AI ACT

AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI

Komentarz

redakcja naukowa
Maria Jędrzejczak, Łukasz Szoszkiewicz, Jędrzej Wydra

Wojciech Biernacki, Jan Denka, Paweł Dudko, Igor Gontarz
Jędrzej Jakubowicz, Krzysztof Jeromin, Maria Jędrzejczak
Karolina Kiejnich-Kruk, Katarzyna Klafkowska-Waśniowska
Michalina Kowala, Zuzanna Kowalska, Michał Krotoszyński
Martyna Kusak, Kamil Łakomy, Patryk Pieniążek
Wojciech Rzepiński, Łukasz Szoszkiewicz, Jędrzej Wydra

Wolters Kluwer

Poszczególne części komentarza napisali:

Wojciech Biernacki – art. 48–50, 52, 54, 55

Wojciech Biernacki, Wojciech Rzepiński – art. 56

Wojciech Biernacki, Jan Denka, Paweł Dudko, Igor Gontarz, Jędrzej Jakubowicz, Krzysztof Jeromin, Maria Jędrzejczak, Karolina Kiejnich-Kruk, Zuzanna Kowalska, Michał Krotoszyński, Kamil Łakomy, Patryk Pieniążek, Wojciech Rzepiński, Łukasz Szoszkiewicz, Jędrzej Wydra – art. 3

Jan Denka – art. 68–70, 85–87, 96, 97

Paweł Dudko – art. 57–63

Paweł Dudko, Jędrzej Jakubowicz – art. 95

Igor Gontarz – art. 40–46

Igor Gontarz, Karolina Kiejnich-Kruk – art. 27

Jędrzej Jakubowicz – art. 72–79

Krzysztof Jeromin – art. 16, 18–22, 47

Krzysztof Jeromin, Jędrzej Wydra – art. 17

Maria Jędrzejczak – art. 1, 2, 4, 107–113

Maria Jędrzejczak, Łukasz Szoszkiewicz, Jędrzej Wydra – Wstęp

Katarzyna Klafkowska-Waśniowska, Wojciech Biernacki – art. 53

Michalina Kowala – art. 91–93

Zuzanna Kowalska – art. 88, 102–106

Zuzanna Kowalska, Łukasz Szoszkiewicz – art. 8, 9

Michał Krotoszyński – art. 80–84

Martyna Kusak – art. 10–12

Kamil Łakomy – art. 7, 23–26

Kamil Łakomy, Wojciech Rzepiński – art. 5

Patryk Pieniążek – art. 64–67, 89, 94, 98–101

Wojciech Rzepiński – art. 6, 14, 28–31, 35–39

Wojciech Rzepiński, Łukasz Szoszkiewicz – art. 33

Łukasz Szoszkiewicz – art. 71, 90

Jędrzej Wydra – art. 13, 15, 32, 34, 51

AI ACT

AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI

Komentarz

redakcja naukowa
Maria Jędrzejczak, Łukasz Szoszkiewicz, Jędrzej Wydra

Wojciech Biernacki, Jan Denka, Paweł Dudko, Igor Gontarz
Jędrzej Jakubowicz, Krzysztof Jeromin, Maria Jędrzejczak
Karolina Kiejnich-Kruk, Katarzyna Klafkowska-Waśniowska
Michalina Kowala, Zuzanna Kowalska, Michał Krotoszyński
Martyna Kusak, Kamil Łakomy, Patryk Pieniążek
Wojciech Rzepiński, Łukasz Szoszkiewicz, Jędrzej Wydra

Wolters Kluwer

WARSZAWA 2025

Fragmenty opracowane przez dr. Igora Gontarza zawierają częściowe wyniki badań zrealizowanych w ramach projektu nr 2022/45/N/HS5/04260 „Kontrola systemów automatycznego decydowania stosowanych w postępowaniu administracyjnym" finansowanego ze środków Narodowego Centrum Nauki

Stan prawny na 8 września 2025 r.

Recenzentka
Dr hab. Marlena Sakowska-Baryła, profesor Uniwersytetu Łódzkiego

Wydawczyni
Monika Pawłowska

Redaktorka prowadząca
Kinga Zając

Opracowanie redakcyjne
JustLuk

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

ISBN 978-83-8390-798-7 *ISBN PDF-a: 978-83-8438-003-1*

Wolters Kluwer Polska Sp. z o.o.
Dział Zarządzania Prawami Autorskimi i Treściami
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 692 477 076
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

Spis treści

Wykaz skrótów

I. Akty prawne

AI Act	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.Urz. UE L 2024/1689)
decyzja EUSI	–	decyzja Komisji C/2024/1459 z 24.01.2024 r. ustanawiająca Europejski Urząd ds. Sztucznej Inteligencji (Dz.Urz. UE C 2024/1459)
dyrektywa 2001/29/WE	–	dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z 22.05.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. UE L 167, s. 10, ze zm.)
dyrektywa 2002/58/WE	–	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201, s. 37, ze zm.)
dyrektywa 2005/29/WE	–	dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z 11.05.2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady (dyrektywa o nieuczciwych praktykach handlowych) (Dz.Urz. UE L 149, s. 22, ze zm.)
dyrektywa 2006/42/WE	–	dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z 17.05.2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE (przekształcenie) (Dz.Urz. UE L 157, s. 24, ze zm.)
dyrektywa 2013/36/UE	–	dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z 26.06.2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.Urz. UE L 176, s. 338, ze zm.)

dyrektywa 2014/53/UE	–	dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z 16.04.2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.Urz. UE L 153, s. 62, ze zm.)
dyrektywa 2014/90/UE	–	dyrektywa Parlamentu Europejskiego i Rady 2014/90/UE z 23.07.2014 r. w sprawie wyposażenia morskiego i uchylająca dyrektywę Rady 96/98/WE (Dz.Urz. UE L 257, s. 146, ze zm.)
dyrektywa 2016/680	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89, ze sprost.)
dyrektywa 2016/797	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/797 z 11.05.2016 r. w sprawie interoperacyjności systemu kolei w Unii Europejskiej (Dz.Urz. UE L 138, s. 44, ze zm.)
dyrektywa 2016/943	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.Urz. UE L 157, s. 1)
dyrektywa 2016/2102	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z 26.10.2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.Urz. UE L 327, s. 1)
dyrektywa 2019/790	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92)
dyrektywa 2019/882	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z 17.04.2019 r. w sprawie wymogów dostępności produktów i usług (Dz.Urz. UE L 151, s. 70)
dyrektywa 2019/1937	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23.10.2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.Urz. UE L 305, s. 17, ze zm.)
dyrektywa 2020/1828	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/1828 z 25.11.2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz.Urz. UE L 409, s. 1, ze zm.)
dyrektywa 2022/2555	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.Urz. UE L 333, s. 80)

dyrektywa 2022/2557	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14.12.2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.Urz. UE L 333, s. 164)
EKPC	–	Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2024 r. poz. 1061 ze zm.)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2025 r. poz. 383)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
k.p.a.	–	ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572 ze zm.)
k.p.c.	–	ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2024 r. poz. 1568 ze zm.)
k.p.k.	–	ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2025 r. poz. 46 ze zm.)
KPP	–	Karta Praw Podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
p.p.s.a.	–	ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2024 r. poz. 935 ze zm.)
pr. aut.	–	ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2025 r. poz. 24 ze zm.)
projekt ustawy o systemach sztucznej inteligencji z 18.08.2025 r.	–	projekt ustawy o systemach sztucznej inteligencji z 18.08.2025 r., https://legislacja.rcl.gov.pl/docs//2/12390551/13087917/13087921/dokument733307.pdf
rozporządzenie 765/2008	–	rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z 9.07.2008 r. ustanawiające wymagania w zakresie akredytacji i uchylające rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L 218, s. 30, ze zm.)
rozporządzenie 182/2011	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16.02.2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.Urz. UE L 55, s. 13)
rozporządzenie 1025/2012	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z 25.10.2012 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.Urz. UE L 316, s. 12, ze zm.)
rozporządzenie 167/2013	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 167/2013 z 5.02.2013 r. w sprawie homologacji i nadzoru rynku pojazdów rolniczych i leśnych (Dz.Urz. UE L 60, s. 1, ze zm.)

