PUBLIC

Artykuł 65

Procedura postępowania na szczeblu krajowym z systemami sztucznej inteligencji stwarzającymi ryzyko

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

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

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

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

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

PUBLIC

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

5. W przypadku niepodjęcia przez operatora systemu sztucznej inteligencji odpowiednich działań naprawczych w terminie, o którym mowa w ust. 2, organ nadzoru rynku wprowadza wszelkie odpowiednie środki tymczasowe w celu zakazania lub ograniczenia udostępniania systemu sztucznej inteligencji na właściwym dla siebie rynku krajowym, wycofania produktu z rynku lub wycofania go od użytkowników. Organ ten niezwłocznie notyfikuje te środki Komisji i pozostałym państwom członkowskim.

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

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

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

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

c) nieprzestrzegania przepisów określonych w art. 52;

d) niezgodności systemów sztucznej inteligencji ogólnego przeznaczenia z wymogami i obowiązkami, o których mowa w art. 4a;

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

8. Jeżeli w terminie trzech miesięcy od dnia otrzymania notyfikacji, o której mowa w ust. 5, ani państwo członkowskie, ani Komisja nie zgłoszą sprzeciwu wobec środka tymczasowego przyjętego przez dane państwo członkowskie, taki środek uznaje się za uzasadniony. Pozostaje to bez uszczerbku dla praw procesowych odnośnego operatora określonych w art. 18 rozporządzenia (UE) 2019/1020. Okres, o którym mowa w zdaniu pierwszym niniejszego ustępu, skraca się do 30 dni w przypadku nieprzestrzegania zakazu praktyk w zakresie sztucznej inteligencji, o których mowa w art. 5.

9. Organy nadzoru rynku we wszystkich państwach członkowskich zapewniają następnie, by bez zbędnej zwłoki zostały wprowadzone odpowiednie środki ograniczające w odniesieniu do danego systemu sztucznej inteligencji, takie jak wycofanie produktu z ich rynku.

PUBLIC

Artykuł 66

Unijna procedura ochronna

1. W przypadku gdy w terminie trzech miesięcy od dnia otrzymania powiadomienia, o którym mowa w art. 65 ust. 5, lub 30 dni w przypadku nieprzestrzegania zakazu praktyk w zakresie sztucznej inteligencji, o których mowa w art. 5, państwo członkowskie zgłosi sprzeciw wobec środka wprowadzonego przez inne państwo członkowskie lub jeżeli Komisja uzna taki środek za sprzeczny z prawem Unii, Komisja niezwłocznie przystępuje do konsultacji z organem nadzoru rynku odpowiedniego państwa członkowskiego i operatorem lub operatorami i poddaje taki środek krajowy ocenie. Na podstawie wyników tej oceny Komisja – w terminie 9 miesięcy lub 60 dni w przypadku nieprzestrzegania zakazu praktyk sztucznej inteligencji, o których mowa w art. 5, licząc od notyfikacji, o której mowa w art. 65 ust. 5 – rozstrzyga, czy środek krajowy jest uzasadniony. O swojej decyzji powiadamia zainteresowane państwo członkowskie. Komisja informuje o takiej decyzji również pozostałe państwa członkowskie.

2. Jeżeli Komisja uzna środek wprowadzony przez odpowiedni organ nadzoru rynku danego państwa członkowskiego za uzasadniony, organy nadzoru rynku wszystkich państw członkowskich zapewniają wprowadzenie w odniesieniu do danego systemu sztucznej inteligencji odpowiednich środków ograniczających, takich jak wycofanie bez zbędnej zwłoki danego systemu sztucznej inteligencji z ich rynku, oraz informują odpowiednio Komisję. Jeżeli Komisja uzna środek krajowy za nieuzasadniony, organ nadzoru rynku zainteresowanego państwa członkowskiego wycofuje dany środek oraz informuje odpowiednio Komisję.

3. W przypadku uznania krajowego środka za uzasadniony i stwierdzenia, że niezgodność systemu sztucznej inteligencji wynika z braków w normach zharmonizowanych lub wspólnych specyfikacjach, o których mowa w art. 40 i 41 niniejszego rozporządzenia, Komisja stosuje procedurę przewidzianą w art. 11 rozporządzenia (UE) nr 1025/2012.

PUBLIC

Artykuł 67

Spełniające wymogi systemy sztucznej inteligencji wysokiego ryzyka lub systemy sztucznej inteligencji ogólnego przeznaczenia, które stwarzają ryzyko

1. Jeżeli po przeprowadzeniu oceny zgodnie z art. 65 organ nadzoru rynku państwa członkowskiego stwierdzi, że chociaż system sztucznej inteligencji wysokiego ryzyka lub system sztucznej inteligencji ogólnego przeznaczenia jest zgodny z niniejszym rozporządzeniem, stwarza on ryzyko dla zdrowia lub bezpieczeństwa osób lub dla praw podstawowych, organ ten zobowiązuje właściwego operatora do wprowadzenia wszelkich odpowiednich środków w celu zapewnienia, aby odnośny system sztucznej inteligencji po wprowadzeniu do obrotu lub oddaniu do użytku nie stwarzał już takiego ryzyka, do wycofania systemu sztucznej inteligencji z rynku lub do wycofania go od użytkowników bez zbędnej zwłoki w wyznaczonym przez ten organ terminie.

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

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

4. Komisja bez zbędnej zwłoki przystępuje do konsultacji z zainteresowanymi państwami członkowskimi i właściwym operatorem i poddaje ocenie wprowadzone środki krajowe. Na podstawie wyników tej oceny Komisja podejmuje decyzję, czy środek krajowy jest uzasadniony, czy nie, i w razie potrzeby proponuje odpowiednie środki.

5. Komisja kieruje swoją decyzję do zainteresowanego państwa członkowskiego oraz informuje wszystkie pozostałe państwa członkowskie.

PUBLIC

Artykuł 68

Niezgodność pod względem formalnym

1. Organ nadzoru rynku państwa członkowskiego wymaga od właściwego dostawcy usunięcia, w terminie który może nakazać, niezgodności, jeżeli ustali, że nastąpiło jedno z poniższych:

   a) umieszczenie oznakowania zgodności z naruszeniem art. 49;

   b) nieumieszczenie oznakowania zgodności;

   c) niesporządzenie deklaracji zgodności UE;

   d) nieprawidłowe sporządzenie deklaracji zgodności UE;

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

2. W przypadku gdy niezgodność, o której mowa w ust. 1, utrzymuje się, zainteresowane państwo członkowskie wprowadza wszelkie odpowiednie środki w celu ograniczenia lub zakazania udostępniania na rynku takiego systemu sztucznej inteligencji wysokiego ryzyka lub zapewnienia, aby system wycofano od użytkowników lub by wycofano go z rynku.