rozporządzenie 168/2013	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 168/2013 z 15.01.2013 r. w sprawie homologacji i nadzoru rynku pojazdów dwu- lub trzykołowych oraz czterokołowców (Dz.Urz. UE L 60, s. 52, ze zm.)
rozporządzenie 2016/679 / RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1)
rozporządzenie 2017/745 / rozporządzenie MDR	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5.04.2017 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.Urz. UE L 117, s. 1, ze zm.)
rozporządzenie 2018/1725	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 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.Urz. UE L 295, s. 39)
rozporządzenie 2019/881 / akt o cyberbezpieczeństwie	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 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.Urz. UE L 151, s. 15, ze zm.)
rozporządzenie 2019/1020	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z 20.06.2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L 169, s. 1, ze zm.)
rozporządzenie 2022/2065	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.Urz. UE L 277, s. 1)
rozporządzenie 2023/988	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z 10.05.2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz.Urz. UE L 135, s. 1, ze zm.)
rozporządzenie wykonawcze 2025/454	–	rozporządzenie wykonawcze Komisji (UE) 2025/454 z 7.03.2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 w odniesieniu do ustanowienia panelu naukowego niezależnych ekspertów w dziedzinie sztucznej inteligencji (Dz.Urz. UE L 454, s. 1)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)
TUE	–	Traktat o Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 13)
u.o.s.	–	ustawa z 14.06.2024 r. o ochronie sygnalistów (Dz.U. poz. 928)

ustawa o ABW	–	ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2025 r. poz. 902 ze zm.)
ZTP	–	rozporządzenie Prezesa Rady Ministrów z 20.06.2002 r. w sprawie „Zasad techniki prawodawczej" (Dz.U. z 2016 r. poz. 283)

II. Czasopisma, publikatory

OSNKW	–	Orzecznictwo Sądu Najwyższego Izba Karna i Wojskowa
OSNwSK	–	Orzecznictwo Sądu Najwyższego w Sprawach Karnych
ZNUJ PPWI	–	Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej

III. Inne

CEN	–	Europejski Komitet Normalizacyjny
CENELEC	–	Europejski Komitet Normalizacyjny Elektrotechniki
EDPB	–	Europejska Rada Ochrony Danych (European Data Protection Board)
EHDS	–	Europejska Przestrzeń Danych Dotyczących Zdrowia
EIOD	–	Europejski Inspektor Ochrony Danych
ENISA	–	Agencja Unii Europejskiej ds. Cyberbezpieczeństwa
ETSI	–	Europejski Instytut Norm Telekomunikacyjnych
FRIA	–	ocena skutków dla praw podstawowych
MŚP	–	małe i średnie przedsiębiorstwa
TSUE	–	Trybunał Sprawiedliwości Unii Europejskiej
UODO	–	Urząd Ochrony Danych Osobowych

Wstęp

Akt w sprawie sztucznej inteligencji wszedł w życie 1.08.2024 r. i co do zasady zacznie być stosowany 2.08.2026 r. (z pewnymi wyjątkami). To pierwszy akt prawny na świecie, który w wiążący i całościowy sposób reguluje wprowadzanie na rynek i stosowanie systemów sztucznej inteligencji przez podmioty publiczne i prywatne.

Celem rozporządzenia jest stworzenie w Unii Europejskiej jednolitych ram prawnych promujących zaufanie do zorientowanej na człowieka sztucznej inteligencji przy jednoczesnym zapewnieniu wysokiej ochrony interesów publicznych, w tym zdrowia, bezpieczeństwa i praw podstawowych.

Rozporządzenie będzie obowiązywało we wszystkich państwach członkowskich w sposób bezpośredni, co ma zapobiec rozdrobnieniu rynku wewnętrznego i ułatwiać wprowadzanie na rynek unijny innowacji opartych na sztucznej inteligencji. Na rzeczywiste osiągnięcie projektowanego ujednolicenia wymogów w tym sektorze będzie wpływać stosowanie nowego prawa przez operatorów, organy nadzorcze i sądy, a także zakres aktywności prawodawców krajowych.

W komentarzu zostały uwzględnione nie tylko przepisy unijnego rozporządzenia, lecz także dokumenty wydane przez Komisję Europejską, jak też projekt krajowej ustawy o systemach sztucznej inteligencji z 18.08.2025 r. W przypadkach wymagających pogłębionych rozważań autorzy sięgali do wypowiedzi doktryny polskiej i międzynarodowej.

Komentarz zawiera praktyczne analizy, konkretne przykłady i szczegółowe wyjaśnienia, które sprawiają, że jest to publikacja przeznaczona nie tylko dla prawników, lecz także dla przedsiębiorców wdrażających systemy sztucznej inteligencji w swojej działalności.

Opracowanie niniejszego komentarza było możliwe dzięki zaangażowaniu osiemnastu autorów o rozległych kompetencjach merytorycznych z zakresu prawa sztucznej inteligencji, będących zarówno naukowcami, jak i przedstawicielami praktyki, w tym prowadzącymi obsługę prawną podmiotów zajmujących się rozwojem oprogramowania z wykorzystaniem rozwiązań opartych na sztucznej inteligencji. W gronie autorów, poza prawnikami, znaleźli się również specjaliści z doświadczeniem programistycznym i statystycznym, jak też posiadający kompetencje z zakresu *data science* i matematycznych podstaw sztucznej inteligencji. To dzięki ich zaangażowaniu możliwe było oddanie publikacji do druku jeszcze przed rozpoczęciem stosowania rozporządzenia. Jak wskazuje objętość komentarza, skala nadchodzących zmian jest rozległa. Oznacza to, że zarówno prawodawca krajowy, jak i adresaci rozporządzenia powinni rozpocząć przygotowania do zapewnienia zgodności systemów sztucznej

inteligencji z aktem dotyczącym tego zagadnienia, w czym niniejsza publikacja będzie mogła, mamy nadzieję, im pomóc.

Liczymy, że niniejszy komentarz stanie się głosem w dyskusji na temat wykładni aktu w sprawie sztucznej inteligencji, ale także ułatwi jego praktyczne zastosowanie. Mamy też nadzieję, że przyczyni się do budowania kompetencji w zakresie AI, których znaczenie zostało podkreślone w rozporządzeniu – są one niezbędne do zapewnienia odpowiedzialnego wdrażania rozwiązań opartych na sztucznej inteligencji w społeczeństwie.

Komentarz uwzględnia stan prawny na dzień 8.09.2025 r.

***

Redaktorzy pragną wyrazić podziękowania Panu Piotrowi Brzyskiemu, Panu Łukaszowi Grzybowskiemu oraz Panu Krzysztofowi Jędrzejewskiemu, członkom Stowarzyszenia Badań i Zastosowań Sztucznej Inteligencji (Association for Research and Applications of Artificial Intelligence, ARAAI), praktykom z zakresu AI, za merytoryczne konsultacje tekstu komentarza, w szczególności zamieszczonych w nim praktycznych przykładów zastosowania przepisów. Dziękujemy za nieocenione wskazówki, które umożliwiły odniesienie zagadnień prawnych do realiów rynku i pracy z systemami sztucznej inteligencji.

Szczególne podziękowania kierujemy również do Pana Profesora Michała Klichowskiego z Centrum Neuronauki Poznawczej oraz Wydziału Studiów Edukacyjnych Uniwersytetu im. Adama Mickiewicza w Poznaniu za konsultacje, które miały istotny wpływ na ostateczny kształt opracowania.

Maria Jędrzejczak, Łukasz Szoszkiewicz, Jędrzej Wydra

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689
z dnia 13 czerwca 2024 r.

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

(Tekst mający znaczenie dla EOG)

(Dz.Urz. UE L 2024/1689)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,
uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 i 114,
uwzględniając wniosek Komisji Europejskiej,
po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,
uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],
uwzględniając opinię Europejskiego Banku Centralnego[2],
uwzględniając opinię Komitetu Regionów[3],
stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[4],
a także mając na uwadze, co następuje:

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

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

(3) Systemy AI mogą być łatwo wdrażane w wielu różnych sektorach gospodarki i obszarach życia społecznego, w tym w wymiarze transgranicznym, i mogą w łatwy sposób być przedmiotem obrotu w całej Unii. Niektóre państwa członkowskie zastanawiają się już nad przyjęciem przepisów krajowych w celu zapewnienia, aby AI była godna zaufania i bezpieczna oraz rozwijana i wykorzystywana w sposób zgodny z obowiązkami wynikającymi z praw podstawowych. Zróżnicowane przepisy krajowe mogą prowadzić do rozdrobnienia rynku wewnętrznego i mogą zmniejszyć pewność prawa dla operatorów, którzy rozwijają, importują lub wykorzystują systemy AI. Aby zatem AI stała się godna zaufania, należy zapewnić spójny i wysoki poziom ochrony w całej Unii poprzez ustanowienie jednolitych obowiązków dla operatorów i zagwarantowanie jednolitej ochrony nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym na podstawie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), zapobiegając jednocześnie rozbieżnościom, które utrudniają swobodny obrót systemami AI oraz powiązanymi produktami i usługami na rynku wewnętrznym, a także utrudniają innowacje w ich zakresie oraz ich wdrażanie i rozpowszechnianie. W zakresie, w jakim niniejsze rozporządzenie zawiera przepisy szczególne dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w odniesieniu do ograniczenia wykorzystywania systemów AI do zdalnej identyfikacji biometrycznej do celów ścigania przestępstw, ograniczenia wykorzystywania systemów AI do oceny ryzyka w odniesieniu do osób fizycznych do celów ścigania przestępstw i ograniczenia wykorzystywania systemów AI kategoryzacji biometrycznej do celów ścigania przestępstw, podstawą niniejszego rozporządzenia w zakresie takich przepisów szczególnych powinien być art. 16 TFUE. W świetle tych przepisów szczególnych i skorzystania z art. 16 TFUE należy skonsultować się z Europejską Radą Ochrony Danych.