Artykuł 68a

Unijne jednostki badawcze w obszarze sztucznej inteligencji

1. Komisja wyznacza co najmniej jedną unijną jednostkę badawczą w obszarze sztucznej inteligencji, na podstawie art. 21 rozporządzenia (UE) 2019/1020.

PUBLIC

2. Bez uszczerbku dla działań unijnych jednostek badawczych, o których to działaniach mowa w art. 21 ust. 6 rozporządzenia (UE) 2019/1020, unijne jednostki badawcze, o których mowa w ust. 1, zapewniają również niezależne doradztwo techniczne lub naukowe na wniosek Rady ds. Sztucznej Inteligencji lub organów nadzoru rynku.

Artykuł 68b

Centralna pula niezależnych ekspertów

1. Na wniosek Rady ds. Sztucznej Inteligencji Komisja – w drodze aktu wykonawczego – ustanawia przepisy dotyczące utworzenia, utrzymywania i finansowania centralnej puli niezależnych ekspertów w celu wsparcia działań w zakresie egzekwowania przepisów niniejszego rozporządzenia.

2. Eksperci są wybierani przez Komisję i włączani do centralnej puli na podstawie ich aktualnej wiedzy naukowej lub technicznej w dziedzinie sztucznej inteligencji, z należytym uwzględnieniem obszarów technicznych objętych wymogami i obowiązkami określonymi w niniejszym rozporządzeniu oraz działań organów nadzoru rynku zgodnie z art. 11 rozporządzenia (UE) 2019/1020. Komisja określa liczbę ekspertów w puli zgodnie istniejącymi potrzebami.

3. Eksperci mogą wykonywać następujące zadania:

a) doradzanie organom nadzoru rynku i wspieranie ich – na wniosek tych organów;

b) wspieranie transgranicznych postępowań wyjaśniających w zakresie nadzoru rynku, o których mowa w art. 58 lit. h);

c) doradzanie i wspieranie Komisji w wykonywaniu jej obowiązków w kontekście klauzuli ochronnej zgodnie z art. 66.

PUBLIC

4. Eksperci wykonują swoje zadania w sposób bezstronny i obiektywny oraz zapewniają poufność informacji i danych uzyskanych podczas wykonywania swoich zadań i działań. Każdy ekspert sporządza deklarację o braku konfliktu interesów, która jest podawana do wiadomości publicznej. Komisja ustanawia systemy i procedury mające na celu aktywne zaradzanie i zapobieganie potencjalnym konfliktom interesów.

5. Państwa członkowskie mogą być zobowiązane do uiszczania opłat za doradztwo i wsparcie ze strony ekspertów. Struktura i poziom opłat, jak również skala i struktura kosztów podlegających zwrotowi są określane przez Komisję w drodze aktu wykonawczego, o którym mowa w ust. 1, z uwzględnieniem celów odpowiedniego wdrożenia niniejszego rozporządzenia, racjonalności pod względem kosztów i konieczności zapewnienia skutecznego dostępu do ekspertów wszystkim państwom członkowskim.

6. Komisja ułatwia państwom członkowskim terminowy dostęp do ekspertów, stosownie do potrzeb, i zapewnia, by połączenie działań wspierających prowadzonych przez unijne jednostki badawcze zgodnie z art. 68a i przez ekspertów zgodnie z niniejszym artykułem było sprawnie zorganizowane i przynosiło możliwie największą wartość dodaną.

PUBLIC

TYTUŁ IX

KODEKSY POSTĘPOWANIA

Artykuł 69

Kodeksy postępowania do celów dobrowolnego stosowania szczególnych wymogów

1. Komisja i państwa członkowskie ułatwiają sporządzanie kodeksów postępowania mających zachęcać do dobrowolnego stosowania – w odniesieniu do systemów sztucznej inteligencji innych niż systemy sztucznej inteligencji wysokiego ryzyka – co najmniej jednego z wymogów określonych w tytule III rozdział 2 niniejszego rozporządzenia w możliwie największym stopniu, przy uwzględnieniu dostępnych rozwiązań technicznych umożliwiających stosowanie takich wymogów.

2. Komisja i państwa członkowskie ułatwiają sporządzanie kodeksów postępowania mających zachęcać do dobrowolnego stosowania – w odniesieniu do wszystkich systemów sztucznej inteligencji – szczególnych wymogów dotyczących na przykład zrównoważenia środowiskowego, w tym w zakresie programowania energooszczędnego, dostępności dla osób z niepełnosprawnościami, udziału zainteresowanych stron w projektowaniu i opracowywaniu systemów sztucznej inteligencji oraz różnorodności zespołów programistycznych, na podstawie jasno określonych celów i kluczowych wskaźników skuteczności działania służących do pomiaru stopnia realizacji tych celów. Komisja i państwa członkowskie ułatwiają również, w stosownych przypadkach, sporządzanie dobrowolnych kodeksów postępowania w odniesieniu do obowiązków użytkowników w powiązaniu z systemami sztucznej inteligencji.

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

4. W ramach wspierania i ułatwiania sporządzania kodeksów postępowania, o których mowa w niniejszym artykule, Komisja i państwa członkowskie uwzględniają szczególne interesy i potrzeby dostawców będących MŚP, w tym przedsiębiorstw typu start-up.

TYTUŁ X

POUFNOŚĆ I KARY

Artykuł 70

Poufność

1. Właściwe organy krajowe, jednostki notyfikowane, Komisja, Rada ds. Sztucznej Inteligencji i wszelkie inne osoby fizyczne lub prawne zaangażowane w stosowanie niniejszego rozporządzenia wprowadzają, zgodnie z prawem Unii lub prawem krajowym, odpowiednie środki techniczne i organizacyjne w celu zapewnienia poufności informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności tak, aby w szczególności:

a) chronić prawa własności intelektualnej oraz poufne informacje handlowe lub tajemnice przedsiębiorstwa osoby fizycznej lub prawnej, w tym kod źródłowy, chyba że zastosowanie mają przypadki określone w art. 5 dyrektywy (UE) 2016/943 w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem;

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

c) chronić interesy bezpieczeństwa publicznego i narodowego;

d) gwarantować uczciwy przebieg postępowań karnych i administracyjnych;

e) chronić integralność informacji niejawnych zgodnie z prawem Unii lub prawem krajowym.

PUBLIC

2. Nie naruszając przepisów ust. 1, 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 użytkownikiem, gdy z systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III pkt 1, 6 i 7, korzystają organy ścigania, organy kontroli granicznej, organy imigracyjne lub organy azylowe, jeżeli takie ujawnienie mogłoby zagrozić interesom bezpieczeństwa publicznego i narodowego. Obowiązek wymiany informacji nie obejmuje szczególnie chronionych danych operacyjnych związanych z działaniami organów ścigania, organów kontroli granicznej, organów imigracyjnych lub azylowych.

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

3. Ust. 1 i 2 pozostają bez uszczerbku dla praw i obowiązków Komisji, państw członkowskich i ich odpowiednich organów, a także jednostek notyfikowanych, w zakresie wymiany informacji i wydawania ostrzeżeń, w tym w kontekście współpracy transgranicznej, oraz obowiązków zainteresowanych stron w zakresie udzielania informacji zgodnie z prawem karnym państw członkowskich.

PUBLIC

Artykuł 71

Kary

1. Zgodnie z zasadami i warunkami określonymi w niniejszym rozporządzeniu państwa członkowskie przyjmują przepisy dotyczące kar, w tym administracyjnych kar pieniężnych, mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i podejmują wszelkie działania niezbędne do zapewnienia ich właściwego i skutecznego wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Uwzględniają one w szczególności wielkość dostawców będących MŚP, w tym przedsiębiorstw typu start-up, ich interesy oraz ich rentowność. Pod uwagę bierze się również to, czy wykorzystywanie systemu sztucznej inteligencji odbywa się w kontekście osobistej działalności pozazawodowej.

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

3. Nieprzestrzeganie jakichkolwiek zakazów dotyczących praktyk w zakresie sztucznej inteligencji określonych w art. 5 podlega administracyjnej karze pieniężnej w wysokości do 30 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 6 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. W przypadku MŚP, w tym przedsiębiorstw typu start-up, kary te wynoszą do 3 % ich rocznego światowego obrotu z poprzedniego roku obrotowego.

4. Administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, podlegają następujące naruszenia przepisów dotyczących operatorów lub jednostek notyfikowanych:

-a) obowiązki dostawców zgodnie z art. 4b i 4c;

a) obowiązki dostawców zgodnie z art. 16;

b) obowiązki innych określonych osób zgodnie z art. 23a;

c) obowiązki upoważnionych przedstawicieli zgodnie z art. 25;

d) obowiązki importerów zgodnie z art. 26;

e) obowiązki dystrybutorów zgodnie z art. 27;

f) obowiązki użytkowników zgodnie z art. 29 ust. 1–6a;

g) wymogi i obowiązki jednostek notyfikowanych zgodnie z art. 33, art. 34 ust. 1, art. 34 ust. 3, art. 34 ust. 4, art. 34a;

h) obowiązki dostawców i użytkowników w zakresie przejrzystości zgodnie z art. 52.

W przypadku MŚP, w tym przedsiębiorstw typu start-up, kary te wynoszą do 2 % ich rocznego światowego obrotu z poprzedniego roku obrotowego.

5. Przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym i właściwym organ krajowym w odpowiedzi na ich wezwanie podlega administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. W przypadku MŚP, w tym przedsiębiorstw typu start-up, kary te wynoszą do 1 % ich rocznego światowego obrotu z poprzedniego roku obrotowego.

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

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

aa) umyślny lub wynikający z zaniedbania charakter naruszenia;

ab) wszelkie działania podjęte przez operatora w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

PUBLIC

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

ba) czy inne organy nałożyły już administracyjne kary pieniężne na tego samego operatora za naruszenia innych przepisów prawa Unii lub prawa krajowego, w przypadku gdy takie naruszenia wynikają z tego samego działania lub zaniechania stanowiącego odnośne naruszenie niniejszego aktu;

c) wielkość operatora dopuszczającego się naruszenia, jego roczny obrót i udział w rynku;

d) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

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

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

9. Wykonywanie przez organ nadzoru rynku uprawnień powierzonych mu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom proceduralnym zgodnie z prawem Unii i prawem państwa członkowskiego, obejmującym prawo do skutecznego sądowego środka ochrony prawnej i rzetelnego procesu.

PUBLIC

Artykuł 72

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

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

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

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

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

2. Nieprzestrzeganie jakichkolwiek zakazów dotyczących praktyk w zakresie sztucznej inteligencji określonych w art. 5 podlega administracyjnej karze pieniężnej w wysokości do 500 000 EUR.

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

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

PUBLIC

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

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

TYTUŁ XI

PRZEKAZANIE UPRAWNIEŃ I PROCEDURA KOMITETOWA

Artykuł 73

Wykonywanie przekazanych uprawnień

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

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

   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.

PUBLIC

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

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

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

Artykuł 74

Procedura komitetowa

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

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

PUBLIC

TYTUŁ XII

PRZEPISY KOŃCOWE

Artykuł 75

Zmiana rozporządzenia (WE) nr 300/2008

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

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

_____

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

PUBLIC

Artykuł 76

Zmiana rozporządzenia (UE) nr 167/2013

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

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

_____

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

Artykuł 77

Zmiana rozporządzenia (UE) nr 168/2013

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

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

_____

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

PUBLIC

Artykuł 78

Zmiana dyrektywy 2014/90/UE

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

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

_____

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

PUBLIC

Artykuł 79

Zmiana dyrektywy (UE) 2016/797

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

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

_____

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

Artykuł 80

Zmiana rozporządzenia (UE) 2018/858

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

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

_____

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

PUBLIC

Artykuł 81

Zmiana rozporządzenia (UE) 2018/1139

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

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

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

_____

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

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

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

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

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

PUBLIC

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

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

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

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

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

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

Artykuł 82

Zmiana rozporządzenia (UE) 2019/2144

W art. 11 rozporządzenia (UE) 2019/2144 dodaje się ustęp w brzmieniu:

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

_____

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

PUBLIC

Artykuł 83

Systemy sztucznej inteligencji już wprowadzone do obrotu lub oddane do użytku

1. Niniejsze rozporządzenie nie ma zastosowania do systemów sztucznej inteligencji, które stanowią elementy wielkoskalowych systemów informatycznych utworzonych na podstawie aktów prawnych wymienionych w załączniku IX i które wprowadzono do obrotu lub oddano do użytku przed dniem [*12 miesięcy od daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*], chyba że na skutek zastąpienia lub zmiany tych aktów prawnych zajdzie znacząca zmiana projektu lub przeznaczenia odnośnego systemu sztucznej inteligencji lub odnośnych systemów sztucznej inteligencji.

   Wymogi określone w niniejszym rozporządzeniu uwzględnia się, w stosownych przypadkach, w ocenach każdego z wielkoskalowych systemów informatycznych utworzonych na podstawie aktów prawnych wymienionych w załączniku IX, które to oceny należy przeprowadzić zgodnie z odnośnymi przepisami tych aktów.