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

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

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

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

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

(9) Zharmonizowane przepisy mające zastosowanie do wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów AI wysokiego ryzyka należy ustanowić zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008[7], decyzją Parlamentu Europejskiego i Rady nr 768/2008/WE[8] oraz rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/1020[9] (zwanymi dalej „nowymi ramami prawnymi"). Zharmonizowane przepisy ustanowione w niniejszym rozporządzeniu powinny mieć zastosowanie we wszystkich sektorach i – zgodnie z nowymi ramami prawnymi – powinny pozostawać bez uszczerbku dla obowiązującego prawa Unii, w szczególności w zakresie ochrony danych, ochrony konsumentów, praw podstawowych, zatrudnienia i ochrony pracowników oraz bezpieczeństwa produktów, wobec którego to prawa niniejsze rozporządzenie ma charakter uzupełniający. W związku z tym wszystkie prawa i środki ochrony prawnej przysługujące na mocy prawa Unii konsumentom i innym osobom, na które systemy AI mogą mieć negatywny wpływ, w tym w odniesieniu do odszkodowania za ewentualne szkody zgodnie z dyrektywą Rady 85/374/EWG[10], pozostają nienaruszone i mają pełne zastosowanie. Ponadto w kontekście zatrudnienia i ochrony pracowników niniejsze rozporządzenie nie powinno zatem mieć wpływu na prawo Unii w dziedzinie polityki społecznej oraz na krajowe prawo pracy zgodne z prawem Unii dotyczące warunków zatrudnienia i pracy, w tym bezpieczeństwa i higieny pracy, oraz stosunków między pracodawcami a pracownikami. Niniejsze rozporządzenie nie powinno mieć też wpływu na korzystanie z praw podstawowych uznanych w państwach członkowskich i na poziomie Unii, w tym z prawa do strajku czy swobody prowadzenia strajku lub innych działań objętych szczególnymi systemami stosunków pracy w państwach członkowskich, ani na korzystanie z prawa do negocjowania, zawierania i egzekwowania układów zbiorowych lub podejmowania działań zbiorowych zgodnie z prawem krajowym. Niniejsze rozporządzenie nie powinno mieć wpływu na przepisy mające na celu poprawę warunków pracy świadczonej za pośrednictwem platform internetowych ustanowione w dyrektywie Parlamentu Europejskiego i Rady w sprawie poprawy warunków pracy za pośrednictwem platform internetowych. Ponadto niniejsze rozporządzenie ma na celu zwiększenie skuteczności takich istniejących praw i środków ochrony prawnej poprzez ustanowienie szczególnych wymogów i obowiązków, w tym w zakresie przejrzystości, dokumentacji technicznej i rejestrowania zdarzeń w ramach systemów AI. Co więcej obowiązki nałożone na mocy niniejszego rozporządzenia na różnych operatorów uczestniczących w łańcuchu wartości AI powinny mieć zastosowanie bez uszczerbku dla prawa krajowego zgodnego z prawem Unii, skutkującego ograniczeniem wykorzystania określonych systemów AI, gdy prawo to nie wchodzi w zakres stosowania niniejszego rozporządzenia lub służy uzasadnionym celom interesu publicznego innym niż cele niniejszego rozporządzenia. Na przykład niniejsze rozporządzenie nie powinno mieć wpływu na krajowe prawo pracy i przepisy dotyczące ochrony małoletnich, tj. osób poniżej 18. roku życia, uwzględniające komentarz ogólny nr 25 z 2021 r. w sprawie praw dziecka w środowisku cyfrowym zamieszczony w Konwencji ONZ o prawach dziecka, w zakresie w jakim prawo to i te przepisy nie dotyczą konkretnie systemów AI i służą innym uzasadnionym celom interesu publicznego.

(10) Podstawowe prawo do ochrony danych osobowych jest gwarantowane w szczególności przez rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[11] i (UE) 2018/1725[12] oraz dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680[13]. Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE[14] dodatkowo chroni życie prywatne i poufność komunikacji, w tym określając warunki dotyczące przechowywania danych osobowych i nieosobowych w urządzeniach końcowych oraz warunki uzyskiwania dostępu do tych danych z urządzeń końcowych. Te unijne akty prawne stanowią podstawę zrównoważonego i odpowiedzialnego przetwarzania danych, w tym w przypadku gdy zbiory danych zawierają połączenie danych osobowych i nieosobowych. Celem niniejszego rozporządzenia nie jest wpływanie na stosowanie obowiązującego prawa Unii regulującego przetwarzanie danych osobowych, w tym

na zadania i uprawnienia niezależnych organów nadzoru właściwych do monitorowania zgodności z tymi instrumentami. W zakresie, w jakim projektowanie, rozwój lub wykorzystywanie systemów AI wiąże się z przetwarzaniem danych osobowych, niniejsze rozporządzenie nie wpływa też na wynikające z prawa Unii lub prawa krajowego obowiązki w dziedzinie ochrony danych osobowych spoczywające na dostawcach i podmiotach stosujących systemy AI, którzy pełnią funkcję administratorów danych lub podmiotów przetwarzających. Należy również wyjaśnić, że osoby, których dane dotyczą, zachowują wszystkie prawa i gwarancje przyznane im na mocy takiego prawa Unii, w tym prawa związane z całkowicie zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, w tym z profilowaniem. Ustanowione w niniejszym rozporządzeniu zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku i wykorzystywania systemów AI powinny ułatwiać skuteczne wdrażanie i umożliwiać korzystanie przez osoby, których dane dotyczą, z praw i innych środków ochrony prawnej zagwarantowanych na podstawie prawa Unii dotyczącego ochrony danych osobowych i innych praw podstawowych.

(11) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla przepisów dotyczących odpowiedzialności dostawców usług pośrednich, określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2065[15].

(12) Pojęcie „systemu AI" w niniejszym rozporządzeniu powinno być jasno zdefiniowane i ściśle powiązane z pracami organizacji międzynarodowych zajmujących się AI, aby zapewnić pewność prawa, ułatwiać międzynarodową konwergencję i szeroką akceptację, przy jednoczesnym zapewnieniu swobody umożliwiającej dostosowanie się do szybkiego rozwoju technologicznego w tej dziedzinie. Ponadto pojęcie to powinno opierać się na kluczowych cechach systemów AI, które odróżniają je od prostszych tradycyjnych systemów oprogramowania lub założeń programistycznych, i nie powinno obejmować systemów opartych na zasadach określonych wyłącznie przez osoby fizyczne w celu automatycznego wykonywania operacji. Jedną z kluczowych cech systemów AI jest ich zdolność do wnioskowania. Ta zdolność do wnioskowania odnosi się do procesu uzyskiwania wyników, takich jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne i wirtualne, oraz do zdolności systemów AI do tworzenia modeli lub algorytmów na podstawie informacji wejściowych lub danych. Techniki, które umożliwiają wnioskowanie podczas tworzenia systemu AI, obejmują mechanizmy uczenia maszynowego, które na podstawie danych uczą się, jak osiągnąć określone cele, oraz podejścia oparte na logice i wiedzy, które polegają na wnioskowaniu na podstawie zakodowanej wiedzy lub symbolicznego przedstawienia zadania, które należy rozwiązać. Zdolność systemu AI do wnioskowania wykracza poza podstawowe przetwarzanie danych w wyniku umożliwiania uczenia się, rozumowania lub modelowania. Termin „maszynowy" odnosi się do faktu, że systemy AI działają z wykorzystaniem maszyn. Odniesienie do wyraźnych lub dorozumianych celów podkreśla, że systemy AI mogą działać według jasno określonych lub dorozumianych celów. Cele systemu AI mogą różnić się od przeznaczenia systemu AI w określonym kontekście. Na potrzeby niniejszego rozporządzenia środowiska należy rozumieć jako konteksty, w których działają systemy AI, natomiast wyniki generowane przez system AI odzwierciedlają różne funkcje wykonywane przez systemy AI i obejmują predykcje, treści, zalecenia lub decyzje. Systemy AI są zaprojektowane tak, aby działały z różnym poziomem autonomii, co oznacza, że są w pewnym stopniu niezależne od zaangażowania ze strony człowieka i zdolne do działania bez interwencji człowieka. Zdolność adaptacji, jaką system AI może wykazać po jego wdrożeniu, odnosi się do zdolności do samouczenia się, która umożliwia zmianę systemu w czasie jego wykorzystywania. Systemy AI mogą być wykorzystywane jako samodzielne rozwiązania lub jako element produktu, niezależnie od tego, czy system jest fizycznie zintegrowany z produktem (wbudowany), czy też służy realizacji funkcji produktu, choć nie jest z nim zintegrowany (niewbudowany).

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

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

(15) Pojęcie „identyfikacji biometrycznej", o którym mowa w niniejszym rozporządzeniu, należy zdefiniować jako zautomatyzowane rozpoznawanie fizycznych, fizjologicznych i behawioralnych cech człowieka, takich jak twarz, ruch gałek ocznych, kształt ciała, głos, właściwości mowy, chód, postawa, tętno, ciśnienie krwi, zapach, sposób pisania na klawiaturze, w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z przechowywanymi w referencyjnej bazie danych danymi biometrycznymi osób fizycznych, niezależnie od tego, czy osoba ta wyraziła na to zgodę. Do tej kategorii

nie należą systemy AI przeznaczone do weryfikacji biometrycznej, która obejmuje uwierzytelnianie, prowadzonej jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie w celu uzyskania dostępu do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń.

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

(17) Pojęcie „systemu zdalnej identyfikacji biometrycznej", o którym mowa w niniejszym rozporządzeniu, należy zdefiniować funkcjonalnie jako system AI służący do identyfikacji osób fizycznych bez aktywnego udziału tych osób, co do zasady na odległość, poprzez porównanie danych biometrycznych danej osoby z danymi biometrycznymi zawartymi w referencyjnej bazie danych, niezależnie od konkretnej stosowanej technologii oraz konkretnych wykorzystywanych procesów lub rodzajów danych biometrycznych. Takie systemy zdalnej identyfikacji biometrycznej są zwykle wykorzystywane do jednoczesnego obserwowania wielu osób lub ich zachowania w celu znacznego ułatwienia identyfikacji osób fizycznych bez ich aktywnego udziału. Do tej kategorii nie należą systemy AI przeznaczone do weryfikacji biometrycznej, która obejmuje uwierzytelnianie, prowadzonej jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, oraz potwierdzenia tożsamości osoby fizycznej wyłącznie w celu uzyskania dostępu do usługi, uruchomienia urządzenia lub uzyskania bezpiecznego dostępu do pomieszczeń. Wyłączenie to jest uzasadnione faktem, że takie systemy w niewielkim stopniu mogą wpływać na prawa podstawowe osób fizycznych w porównaniu z systemami zdalnej identyfikacji biometrycznej, które mogą być wykorzystywane do przetwarzania danych biometrycznych dużej liczby osób bez ich aktywnego udziału. W przypadku systemów działających „w czasie rzeczywistym" zbieranie danych biometrycznych, porównanie i identyfikacja następują natychmiast, niemal natychmiast lub w każdym razie bez znacznego opóźnienia. W związku z tym nie powinno być możliwości obchodzenia przepisów niniejszego rozporządzenia dotyczących stosowania systemów AI „w czasie rzeczywistym" poprzez wprowadzanie niewielkich opóźnień. Systemy identyfikacji „w czasie rzeczywistym" obejmują wykorzystanie materiału rejestrowanego „na żywo" lub „niemal na żywo", takiego jak materiał wideo generowany przez kamerę lub inne urządzenie o podobnej funkcjonalności. Natomiast w przypadku systemów identyfikacji post factum dane biometryczne zostały już zebrane, a porównanie i identyfikacja następują ze znacznym opóźnieniem. Dotyczy to materiałów, takich jak zdjęcia lub materiały wideo generowane przez kamery telewizji przemysłowej lub urządzenia prywatne, które to materiały zostały wygenerowane, zanim użyto systemu identyfikacji w stosunku do danej osoby fizycznej.

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

(19) Do celów niniejszego rozporządzenia pojęcie „przestrzeni publicznej" należy rozumieć jako odnoszące się do każdej przestrzeni fizycznej, która jest dostępna dla nieokreślonej liczby osób fizycznych, niezależnie od tego, czy dana przestrzeń jest własnością prywatną czy publiczną, a także niezależnie od rodzaju działalności, dla której się ją wykorzystuje, takiej jak działalność handlowa (na przykład sklepy, restauracje,

kawiarnie), działalność usługowa (na przykład banki, działalność zawodowa, hotelarstwo), działalność sportowa (na przykład baseny, sale do ćwiczeń, stadiony), działalność transportowa (na przykład dworce autobusowe i kolejowe, stacje metra, lotniska, środki transportu), działalność rozrywkowa (na przykład kina, teatry, muzea, sale koncertowe i konferencyjne) lub przestrzenie służące wypoczynkowi lub innym celom (na przykład drogi publiczne i place, parki, lasy i place zabaw). Przestrzeń należy uznać za przestrzeń publiczną również wtedy, gdy niezależnie od potencjalnych ograniczeń w zakresie pojemności lub bezpieczeństwa, dostęp do niej podlega pewnym określonym z góry warunkom, które mogą zostać spełnione przez nieokreśloną liczbę osób, takich jak zakup biletu wstępu lub biletu na przejazd, uprzednia rejestracja lub osiągnięcie określonego wieku. Danej przestrzeni nie należy natomiast uznawać za przestrzeń publiczną, jeśli dostęp do niej ograniczony jest do konkretnych i określonych osób fizycznych na mocy prawa Unii lub prawa krajowego bezpośrednio związanego z bezpieczeństwem publicznym lub ochroną publiczną lub w wyniku wyraźnego wyrażenia woli przez osobę posiadającą odpowiednie uprawnienia związane z taką przestrzenią. Faktyczna możliwość samego dostępu (taka jak niezamknięte drzwi, otwarta bramka w ogrodzeniu) nie oznacza, że dana przestrzeń stanowi przestrzeń publiczną, jeśli istnieją wskazania lub okoliczności sugerujące inaczej (takie jak znaki zakazujące dostępu lub go ograniczające). Tereny przedsiębiorstw i fabryk, a także biura i miejsca pracy, do których dostęp powinni mieć wyłącznie odpowiedni pracownicy i usługodawcy, to przestrzenie, które nie stanowią przestrzeni publicznej. Do przestrzeni publicznej nie zaliczają się więzienia ani strefy kontroli granicznej. Niektóre przestrzenie mogą zawierać zarówno przestrzenie publiczne, jak i niepubliczne, takie jak hol w prywatnym budynku mieszkalnym prowadzący do gabinetu lekarskiego lub lotnisko. Przestrzenie internetowe również nie są objęte tym pojęciem, ponieważ nie są to przestrzenie fizyczne. To, czy dana przestrzeń jest dostępna publicznie, powinno być jednak ustalane indywidualnie w każdym przypadku, z uwzględnieniem specyfiki danej sytuacji.