2. Niniejsze rozporządzenie ma zastosowanie do systemów sztucznej inteligencji wysokiego ryzyka innych niż te określone w ust. 1, które wprowadzono do obrotu lub oddano do użytku przed dniem [*data rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*], wyłącznie wówczas, gdy po tej dacie projekt lub przeznaczenie tych systemów ulegną znaczącym zmianom.

Artykuł 84

Ocena i przegląd

1. [skreśla się]

1b. Komisja ocenia potrzebę wprowadzenia zmian w wykazie zawartym w załączniku III co 24 miesiące od daty wejścia w życie niniejszego rozporządzenia do końca okresu obowiązywania uprawnień. Wyniki oceny są przedstawiane Parlamentowi Europejskiemu i Radzie.

2. Do dnia [*trzy lata od daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*], a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszego rozporządzenia. Sprawozdania te są podawane do wiadomości publicznej.

3. W sprawozdaniach, o których mowa w ust. 2, szczególną uwagę zwraca się na następujące kwestie:

   a) stan zasobów finansowych, wyposażenia technicznego i zasobów ludzkich właściwych organów krajowych wymaganych, by mogły one skutecznie wykonywać zadania powierzone im na podstawie niniejszego rozporządzenia;

   b) sytuację w zakresie kar, a w szczególności administracyjnych kar pieniężnych, o których mowa w art. 71 ust. 1, nakładanych przez państwa członkowskie w przypadku naruszenia przepisów niniejszego rozporządzenia.

4. Do dnia [*trzy lata od daty rozpoczęcia stosowania niniejszego rozporządzenia, o której mowa w art. 85 ust. 2*], a następnie co cztery lata, w stosownych przypadkach, Komisja ocenia wpływ i skuteczność dobrowolnych kodeksów postępowania sprzyjających stosowaniu wymogów określonych w tytule III rozdział 2 w odniesieniu do systemów sztucznej inteligencji innych niż systemy sztucznej inteligencji wysokiego ryzyka oraz ewentualnie innych dodatkowych wymogów dotyczących systemów sztucznej inteligencji, w tym w zakresie zrównoważenia środowiskowego.

5. Do celów ust. 1a–4 Rada ds. Sztucznej Inteligencji, państwa członkowskie i właściwe organy krajowe przekazują Komisji informacje na jej wniosek.

6. Dokonując ocen i przeglądów, o których mowa w ust. 1a–4, Komisja uwzględnia stanowiska i ustalenia Rady ds. Sztucznej Inteligencji, Parlamentu Europejskiego, Rady Unii Europejskiej oraz innych stosownych podmiotów lub źródeł.

7. W razie potrzeby Komisja przedkłada odpowiednie wnioski w celu zmiany niniejszego rozporządzenia, uwzględniając w szczególności rozwój technologii oraz stan postępu w społeczeństwie informacyjnym.

PUBLIC

Artykuł 85

Wejście w życie i rozpoczęcie stosowania

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie stosuje się od dnia [36 miesięcy po wejściu w życie niniejszego rozporządzenia] r.

3. Na zasadzie odstępstwa od ust. 2:

   a) tytuł III rozdział 4 i tytuł VI stosuje się od dnia [dwanaście miesięcy od daty wejścia w życie niniejszego rozporządzenia] r.;

   b) art. 71 stosuje się od dnia [dwanaście miesięcy od daty wejścia w życie niniejszego rozporządzenia] r.

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

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący / Przewodnicząca	*Przewodniczący / Przewodnicząca*

PUBLIC

ZAŁĄCZNIK I

[skreśla się]

PUBLIC

ZAŁĄCZNIK II

WYKAZ UNIJNEGO PRAWODAWSTWA HARMONIZACYJNEGO

Sekcja A – Wykaz unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych

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

2. dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz.U. L 170 z 30.6.2009, s. 1);

3. dyrektywa Parlamentu Europejskiego i Rady 2013/53/UE z dnia 20 listopada 2013 r. w sprawie rekreacyjnych jednostek pływających i skuterów wodnych i uchylająca dyrektywę 94/25/WE (Dz.U. L 354 z 28.12.2013, s. 90);

4. dyrektywa Parlamentu Europejskiego i Rady 2014/33/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących dźwigów i elementów bezpieczeństwa do dźwigów (Dz.U. L 96 z 29.3.2014, s. 251);

5. dyrektywa Parlamentu Europejskiego i Rady 2014/34/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do urządzeń i systemów ochronnych przeznaczonych do użytku w atmosferze potencjalnie wybuchowej (Dz.U. L 96 z 29.3.2014, s. 309);

6. dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153 z 22.5.2014, s. 62);

7. dyrektywa Parlamentu Europejskiego i Rady 2014/68/UE z dnia 15 maja 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku urządzeń ciśnieniowych (Dz.U. L 189 z 27.6.2014, s. 164);

PUBLIC

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).

PUBLIC

Sekcja B. Wykaz innego unijnego prawodawstwa harmonizacyjnego

1. 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);

2. 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);

3. 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);

4. 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);

5. 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);

6. 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);

PUBLIC

7. 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);

8. 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.

PUBLIC

ZAŁĄCZNIK III

SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA, O KTÓRYCH MOWA W ART. 6 UST. 3

PUBLIC

W każdym z obszarów wymienionych w pkt 1–8 wymienione konkretnie pod każdą literą systemy sztucznej inteligencji uznaje się za systemy sztucznej inteligencji wysokiego ryzyka zgodnie z art. 6 ust. 3:

1. Biometria:

   a) Systemy zdalnej identyfikacji biometrycznej.

2. Infrastruktura krytyczna:

   a) systemy sztucznej inteligencji przeznaczone do stosowania jako związane z bezpieczeństwem elementy procesów zarządzania krytyczną infrastrukturą cyfrową, ruchem drogowym oraz zaopatrzeniem w wodę, gaz, ciepło i energię elektryczną i ich obsługi;

3. kształcenie i szkolenie zawodowe:

   a) systemy sztucznej inteligencji przeznaczone do celów podejmowania decyzji o dostępie do instytucji lub programów edukacyjnych i instytucji lub programów szkolenia zawodowego lub nadawania osobom przydziału do tych instytucji lub programów na wszystkich poziomach;

   b) systemy sztucznej inteligencji przeznaczone do oceny efektów uczenia się, także w przypadku gdy efekty te są wykorzystywane do kierowania procesem uczenia się osób fizycznych w instytucjach lub programach edukacyjnych i instytucjach lub programach szkolenia zawodowego na wszystkich poziomach.

4. zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia:

   a) systemy sztucznej inteligencji przeznaczone 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 sztucznej inteligencji przeznaczone do celów podejmowania decyzji o awansie i rozwiązaniu stosunku pracy, przydzielania zadań w oparciu o indywidualne zachowanie lub cechy osobowości oraz do monitorowania i oceny wydajności i zachowania osób pozostających w takich stosunkach;

5. dostęp do podstawowych usług prywatnych oraz usług i podstawowych świadczeń publicznych, a także korzystanie z nich:

a) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy publiczne lub w imieniu organów publicznych w celu oceny kwalifikowalności osób fizycznych do podstawowych świadczeń i usług publicznych, jak również w celu przyznawania, ograniczania, unieważniania lub żądania zwrotu takich świadczeń i usług;

b) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu oceny zdolności kredytowej osób fizycznych lub ustalenia ich punktowej oceny kredytowej, z wyjątkiem systemów sztucznej inteligencji oddawanych do użytku – do ich własnych celów – przez dostawców będących mikroprzedsiębiorstwami oraz małymi przedsiębiorstwami zgodnie z definicją w załączniku do zalecenia Komisji 2003/361/WE;

c) systemy sztucznej inteligencji przeznaczone do wykorzystania w celu wysyłania lub ustalania priorytetów w wysyłaniu służb ratunkowych w sytuacjach kryzysowych, w tym straży pożarnej i pomocy medycznej;

d) systemy sztucznej inteligencji przeznaczone do wykorzystania do celu oceny ryzyka i ustalenia stawki dla osób fizycznych w przypadku ubezpieczeń na życie i zdrowotnych, z wyjątkiem systemów sztucznej inteligencji oddawanych do użytku – do ich własnych celów – przez dostawców będących mikroprzedsiębiorstwami oraz małymi przedsiębiorstwami zgodnie z definicją w załączniku do zaleceniu Komisji 2003/361/WE.

6. ściganie przestępstw:

a) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy ścigania lub w ich imieniu do oceny ryzyka popełnienia przestępstwa lub ponownego popełnienia przestępstwa przez osobę fizyczną lub ryzyka, że osoba fizyczna stanie się potencjalną ofiarą przestępstwa;

b) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy ścigania lub w ich imieniu jako poligrafy i podobne narzędzia lub w celu wykrywania stanu emocjonalnego osoby fizycznej;

c) [skreśla się]

d) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy ścigania lub w ich imieniu do oceny wiarygodności dowodów w toku ścigania przestępstw lub prowadzenia dochodzeń w ich sprawie;

e) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy ścigania lub w ich imieniu do przewidywania wystąpienia lub ponownego wystąpienia rzeczywistego lub potencjalnego przestępstwa na podstawie profilowania osób fizycznych, o którym mowa w art. 3 pkt 4 dyrektywy (UE) 2016/680, lub do oceny cech osobowości i charakterystyki lub wcześniejszego zachowania przestępnego osób fizycznych lub grup;

f) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy ścigania lub w ich imieniu do profilowania osób fizycznych, o którym mowa w art. 3 pkt 4 dyrektywy (UE) 2016/680, w toku wykrywania i ścigania przestępstw lub prowadzenia dochodzeń w ich sprawie.

g) [skreśla się]

7. zarządzanie migracją, azylem i kontrolą graniczną:

a) systemy sztucznej inteligencji przeznaczone do wykorzystania przez właściwe organy publiczne lub w ich imieniu jako poligrafy i podobne narzędzia lub w celu wykrywania stanu emocjonalnego osoby fizycznej;

b) systemy sztucznej inteligencji przeznaczone do wykorzystania przez właściwe organy publiczne lub w ich imieniu w celu oceny ryzyka, w tym zagrożenia dla bezpieczeństwa, ryzyka migracji nieuregulowanej lub zagrożeń dla zdrowia, stwarzanych przez osobę fizyczną, która zamierza wjechać lub wjechała na terytorium państwa członkowskiego;

PUBLIC

c) [skreśla się]

d) systemy sztucznej inteligencji przeznaczone do wykorzystania przez właściwe organy publiczne lub w ich imieniu przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu.

8. sprawowanie wymiaru sprawiedliwości i procesy demokratyczne:

a) systemy sztucznej inteligencji przeznaczone do wykorzystania przez organ sądowy lub w jego imieniu do interpretacji stanu faktycznego lub przepisów prawa oraz do zastosowania prawa do konkretnego stanu faktycznego.

PUBLIC

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 sztucznej inteligencji:

1. ogólny opis systemu sztucznej inteligencji, w tym:

   a) jego przeznaczenie, dane osoby lub osób, które opracowały system, datę i wersję systemu;

   b) sposób, w jaki system sztucznej inteligencji, w stosownych przypadkach, współdziała lub może być wykorzystany do współdziałania ze sprzętem lub oprogramowaniem, które nie są częścią samego systemu sztucznej inteligencji;

   c) wersje odpowiedniego oprogramowania lub oprogramowania układowego oraz wszelkie wymogi związane z aktualizacją wersji;

   d) opis wszystkich form, w jakich system sztucznej inteligencji wprowadza się do obrotu lub oddaje do użytku (np. pakiet oprogramowania wbudowany w urządzenie, do pobrania, API, itp.);

   e) opis sprzętu, na którym system sztucznej inteligencji ma być eksploatowany;

   f) w przypadku gdy system sztucznej inteligencji jest elementem produktów – zdjęcia lub ilustracje przedstawiające cechy zewnętrzne, oznakowanie i układ wewnętrzny tych produktów;

   g) instrukcję obsługi dla użytkownika oraz, w stosownych przypadkach, instrukcję instalacji;

2. szczegółowy opis elementów systemu sztucznej inteligencji oraz procesu jego opracowywania, w tym:

   a) metody i działania zastosowane w celu opracowania systemu sztucznej inteligencji, w tym, w stosownych przypadkach, skorzystanie z już wytrenowanych systemów lub narzędzi dostarczonych przez osoby trzecie oraz wskazanie, w jaki sposób dostawca wykorzystał, zintegrował lub zmodyfikował te systemy lub narzędzia;