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

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

(22) Ze względu na swój cyfrowy charakter niektóre systemy AI powinny zostać objęte zakresem stosowania niniejszego rozporządzenia, nawet jeśli nie zostały wprowadzane do obrotu, oddane do użytku ani są wykorzystywane w Unii. Dotyczy to na przykład operatora mającego siedzibę w Unii, który zleca operatorowi mającemu siedzibę w państwie trzecim określone usługi w związku z działaniem, które ma być wykonywane przez system AI, który zostałby zakwalifikowany jako system wysokiego ryzyka. W takich okolicznościach system AI wykorzystywany w państwie trzecim przez operatora mógłby przetwarzać dane, które legalnie zgromadzono w Unii i przekazano poza Unię, oraz przekazywać zlecającemu operatorowi z Unii wynik przetwarzania tych danych przez system AI, natomiast sam system AI nie byłby wprowadzony do obrotu lub oddany do użytku w Unii ani nie byłby w Unii wykorzystywany. Aby zapobiec obchodzeniu przepisów niniejszego rozporządzenia oraz zapewnić skuteczną ochronę osób fizycznych znajdujących się w Unii, niniejsze rozporządzenie powinno mieć również zastosowanie do dostawców i podmiotów stosujących systemy AI, którzy mają siedzibę lub miejsce zamieszkania w państwie trzecim, w zakresie, w jakim wyniki wytworzone przez te systemy są przeznaczone do wykorzystywania

w Unii. Aby uwzględnić jednak istniejące ustalenia i szczególne potrzeby w zakresie przyszłej współpracy z partnerami zagranicznymi, z którymi wymienia się informacje i dowody, niniejszego rozporządzenia nie powinno się stosować do organów publicznych państwa trzeciego i organizacji międzynarodowych działających w ramach współpracy lub na mocy zawartych na poziomie Unii lub poziomie krajowym umów międzynarodowych o współpracy organów ścigania i wymiarów sprawiedliwości z Unią lub państwami członkowskimi, pod warunkiem zapewnienia przez to państwo trzecie lub organizację międzynarodową odpowiednich zabezpieczeń w odniesieniu do ochrony podstawowych praw i wolności osób fizycznych. W stosownych przypadkach może to obejmować działania podmiotów, którym państwa trzecie powierzyły wykonywanie szczególnych zadań w ramach wsparcia ścigania przestępstw i współpracy wymiarów sprawiedliwości. Takie ramy współpracy lub umowy zostały ustanowione dwustronnie między państwami członkowskimi a państwami trzecimi lub między Unią Europejską, Europolem i innymi agencjami Unii a państwami trzecimi i organizacjami międzynarodowymi. Organy właściwe do sprawowania nadzoru nad organami ścigania i organami wymiaru sprawiedliwości na mocy niniejszego rozporządzenia powinny ocenić, czy te ramy współpracy lub umowy międzynarodowe zawierają odpowiednie zabezpieczenia w odniesieniu do ochrony podstawowych praw i wolności osób fizycznych. Będące odbiorcami organy krajowe oraz instytucje, organy i jednostki organizacyjne Unii korzystające z takich wyników w Unii pozostają odpowiedzialne za zapewnienie zgodności ich stosowania z prawem Unii. W przypadku zmiany takich umów międzynarodowych lub zawarcia nowych w przyszłości umawiające się strony powinny dołożyć wszelkich starań, by dostosować takie umowy do wymogów niniejszego rozporządzenia.

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

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

(25) Niniejsze rozporządzenie powinno wspierać innowacje, szanować wolność nauki i nie powinno osłabiać działalności badawczo-rozwojowej. Należy zatem wyłączyć z jego zakresu stosowania systemy i modele AI rozwinięte i oddane do użytku wyłącznie do celów badań naukowych i rozwojowych. Ponadto należy zapewnić, aby niniejsze rozporządzenie nie wpływało w żaden inny sposób na działalność badawczo-rozwojową dotyczącą systemów lub modeli AI przed wprowadzeniem tych systemów lub modeli do obrotu lub oddaniem ich do użytku. Przepisów niniejszego rozporządzenia nie powinno się również stosować do zorientowanej na produkty działalności badawczej, testowej i rozwojowej dotyczącej

systemów lub modeli AI przed oddaniem tych systemów i modeli do użytku lub wprowadzaniem ich do obrotu. Wyłączenie to pozostaje to bez uszczerbku dla obowiązku zapewnienia zgodności z niniejszym rozporządzeniem, gdy system AI objęty zakresem stosowania niniejszego rozporządzenia jest wprowadzany do obrotu lub oddawany do użytku w wyniku takiej działalności badawczo-rozwojowej, oraz dla stosowania przepisów dotyczących piaskownic regulacyjnych w zakresie AI i testów w warunkach rzeczywistych. Ponadto bez uszczerbku dla wyłączenia systemów AI rozwiniętych i oddanych do użytku wyłącznie do celów badań naukowych i rozwojowych, wszelkie inne systemy AI, które mogą być wykorzystywane do prowadzenia wszelkiej działalności badawczo-rozwojowej, powinny podlegać przepisom niniejszego rozporządzenia. W każdym przypadku wszelka działalność badawczo-rozwojowa powinna być prowadzona zgodnie z uznanymi normami etycznymi i zawodowymi dotyczącymi badań naukowych oraz zgodnie z mającym zastosowanie prawem Unii.

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

(27) Chociaż podstawą proporcjonalnego i skutecznego zbioru wiążących przepisów jest podejście oparte na analizie ryzyka, należy przypomnieć Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji z 2019 r. opracowane przez niezależną grupę ekspertów wysokiego szczebla ds. AI powołaną przez Komisję. W tych wytycznych grupa ekspertów wysokiego szczebla ds. AI opracowała siedem niewiążących zasad etycznych dotyczących AI, które mają pomóc zapewnić, aby AI była godna zaufania i zgodna z normami etycznymi. Te siedem zasad to: przewodnia i nadzorcza rola człowieka; solidność techniczna i bezpieczeństwo; ochrona prywatności i zarządzanie danymi; przejrzystość; różnorodność, niedyskryminacja i sprawiedliwość; dobrostan społeczny i środowiskowy oraz odpowiedzialność. Bez uszczerbku dla prawnie wiążących wymogów niniejszego rozporządzenia i wszelkich innych mających zastosowanie przepisów prawa Unii, wytyczne te przyczyniają się do zaprojektowania spójnej, wiarygodnej i zorientowanej na człowieka AI, zgodnie z Kartą i wartościami, na których opiera się Unia. Zgodnie z wytycznymi grupy ekspertów wysokiego szczebla ds. AI przewodnia i nadzorcza rola człowieka oznacza, że systemy AI rozwija się i wykorzystuje jako narzędzia służące ludziom, szanujące godność ludzką i autonomię osobistą oraz działające w sposób, który może być odpowiednio kontrolowany i nadzorowany przez człowieka. Solidność techniczna i bezpieczeństwo oznaczają, że systemy AI rozwija się i wykorzystuje w taki sposób, by okazały się wytrzymałe w przypadku wystąpienia problemów oraz odporne na próby zmiany ich wykorzystania lub skuteczności działania, co pozwoli zapobiec bezprawnemu wykorzystaniu przez osoby trzecie i zminimalizować niezamierzone szkody. Ochrona prywatności i zarządzanie danymi oznaczają, że systemy AI rozwija się i wykorzystuje zgodnie z przepisami dotyczącymi prywatności i ochrony danych, przy czym przetwarzanie danych spełnia wysokie standardy pod względem jakości i integralności. Przejrzystość oznacza, że systemy AI rozwija się i wykorzystuje w sposób umożliwiający odpowiednią identyfikowalność i wytłumaczalność, jednocześnie informując ludzi o tym, że komunikują się z systemem AI lub podejmują z nim interakcję, a także należycie informując podmioty stosujące o zdolnościach i ograniczeniach tego systemu AI, a osoby, na które AI ma wpływ, o przysługujących im prawach. Różnorodność, niedyskryminacja i sprawiedliwość oznaczają, że systemy AI rozwija się i wykorzystuje w sposób, który angażuje różne podmioty i propaguje równy dostęp, równouprawnienie płci i różnorodność kulturową, jednocześnie unikając dyskryminujących skutków i niesprawiedliwej stronniczości, których zakazują prawo Unii lub prawo krajowe. Dobrostan społeczny i środowiskowy oznacza, że systemy AI rozwija się i wykorzystuje w sposób zrównoważony, przyjazny dla środowiska i przynoszący korzyści wszystkim ludziom, jednocześnie monitorując i oceniając długoterminowy wpływ tych systemów na osoby fizyczne, społeczeństwo i demokrację. Stosowanie tych zasad powinno w miarę możliwości znaleźć odzwierciedlenie w projektowaniu i wykorzystywaniu modeli AI. Zasady te powinny w każdym przypadku stanowić fundament przy opracowywaniu kodeksów postępowania na podstawie niniejszego rozporządzenia. Wszystkie zainteresowane strony, w tym przedstawicieli przemysłu, środowisko akademickie, społeczeństwo obywatelskie i organizacje normalizacyjne, zachęca się, by przy opracowywaniu dobrowolnych najlepszych praktyk i norm uwzględniali odpowiednio przedmiotowe zasady etyczne.

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

(29) Techniki manipulacyjne oparte na AI mogą być wykorzystywane w celu nakłaniania osób do niepożądanych zachowań lub w celu wprowadzania ich w błąd poprzez skłanianie ich do podejmowania decyzji w sposób, który podważa i ogranicza ich autonomię, decyzyjność i swobodę wyboru. Wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie niektórych systemów AI, których celem lub skutkiem jest znacząca zmiana ludzkiego zachowania, w związku z czym mogą wystąpić poważne szkody, w szczególności mające wystarczająco istotny niepożądany wpływ na zdrowie fizyczne, psychiczne lub na interesy finansowe, są szczególnie niebezpieczne i w związku z tym powinny być zakazane. Takie systemy AI wykorzystują elementy działające podprogowo, takie jak bodźce dźwiękowe, bodźce będące obrazami lub materiałami wideo, których nie można dostrzec, ponieważ bodźce takie wykraczają poza świadomą ludzką percepcję, lub stosują inne techniki manipulacyjne lub wprowadzające w błąd, które podważają lub ograniczają autonomię człowieka, decyzyjność lub swobodę wyboru w taki sposób, że osoby nie są świadome takich technik lub nawet jeśli są ich świadome, mogą zostać wprowadzone w błąd lub nie są w stanie sprawować nad nimi kontroli ani im się sprzeciwić. Przyczyniać się do tego mogą na przykład interfejsy maszyna-mózg lub rzeczywistość wirtualna, ponieważ pozwalają one na większą kontrolę nad tym, jakim bodźcom są poddawane osoby, do tego stopnia, że mogą one znacząco zmieniać zachowanie tych osób w sposób znacząco szkodliwy. Ponadto systemy AI mogą również w inny sposób wykorzystywać słabości danej osoby lub określonej grupy osób ze względu na ich wiek, niepełnosprawność w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/882[16] lub szczególną sytuację społeczną lub ekonomiczną, która może sprawić, że osoby te, takie jak osoby żyjące w skrajnym ubóstwie, osoby z mniejszości etnicznych lub religijnych, będą bardziej narażone na ich wykorzystanie. Takie systemy AI mogą być wprowadzane do obrotu, oddawane do użytku lub wykorzystywane w celu lub ze skutkiem znaczącej zmiany zachowania danej osoby, oraz w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić poważną szkodę tej osoby lub innej osoby lub grupy osób, w tym szkody kumulujące się z biegiem czasu, i w związku z tym powinny być zakazane. Nie można zakładać, że zaistniał zamiar dokonania zmiany zachowania, jeżeli zmiana ta wynika z czynników, które mają charakter zewnętrzny w stosunku do systemu AI i które są poza kontrolą dostawcy lub podmiotu stosującego, a zatem ani dostawca ani podmiot stosujący AI nie mogą ich racjonalnie przewidzieć ani im przeciwdziałać. W każdym razie nie ma znaczenia, czy dostawca lub podmiot stosujący mieli zamiar wyrządzić poważną szkodę, istotny jest fakt, że szkoda wynika z praktyk manipulacyjnych opartych na AI lub ich wykorzystywania. Zakazy dotyczące takich praktyk w zakresie AI stanowią uzupełnienie przepisów zawartych w dyrektywie Parlamentu Europejskiego i Rady 2005/29/WE[17], w szczególności przepisu zakazującego stosowania we wszelkich okolicznościach nieuczciwych praktyk handlowych powodujących dla konsumentów szkody ekonomiczne lub finansowe, niezależnie od tego, czy praktyki te stosuje się za pomocą systemów AI czy w innym kontekście. Zawarty w niniejszym rozporządzeniu zakaz praktyk polegających na manipulacji lub wykorzystywaniu nie powinien mieć wpływu na zgodne z prawem praktyki w kontekście leczenia, takie jak terapia psychologiczna w związku z chorobą psychiczną lub rehabilitacja fizyczna, gdy praktyki te są prowadzone zgodnie z mającymi zastosowanie prawem i normami medycznymi, na przykład za wyraźną zgodą danej osoby fizycznej lub jej przedstawiciela prawnego. Ponadto powszechne i zasadne praktyki handlowe, na przykład w dziedzinie reklamy, które są zgodne z mającym zastosowanie prawem, nie powinny być same w sobie uznawane za szkodliwe praktyki manipulacyjne oparte na AI.

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

(31) Systemy AI, które umożliwiają prowadzenie przez podmioty publiczne lub prywatne scoringu społecznego, mogą prowadzić do wyników stanowiących dyskryminację i do wykluczenia pewnych grup. Mogą one naruszać prawo do godności i niedyskryminacji oraz wartości, jakimi są równość i sprawiedliwość. Takie systemy AI oceniają lub klasyfikują osoby fizyczne lub grupy osób fizycznych na podstawie wielu punktów danych dotyczących ich zachowań społecznych w wielu kontekstach lub na podstawie znanych, wywnioskowanych lub przewidywanych cech osobistych lub cech osobowości w określonych przedziałach czasowych. Scoring społeczny uzyskany w rezultacie działania takich systemów AI może prowadzić do krzywdzącego lub niekorzystnego traktowania osób fizycznych lub całych grup osób fizycznych w kontekstach społecznych, które nie są związane z kontekstem, w którym pierwotnie wygenerowano lub zgromadzono dane, lub do krzywdzącego traktowania, które jest nieproporcjonalne lub nieuzasadnione w stosunku do wagi ich zachowań społecznych. Należy zatem

zakazać systemów AI, w których stosuje się takie niedopuszczalne praktyki scoringu, które przynoszą takie krzywdzące lub niekorzystne wyniki. Zakaz ten nie powinien mieć wpływu na zgodne z prawem praktyki oceny osób fizycznych, które są stosowane w konkretnym celu zgodnie z prawem Unii i prawem krajowym.

(32) Wykorzystanie systemów AI do zdalnej identyfikacji biometrycznej osób fizycznych w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw szczególnie ingeruje w prawa i wolności zainteresowanych osób, do tego stopnia że może ono wpływać na życie prywatne dużej części społeczeństwa, wywoływać poczucie stałego nadzoru i pośrednio zniechęcać do korzystania z wolności zgromadzeń i innych praw podstawowych. Techniczne niedokładności systemów AI przeznaczonych do zdalnej identyfikacji biometrycznej osób fizycznych mogą prowadzić do nieobiektywnych wyników i wywoływać skutki w postaci dyskryminacji. Takie ewentualne nieobiektywne wyniki i skutki w postaci dyskryminacji są szczególnie istotne w odniesieniu do wieku, pochodzenia etnicznego, rasy, płci lub niepełnosprawności. Ponadto bezpośredniość oddziaływania i ograniczone możliwości późniejszej kontroli lub korekty wykorzystania takich systemów działających w czasie rzeczywistym niosą ze sobą zwiększone ryzyko dla praw i wolności osób zainteresowanych w związku z działaniami organów ścigania lub na które działania te miały wpływ.

(33) Wykorzystanie tych systemów w celu ścigania przestępstw powinno zatem być zabronione, z wyjątkiem wyczerpującej listy wąsko zdefiniowanych sytuacji, w których wykorzystanie to jest bezwzględnie konieczne do realizacji istotnego interesu publicznego, którego waga przeważa nad ryzykiem. Sytuacje te obejmują poszukiwanie określonych ofiar przestępstw, w tym osób zaginionych; zapobieganie niektórym zagrożeniom życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu; oraz lokalizowanie lub identyfikowanie sprawców przestępstw lub podejrzanych o popełnienie przestępstw wymienionych w załączniku do niniejszego rozporządzenia, w przypadku gdy przestępstwa te podlegają w danym państwie członkowskim karze pozbawienia stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy Parlamentu Europejskiego i Rady 97/7/WE, 98/27/WE i 2002/65/WE oraz rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 2006/2004 (dyrektywa o nieuczciwych praktykach handlowych) (Dz.U. L 149 z 11.6.2005, s. 22). wolności lub środkowi polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej cztery lata, zgodnie z ich definicją w prawie tego państwa członkowskiego. Taki próg kary pozbawienia wolności lub środka polegającego na pozbawieniu wolności zgodnie z prawem krajowym pozwala zapewnić, aby przestępstwo było na tyle poważne, by potencjalnie uzasadniać wykorzystanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym. Ponadto wykaz przestępstw przedstawiony w załączniku do niniejszego rozporządzenia opiera się na 32 przestępstwach wymienionych w decyzji ramowej Rady 2002/584/WSiSW[18], biorąc pod uwagę, że niektóre z tych przestępstw mogą w praktyce mieć większe znaczenie niż inne, ponieważ można przewidzieć, że korzystanie ze zdalnej identyfikacji biometrycznej w czasie rzeczywistym może być w bardzo różnym stopniu konieczne i proporcjonalne do praktycznych celów lokalizowania lub identyfikowania sprawcy poszczególnych wymienionych przestępstw lub podejrzanego o popełnienie tych przestępstw, przy uwzględnieniu prawdopodobnych różnic w odniesieniu do powagi, prawdopodobieństwa i skali szkody lub ewentualnych negatywnych konsekwencji. Bezpośrednie zagrożenie życia lub bezpieczeństwa fizycznego osób fizycznych może również wynikać z poważnego zakłócenia funkcjonowania infrastruktury krytycznej zdefiniowanej w art. 2 pkt 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557[19], w przypadku gdy zakłócenie lub zniszczenie takiej infrastruktury krytycznej spowodowałoby bezpośrednie zagrożenie życia lub bezpieczeństwa fizycznego osoby, w tym poprzez poważną szkodę w dostarczaniu podstawowych dostaw dla ludności lub w wykonywaniu podstawowych funkcji państwa. Ponadto niniejsze rozporządzenie powinno utrzymać możliwość przeprowadzania przez organy ścigania, organy kontroli granicznej, organy imigracyjne lub organy azylowe kontroli tożsamości w obecności danej osoby zgodnie z warunkami określonymi w prawie Unii i prawie krajowym w odniesieniu do takich kontroli. W szczególności organy ścigania, organy kontroli granicznej, organy imigracyjne lub organy azylowe powinny mieć możliwość korzystania z systemów informacyjnych, zgodnie z prawem Unii lub prawem krajowym, w celu zidentyfikowania osób, które podczas kontroli tożsamości odmawiają identyfikacji lub nie są w stanie podać lub dowieść swojej tożsamości – bez konieczności uzyskiwania uprzedniego zezwolenia na podstawie niniejszego rozporządzenia. Może to na przykład dotyczyć osoby mającej związek z przestępstwem, która nie chce lub – w wyniku wypadku lub z powodu stanu zdrowia – nie jest w stanie ujawnić swojej tożsamości organom ścigania.