PUBLIC

b) specyfikacje projektowe systemu, a mianowicie ogólna logiki systemu sztucznej inteligencji i algorytmów; kluczowe decyzje projektowe wraz z uzasadnieniem i przyjętymi założeniami, również w odniesieniu do osób lub grup osób, wobec których system ma być wykorzystywany; główne wybory klasyfikacyjne; wskazanie, pod kątem czego system ma być optymalizowany, i znaczenie poszczególnych parametrów; opis oczekiwanego wyniku działania systemu; decyzje dotyczące wszelkich możliwych kompromisów w zakresie rozwiązań technicznych przyjętych w celu spełnienia wymogów określonych w tytule III rozdział 2;

c) opis architektury systemu wyjaśniający, w jaki sposób elementy oprogramowania współgrają ze sobą lub wzajemnie się uzupełniają oraz włączają się w ogólne przetwarzanie; zasoby obliczeniowe wykorzystywane do opracowania, trenowania, testowania i walidacji systemu sztucznej inteligencji;

d) w stosownych przypadkach wymogi dotyczące danych w zakresie arkuszy danych opisujących metodyki i techniki trenowania systemu oraz wykorzystane zbiory danych treningowych, w tym ogólny opis tych zbiorów danych, informacje o ich pochodzeniu, ich zakresie i głównych cechach; sposób, w jaki uzyskano i wybrano dane; 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 użytkownikom interpretacji wyników działania systemów sztucznej inteligencji, zgodnie z art. 13 ust. 3 lit. d);

f) w stosownych przypadkach szczegółowy opis z góry zaplanowanych zmian w systemie sztucznej inteligencji i jego skuteczności działania wraz ze wszystkimi istotnymi informacjami dotyczącymi rozwiązań technicznych przyjętych w celu zapewnienia ciągłej zgodności systemu sztucznej inteligencji z odpowiednimi wymogami określonymi w tytule III rozdział 2;

PUBLIC

g) zastosowane procedury walidacji i testowania, w tym informacje o wykorzystanych danych walidacyjnych i danych testowych oraz ich głównych cechach; wskaźniki stosowane do pomiaru dokładności, solidności, cyberbezpieczeństwa i zgodności z innymi stosownymi wymogami określonymi w tytule III rozdział 2, jak również potencjalnie dyskryminujących skutków; 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);

3. szczegółowe informacje dotyczące monitorowania, funkcjonowania i kontroli systemu sztucznej inteligencji, w szczególności w odniesieniu do: jego możliwości i ograniczeń w zakresie skuteczności działania, w tym stopnie dokładności w przypadku określonych osób lub grup osób, wobec których system ma być wykorzystywany, oraz ogólny spodziewany poziom dokładności w stosunku do jego przeznaczenia; możliwych do przewidzenia niezamierzonych wyników działania i źródeł zagrożeń dla zdrowia i bezpieczeństwa, praw podstawowych i dyskryminacji w świetle przeznaczenia systemu sztucznej inteligencji; środków nadzoru ze strony człowieka wymaganych na podstawie art. 14, w tym środków technicznych wprowadzonych w celu ułatwienia użytkownikom interpretacji wyników działania systemów sztucznej inteligencji; w stosownych przypadkach specyfikacji dotyczących danych wejściowych;

4. szczegółowy opis systemu zarządzania ryzykiem zgodnie z art. 9;

5. opis odpowiednich zmian dokonanych przez dostawcę w systemie w czasie trwania cyklu życia tego systemu;

6. 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 tytule III rozdział 2, w tym wykaz innych odpowiednich zastosowanych norm i specyfikacji technicznych;

7. kopię deklaracji zgodności UE;

8. szczegółowy opis systemu stosowanego do oceny skuteczności działania systemu sztucznej inteligencji po wprowadzeniu do obrotu zgodnie z art. 61, w tym plan monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 61 ust. 3.

ZAŁĄCZNIK V

DEKLARACJA ZGODNOŚCI UE

W deklaracji zgodności UE, o której mowa w art. 48, zamieszcza się wszystkie następujące informacje:

1. nazwę i rodzaj systemu sztucznej inteligencji oraz wszelkie dodatkowe jednoznaczne odniesienia umożliwiające identyfikację i identyfikowalność systemu sztucznej inteligencji;

2. nazwę/imię i nazwisko i adres dostawcy lub, w stosownych przypadkach, jego upoważnionego przedstawiciela;

3. oświadczenie, że deklarację zgodności UE wydano na wyłączną odpowiedzialność dostawcy;

4. oświadczenie, że przedmiotowy system sztucznej inteligencji jest zgodny z niniejszym rozporządzeniem oraz, w stosownych przypadkach, z wszelkimi innymi odpowiednimi przepisami Unii, w których przewidziano wydanie deklaracji zgodności UE;

5. odniesienia do wszelkich zastosowanych odpowiednich norm zharmonizowanych lub wszelkich innych wspólnych specyfikacji, z którymi deklaruje się zgodność;

6. w stosownych przypadkach nazwę i numer identyfikacyjny jednostki notyfikowanej, opis przeprowadzonej procedury oceny zgodności oraz dane identyfikacyjne wydanego certyfikatu;

7. miejsce i datę wystawienia deklaracji, imię i nazwisko oraz stanowisko osoby, która złożyła podpis pod dokumentem, oraz wskazanie, z czyjego upoważnienia i w czyim imieniu ta osoba podpisała dokument, oraz podpis.

PUBLIC

ZAŁĄCZNIK VI

PROCEDURA OCENY ZGODNOŚCI OPIERAJĄCA SIĘ NA KONTROLI WEWNĘTRZNEJ

1. Procedura oceny zgodności opierająca się na kontroli wewnętrznej jest procedurą oceny zgodności przeprowadzaną na podstawie pkt 2–4.

2. Dostawca sprawdza, czy ustanowiony system zarządzania jakością spełnia wymogi art. 17.

3. Dostawca analizuje informacje zawarte w dokumentacji technicznej, aby ocenić zgodność systemu sztucznej inteligencji z odpowiednimi zasadniczymi wymogami określonymi w tytule III rozdział 2.

4. Dostawca sprawdza również, czy proces projektowania i opracowywania systemu sztucznej inteligencji oraz proces jego monitorowania po wprowadzeniu do obrotu, o którym mowa w art. 61, są zgodne z dokumentacją techniczną.

PUBLIC

ZAŁĄCZNIK VII

ZGODNOŚĆ OPIERAJĄCA SIĘ NA OCENIE SYSTEMU ZARZĄDZANIA JAKOŚCIĄ I OCENIE DOKUMENTACJI TECHNICZNEJ

PUBLIC

1. Wprowadzenie

Zgodność opierająca się na ocenie systemu zarządzania jakością i ocenie dokumentacji technicznej jest procedurą oceny zgodności przeprowadzaną na podstawie pkt 2–5.

2. Informacje ogólne

Zatwierdzony system zarządzania jakością w zakresie projektowania, opracowywania i testowania systemów sztucznej inteligencji zgodnie z art. 17 ocenia się zgodnie z pkt 3 i poddaje nadzorowi zgodnie z pkt 5. Dokumentację techniczną systemu sztucznej inteligencji ocenia się zgodnie z pkt 4.