(34) W celu zapewnienia, aby systemy te były wykorzystywane w sposób odpowiedzialny i proporcjonalny, należy również zastrzec, że w każdej z tych wąsko zdefiniowanych sytuacji z wyczerpującej listy należy uwzględniać pewne elementy, w szczególności charakter sytuacji, która skutkowała złożeniem wniosku, wpływ wykorzystania takich systemów na prawa i wolności wszystkich zainteresowanych osób, a także zabezpieczenia i warunki przewidziane na potrzeby wykorzystania takich systemów. Ponadto wykorzystanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej

w celu ścigania przestępstw powinno mieć miejsce jedynie, by potwierdzić tożsamość konkretnej poszukiwanej osoby, i nie powinno wykraczać poza to, co jest bezwzględnie konieczne w odniesieniu do przedziału czasowego, a także zakresu geograficznego i podmiotowego, z uwzględnieniem w szczególności dowodów lub wskazówek dotyczących zagrożeń, ofiar lub sprawcy. Wykorzystanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej powinno być dozwolone tylko wtedy, gdy odpowiedni organ ścigania przeprowadził ocenę skutków dla praw podstawowych oraz, o ile niniejsze rozporządzenie nie stanowi inaczej, zarejestrował system w bazie danych, jak określono w niniejszym rozporządzeniu. Referencyjna baza danych osób powinna być odpowiednia dla każdego przypadku wykorzystania w każdej z wyżej wymienionych sytuacji.

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

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

(37) Ponadto należy zapewnić, z zastosowaniem wyczerpujących ram określonych w niniejszym rozporządzeniu, aby takie wykorzystanie na terytorium państwa członkowskiego zgodnie z niniejszym rozporządzeniem było możliwe tylko wówczas, gdy – i w zakresie, w jakim – dane państwo członkowskie postanowiło wyraźnie przewidzieć możliwość zezwolenia na takie wykorzystanie w swoich szczegółowych przepisach prawa krajowego. W związku z tym państwa członkowskie mogą na mocy niniejszego rozporządzenia w ogóle nie przewidywać takiej możliwości lub przewidzieć ją jedynie w odniesieniu do niektórych celów mogących uzasadniać dozwolone wykorzystanie, określonych w niniejszym rozporządzeniu. Komisja powinna zostać powiadomiona o takich przepisach krajowych w terminie 30 dni od ich przyjęcia.

(38) Wykorzystanie systemów AI do zdalnej identyfikacji biometrycznej osób fizycznych w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw nieuchronnie wiąże się z przetwarzaniem danych biometrycznych. Przepisy niniejszego rozporządzenia zakazujące, z zastrzeżeniem pewnych wyjątków, takiego wykorzystywania, a których podstawę stanowi art. 16 TFUE, powinny mieć zastosowanie jako *lex specialis* w odniesieniu do przepisów dotyczących przetwarzania danych biometrycznych zawartych w art. 10 dyrektywy (UE) 2016/680, regulując tym samym w sposób wyczerpujący takie wykorzystywanie i przetwarzanie wspomnianych danych biometrycznych. W związku z tym takie wykorzystywanie i przetwarzanie powinno być możliwe wyłącznie w zakresie, w jakim jest zgodne z ramami określonymi w niniejszym rozporządzeniu, przy czym wykorzystywanie takich systemów i przetwarzanie takich danych przez właściwe organy – gdy działają w celu ścigania przestępstw – w oparciu o przesłanki wymienione w art. 10 dyrektywy (UE) 2016/680 może mieć miejsce wyłącznie w granicach wyznaczonych przez te ramy. W tym kontekście niniejsze rozporządzenie nie ma na celu ustanowienia podstawy prawnej do przetwarzania danych osobowych na podstawie art. 8 dyrektywy (UE) 2016/680. Wykorzystywanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów innych niż ściganie przestępstw, w tym przez właściwe organy, nie powinno być jednak objęte

szczególnymi ramami dotyczącymi takiego wykorzystywania w celu ścigania przestępstw, określonymi w niniejszym rozporządzeniu. Takie wykorzystywanie do celów innych niż ściganie przestępstw nie powinno zatem podlegać wymogowi uzyskania zezwolenia na mocy niniejszego rozporządzenia ani obowiązującym szczegółowym przepisom prawa krajowego, które mogą stanowić podstawę ubiegania się o takie zezwolenie.

(39) Wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane z wykorzystaniem systemów AI do identyfikacji biometrycznej, inne niż w związku z wykorzystywaniem systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw zgodnie z przepisami niniejszego rozporządzenia, powinno pozostawać zgodne z wymogami wynikającymi z art. 10 dyrektywy (UE) 2016/680. Do celów innych niż ściganie przestępstw art. 9 ust. 1 rozporządzenia (UE) 2016/679 i art. 10 ust. 1 rozporządzenia (UE) 2018/1725 zakazują przetwarzania danych biometrycznych z uwzględnieniem ograniczonej liczby wyjątków określonych w tych artykułach. W ramach stosowania art. 9 ust. 1 rozporządzenia (UE) 2016/679 wykorzystywanie zdalnej identyfikacji biometrycznej do celów innych niż ściganie przestępstw było już przedmiotem decyzji zakazujących takiego wykorzystywania, wydawanych przez krajowe organy ochrony danych.

(40) Zgodnie z art. 6a Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i TFUE, Irlandia nie jest związana przepisami ustanowionymi w art. 5 ust. 1 akapit pierwszy lit. g) – w takim zakresie, w jakim dotyczy on wykorzystania systemów kategoryzacji biometrycznej w odniesieniu do działań w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w art. 5 ust. 1 akapit pierwszy lit. d) – w takim zakresie, w jakim dotyczy on wykorzystania systemów AI objętych tym przepisem, w art. 5 ust. 1 akapit pierwszy lit. h), art. 5 ust. 2–6 i art. 26 ust. 10 niniejszego rozporządzenia przyjętymi na podstawie art. 16 TFUE, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres stosowania części trzeciej tytuł V rozdziały 4 lub 5 TFUE, jeśli Irlandia nie jest związana przepisami Unii w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy zapewnić zgodność z przepisami ustanowionymi na podstawie art. 16 TFUE.

(41) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i TFUE, Dania nie jest związana przepisami określonymi w art. 5 ust. 1 akapit pierwszy lit. g) – w takim zakresie, w jakim dotyczy on wykorzystania systemów kategoryzacji biometrycznej w odniesieniu do działań w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w art. 5 ust. 1 akapit pierwszy lit. d) – w takim zakresie, w jakim dotyczy on wykorzystania systemów AI objętych tym przepisem, w art. 5 ust. 1 lit. h), art. 5 ust. 2- 6 i art. 26 ust. 10 niniejszego rozporządzenia przyjętymi na podstawie art. 16 TFUE, które dotyczą przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdziały 4 lub 5 TFUE, ani przepisy te nie mają do niej zastosowania.