3. System zarządzania jakością

3.1. Wniosek dostawcy zawiera:

a) nazwę/imię i nazwisko i adres dostawcy oraz, jeśli wniosek jest składany przez upoważnionego przedstawiciela, również jego nazwę/imię i nazwisko i adres;

b) wykaz systemów sztucznej inteligencji objętych tym samym systemem zarządzania jakością;

c) dokumentację techniczną każdego systemu sztucznej inteligencji objętego tym samym systemem zarządzania jakością;

d) dokumentację dotyczącą systemu zarządzania jakością, która obejmuje wszystkie aspekty wymienione w art. 17;

e) opis procedur zapewniających stałą adekwatność i skuteczność systemu zarządzania jakością;

f) pisemne oświadczenie, że tego samego wniosku nie złożono w żadnej innej jednostce notyfikowanej.

3.2. System zarządzania jakością podlega ocenie jednostki notyfikowanej, która ustala, czy spełnia on wymogi, o których mowa w art. 17.

O decyzji informuje się dostawcę lub jego upoważnionego przedstawiciela.

Informacja taka zawiera wnioski z oceny systemu zarządzania jakością oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

3.3. Dostawca w dalszym ciągu wdraża i utrzymuje zatwierdzony system zarządzania jakością, tak aby pozostawał on adekwatny i skuteczny.

3.4. Dostawca powiadamia jednostkę notyfikowaną o wszelkich zamierzonych zmianach w zatwierdzonym systemie zarządzania jakością lub w wykazie systemów sztucznej inteligencji objętych tym systemem.

Proponowane zmiany podlegają weryfikacji przeprowadzanej przez jednostkę notyfikowaną, która decyduje, czy zmieniony system zarządzania jakością nadal spełnia wymogi, o których mowa w pkt 3.2, czy też konieczna jest jego ponowna ocena.

Jednostka notyfikowana informuje dostawcę o swojej decyzji. Taka informacja zawiera wnioski z weryfikacji zmian oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

4. Kontrola dokumentacji technicznej.

4.1. Oprócz wniosku, o którym mowa w pkt 3, dostawca składa wniosek do wybranej przez siebie jednostki notyfikowanej o ocenę dokumentacji technicznej dotyczącej systemu sztucznej inteligencji, który dostawca zamierza wprowadzić do obrotu lub oddać do użytku i który jest objęty systemem zarządzania jakością, o którym mowa w pkt 3.

PUBLIC

4.2. Wniosek zawiera:

a) nazwę i adres dostawcy;

b) pisemne oświadczenie, że tego samego wniosku nie złożono w żadnej innej jednostce notyfikowanej;

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

4.3. Ocenę dokumentacji technicznej przeprowadza jednostka notyfikowana. W stosownych przypadkach i w zakresie ograniczonym do tego, co jest niezbędne do wykonywania jej zadań, jednostka notyfikowana otrzymuje pełny dostęp do wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, w tym, w stosownych przypadkach i z zastrzeżeniem gwarancji bezpieczeństwa, za pośrednictwem interfejsów programowania aplikacji („API") lub innych odpowiednich środków i narzędzi technicznych umożliwiających zdalny dostęp.

4.4. Analizując dokumentację techniczną, jednostka notyfikowana może zażądać od dostawcy przedstawienia dalszych dowodów lub przeprowadzenia dalszych testów w celu umożliwienia właściwej oceny zgodności systemu sztucznej inteligencji z wymogami określonymi w tytule III rozdział 2. Jeżeli jednostka notyfikowana nie jest usatysfakcjonowana testami przeprowadzonymi przez dostawcę, jednostka notyfikowana przeprowadza bezpośrednio, stosownie do okoliczności, odpowiednie testy.

4.5. Jednostkom notyfikowanym udziela się dostępu do kodu źródłowego systemu sztucznej inteligencji na ich uzasadniony wniosek i wyłącznie wtedy, gdy spełnione są łącznie następujące warunki:

a) dostęp do kodu źródłowego jest niezbędny do oceny zgodności systemu sztucznej inteligencji wysokiego ryzyka z wymogami określonymi w tytule III rozdział 2; oraz

b) zostały wyczerpane lub okazały się niewystarczające procedury testowania/audytu i weryfikacji w oparciu o dane i dokumentację dostarczone przez dostawcę.

PUBLIC

4.6. O decyzji informuje się dostawcę lub jego upoważnionego przedstawiciela. Taka informacja zawiera wnioski z oceny dokumentacji produktu oraz uzasadnioną decyzję dotyczącą dokonanej oceny.

W przypadku gdy system sztucznej inteligencji spełnia wymogi określone w tytule III rozdział 2, jednostka notyfikowana wydaje unijny certyfikat oceny dokumentacji technicznej. Certyfikat zawiera nazwę i adres dostawcy, wnioski z oceny, ewentualne warunki jego ważności oraz dane niezbędne do identyfikacji systemu sztucznej inteligencji.

Certyfikat wraz z załącznikami musi zawierać wszystkie istotne informacje umożliwiające ewaluację zgodności systemu sztucznej inteligencji oraz, w stosownych przypadkach, kontrolę systemu sztucznej inteligencji podczas jego użytkowania.

W przypadku gdy system sztucznej inteligencji nie spełnia wymogów określonych w tytule III rozdział 2, jednostka notyfikowana odmawia wydania unijnego certyfikatu oceny dokumentacji technicznej i informuje o tym wnioskodawcę, podając szczegółowe uzasadnienie odmowy.

W przypadku gdy system sztucznej inteligencji nie spełnia wymogu dotyczącego danych wykorzystanych do jego trenowania, przed złożeniem wniosku o nową ocenę zgodności system sztucznej inteligencji należy poddać ponownemu treningowi. W takim przypadku uzasadniona decyzja jednostki notyfikowanej o odmowie wydania unijnego certyfikatu oceny dokumentacji technicznej zawiera szczegółowe uwagi na temat jakości danych wykorzystanych do treningu systemu sztucznej inteligencji, w szczególności na temat przyczyn niezgodności.

PUBLIC

4.7. Wszystkie zmiany w systemie sztucznej inteligencji, które mogłyby wpłynąć na zgodność systemu sztucznej inteligencji z wymogami lub jego przeznaczeniem, podlegają zatwierdzeniu przez jednostkę notyfikowaną, która wydała unijny certyfikat oceny dokumentacji technicznej. Dostawca informuje taką jednostkę notyfikowaną, jeżeli zamierza wprowadzić takie zmiany lub jeżeli w inny sposób dowiedział się o ich zaistnieniu. Zamierzone zmiany ocenia jednostka notyfikowana, która decyduje, czy zmiany te wymagają przeprowadzenia nowej oceny zgodności zgodnie z art. 43 ust. 4, czy też można je uwzględnić w formie suplementu do unijnego certyfikatu oceny dokumentacji technicznej. W tym ostatnim przypadku jednostka notyfikowana ocenia zmiany, informuje dostawcę o swojej decyzji i, w przypadku zatwierdzenia zmian, wydaje dostawcy suplement do unijnego certyfikatu oceny dokumentacji technicznej.

5. Nadzór nad zatwierdzonym systemem zarządzania jakością.

5.1. Celem nadzoru sprawowanego przez jednostkę notyfikowaną, o której mowa w pkt 3, jest zapewnienie, aby dostawca należycie wywiązywał się z warunków, jakimi obwarowano zatwierdzony system zarządzania jakością.

5.2. Do celów oceny dostawca umożliwia jednostce notyfikowanej dostęp do pomieszczeń, w których odbywa się projektowanie, opracowywanie i testowanie systemów sztucznej inteligencji. 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 sztucznej inteligencji, w odniesieniu do których wydano unijny certyfikat oceny dokumentacji technicznej.

PUBLIC

ZAŁĄCZNIK VIII

INFORMACJE PRZEKAZYWANE PRZY REJESTRACJI OPERATORÓW I SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA ZGODNIE Z ART. 51

Dostawcy, upoważnieni przedstawiciele i użytkownicy będący organami, agencjami lub podmiotami publicznymi przekazują informacje, o których mowa w części I. Dostawcy lub, w stosownych przypadkach, upoważnieni przedstawiciele zapewniają kompletność, poprawność i aktualność informacji na temat ich systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w części II pkt 1–11. Informacje określone w pkt II.12 są automatycznie generowane przez bazę danych.

Część I. Informacje dotyczące operatorów (przy rejestracji operatora)

-1. rodzaj operatora (dostawca, upoważniony przedstawiciel lub użytkownik);

1. nazwa/imię i nazwisko, adres i dane kontaktowe dostawcy;

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

Część II. Informacje dotyczące systemu sztucznej inteligencji wysokiego ryzyka

1. nazwa/imię i nazwisko, adres i dane kontaktowe dostawcy;

2. w stosownych przypadkach nazwa/imię i nazwisko, adres i dane kontaktowe upoważnionego przedstawiciela;

3. nazwa handlowa systemu sztucznej inteligencji oraz wszelkie dodatkowe jednoznaczne odniesienia umożliwiające identyfikację i identyfikowalność systemu sztucznej inteligencji;

4. opis przeznaczenia systemu sztucznej inteligencji;

5. status systemu sztucznej inteligencji (dostępny na rynku lub użytkowany; niewprowadzany już do obrotu/już nieużytkowany, wycofany od użytkowników);

6. rodzaj, numer i datę ważności certyfikatu wydanego przez jednostkę notyfikowaną oraz w stosownych przypadkach nazwę lub numer identyfikacyjny tej jednostki notyfikowanej;

7. w stosownych przypadkach skan certyfikatu, o którym mowa w pkt 6;

8. państwa członkowskie, w których system sztucznej inteligencji wprowadza się lub wprowadzono do obrotu, oddaje się lub oddano do użytku bądź udostępnia się lub udostępniono w Unii;

9. kopia deklaracji zgodności UE, o której mowa w art. 48;

10. elektroniczna instrukcja obsługi;

11. adres URL odsyłający do dodatkowych informacji (opcjonalnie);

12. nazwa/imię i nazwisko, adres i dane kontaktowe użytkowników.

PUBLIC

ZAŁĄCZNIK VIIIa

INFORMACJE, KTÓRE NALEŻY PRZEDŁOŻYĆ PRZY REJESTRACJI SYSTEMÓW SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA WYMIENIONYCH W ZAŁĄCZNIKU III W ODNIESIENIU DO TESTÓW W WARUNKACH RZECZYWISTYCH ZGODNIE Z ART. 54a

PUBLIC

W odniesieniu do testów w warunkach rzeczywistych, które podlegają rejestracji zgodnie z art. 54a, przekazuje się, a następnie aktualizuje następujące informacje:

1. ogólnounijny niepowtarzalny numer identyfikacyjny testów w warunkach rzeczywistych;

2. nazwę i dane kontaktowe dostawcy lub potencjalnego dostawcy i użytkowników uczestniczących w testach w warunkach rzeczywistych;

3. krótki opis systemu sztucznej inteligencji, 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 IX

PRZEPISY UNII DOTYCZĄCE WIELKOSKALOWYCH SYSTEMÓW INFORMATYCZNYCH W PRZESTRZENI WOLNOŚCI, BEZPIECZEŃSTWA I SPRAWIEDLIWOŚCI

PUBLIC

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) wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 767/2008, rozporządzenie (WE) nr 810/2009, rozporządzenie (UE) 2017/2226, rozporządzenie (UE) 2016/399, rozporządzenie XX/2018 [rozporządzenie w sprawie interoperacyjności] i decyzję 2004/512/WE oraz uchylającego decyzję Rady 2008/633/WSiSW – COM(2018) 302 final. Do aktualizacji po przyjęciu rozporządzenia (kwiecień/maj 2021 r.) przez współprawodawców.

3. Eurodac:

a) zmieniony wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania danych biometrycznych w celu skutecznego stosowania rozporządzenia (UE) XXX/XXX [rozporządzenie w sprawie zarządzania azylem i migracją] i rozporządzenia (UE) XXX/XXX [rozporządzenie w sprawie przesiedleń] na potrzeby identyfikowania nielegalnie przebywających obywateli państw trzecich lub bezpaństwowców oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego oraz zmieniającego rozporządzenia (UE) 2018/1240 i (UE) 2019/818 – COM(2020) 614 final.

4. System wjazdu/wyjazdu:

a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz.U. L 327 z 9.12.2017, s. 20).

5. Europejski system informacji o podróży oraz zezwoleń na podróż:

a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz.U. L 236 z 19.9.2018, s. 1);

b) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1241 z dnia 12 września 2018 r. zmieniające rozporządzenie (UE) 2016/794 w celu ustanowienia europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) (Dz.U. L 236 z 19.9.2018, s. 72).

6. Europejski system przekazywania informacji z rejestrów karnych dotyczących obywateli państw trzecich i bezpaństwowców:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.U. L 135 z 22.5.2019, s. 1).

7. Interoperacyjność:

   a) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze granic i polityki wizowej (Dz.U. L 135 z 22.5.2019, s. 27);

   b) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/818 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze współpracy policyjnej i sądowej, azylu i migracji (Dz.U. L 135 z 22.5.2019, s. 85).

PUBLIC