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

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

(44) Istnieją poważne obawy co do podstaw naukowych systemów AI mających na celu rozpoznawanie emocji lub wyciąganie wniosków na temat emocji, zwłaszcza że wyrażanie emocji znacznie się różni w zależności od kultur i sytuacji, a nawet w przypadku pojedynczej osoby. Wśród głównych wad takich systemów znajdują się ograniczona wiarygodność, nieprecyzyjność i ograniczona możliwość uogólnienia.

W związku z tym systemy AI rozpoznające emocje lub zamiary osób fizycznych lub wyciągające wnioski na temat emocji lub zamiarów na podstawie danych biometrycznych tych osób mogą prowadzić do dyskryminacyjnych wyników i mogą naruszać prawa i wolności zainteresowanych osób. Biorąc pod uwagę brak równowagi sił w kontekście pracy lub edukacji, w połączeniu z inwazyjnym charakterem tych systemów, systemy takie mogą prowadzić do krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup. W związku z tym należy zakazać wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów AI przeznaczonych do wykrywania stanu emocjonalnego osób fizycznych w sytuacjach związanych z miejscem pracy i edukacją. Zakaz ten nie powinien obejmować systemów AI wprowadzanych do obrotu wyłącznie ze względów medycznych lub bezpieczeństwa, takich jak systemy przeznaczone do użytku terapeutycznego.

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

(46) Systemy AI wysokiego ryzyka powinny być wprowadzane do obrotu w Unii, oddawane do użytku lub wykorzystywane wyłącznie wówczas, gdy są zgodne z określonymi obowiązkowymi wymogami. Wymogi te powinny zapewniać, aby systemy AI wysokiego ryzyka dostępne w Unii lub takie, których wyniki są w inny sposób wykorzystywane w Unii, nie stwarzały niedopuszczalnego ryzyka dla istotnych interesów publicznych Unii uznanych w prawie Unii i przez to prawo chronionych. W oparciu o nowe ramy prawne, jak wyjaśniono w zawiadomieniu Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022"[20], ogólna zasada stanowi, że do jednego produktu można stosować więcej niż jeden akt prawny unijnego prawodawstwa harmonizacyjnego, taki jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745[21], rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746[22] lub dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady[23], ponieważ udostępnianie lub oddawanie do użytku może mieć miejsce tylko wtedy, gdy produkt jest zgodny z całością obowiązującego unijnego prawodawstwa harmonizacyjnego. Aby zapewnić spójność i uniknąć niepotrzebnych obciążeń administracyjnych lub kosztów, dostawcy produktu, który zawiera co najmniej jeden system AI wysokiego ryzyka, do którego stosuje się wymogi niniejszego rozporządzenia oraz unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku do niniejszego rozporządzenia, powinni mieć swobodę w zakresie decyzji operacyjnych dotyczących sposobu zapewnienia w optymalny sposób zgodności produktu zawierającego co najmniej jeden system AI ze wszystkimi mającymi zastosowanie wymogami unijnego prawodawstwa harmonizacyjnego. Jako systemy AI wysokiego ryzyka należy uznawać jedynie te systemy AI, które mają znaczący szkodliwy wpływ na zdrowie, bezpieczeństwo i prawa podstawowe osób w Unii, przy czym takie ograniczenie powinno minimalizować wszelkie potencjalne przeszkody w handlu międzynarodowym.

(47) Systemy AI mogą mieć niepożądany wpływ na zdrowie i bezpieczeństwo osób, w szczególności w przypadku gdy takie systemy funkcjonują jako związane z bezpieczeństwem elementy produktów. Zgodnie z celami unijnego prawodawstwa harmonizacyjnego, polegającymi na ułatwieniu swobodnego przepływu produktów na rynku wewnętrznym oraz zapewnieniu, aby na rynek trafiały wyłącznie produkty bezpieczne i zgodne w pozostałym zakresie, istotne jest odpowiednie zapobieganie ryzyku dla bezpieczeństwa, które mogą być powodowane przez produkt jako całość ze względu na jego elementy cyfrowe, w tym systemy AI, a także ograniczanie tych zagrożeń. Na przykład coraz bardziej autonomiczne roboty, zarówno w kontekście działalności produkcyjnej, jak i świadczenia pomocy oraz opieki osobistej, powinny być w stanie bezpiecznie funkcjonować i wykonywać swoje funkcje w złożonych środowiskach. Podobnie w sektorze opieki zdrowotnej, w którym chodzi o szczególnie wysoką stawkę, jaką jest życie i zdrowie, coraz bardziej zaawansowane systemy diagnostyczne i systemy wspomagające decyzje podejmowane przez człowieka powinny być niezawodne i dokładne.

(48) Przy klasyfikowaniu systemu AI jako systemu wysokiego ryzyka zasadnicze znaczenie ma to, w jakim stopniu system AI wywiera niepożądany wpływ na prawa podstawowe chronione na mocy Karty. Do praw tych należą prawo do godności człowieka, poszanowanie życia prywatnego i rodzinnego, ochrona danych osobowych, wolność wypowiedzi i informacji, wolność zgromadzania się i stowarzyszania się oraz prawo do niedyskryminacji, prawo do edukacji, ochrona konsumentów, prawa pracownicze, prawa osób z niepełnosprawnościami, równość płci, prawa własności intelektualnej, prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawo do obrony i domniemania niewinności, a także prawo do dobrej administracji. Oprócz tych praw należy podkreślić, że dzieciom przysługują szczególne prawa zapisane w art. 24 Karty oraz w Konwencji ONZ o prawach dziecka, szerzej rozwinięte w komentarzu ogólnym nr 25 w sprawie praw dziecka w środowisku cyfrowym zamieszczony w Konwencji ONZ o prawach dziecka, które to prawa wymagają uwzględnienia szczególnej wrażliwości dzieci oraz zapewnienia im takiej ochrony i opieki, jaka jest konieczna dla ich dobra. Podstawowe prawo do wysokiego poziomu ochrony środowiska zapisane w Karcie i wdrażane w strategiach politycznych Unii również należy uwzględnić w ocenie dotkliwości szkody, jaką może wyrządzić system AI, w tym w odniesieniu do zdrowia i bezpieczeństwa osób.

(49) W odniesieniu do systemów AI wysokiego ryzyka, które są związanymi z bezpieczeństwem elementami produktów lub systemów objętych zakresem stosowania rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008[24], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 167/2013[25], rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013[26], dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE[27], dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/797[28], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858[29], rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139[30] oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2144[31] lub które same są takimi produktami lub systemami, wskazane jest dokonanie zmian tych aktów w celu zapewnienia, aby Komisja, przyjmując wszelkie stosowne akty delegowane lub wykonawcze na podstawie wspomnianych aktów, uwzględniła – w oparciu o techniczną i regulacyjną charakterystykę każdego sektora oraz bez ingerowania w istniejące mechanizmy zarządzania, oceny zgodności i egzekwowania oraz w powołane na mocy tych aktów organy – obowiązkowe wymogi dotyczące systemów AI wysokiego ryzyka ustanowione w niniejszym rozporządzeniu.

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

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

(52) W odniesieniu do samodzielnych systemów AI, a mianowicie systemów AI wysokiego ryzyka inne niż te, które są związanymi z bezpieczeństwem elementami produktów lub które same są produktami, należy je klasyfikować jako systemy wysokiego ryzyka, jeżeli w związku z ich przeznaczeniem stwarzają one wysokie ryzyko szkody dla zdrowia i bezpieczeństwa lub praw podstawowych osób, biorąc pod uwagę zarówno dotkliwość potencjalnych szkód, jak i prawdopodobieństwo ich wystąpienia, oraz jeżeli są one wykorzystywane w szeregu ściśle określonych z góry obszarów wskazanych w niniejszym rozporządzeniu. Identyfikacja tych systemów opiera się na tej samej metodyce i kryteriach przewidzianych również w odniesieniu do wszelkich przyszłych zmian w wykazie systemów AI wysokiego ryzyka, do przyjmowania których – w drodze aktów delegowanych – powinna być uprawniona Komisja, aby uwzględniać szybkie tempo rozwoju technologicznego, a także potencjalne zmiany w wykorzystaniu systemów AI.

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

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

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

(55) W odniesieniu do zarządzania infrastrukturą krytyczną i jej działania jako systemy wysokiego ryzyka należy klasyfikować systemy AI, które są przeznaczone do wykorzystania jako związane z bezpieczeństwem elementy procesów zarządzania i działania w przypadku krytycznej infrastruktury cyfrowej wymienionej w pkt 8 załącznika do dyrektywy (UE) 2022/2557, ruchu drogowego i zaopatrzenia w wodę, gaz, ciepło i energię elektryczną, ponieważ ich awaria lub nieprawidłowe działanie mogą stworzyć ryzyko dla życia i zdrowia osób na dużą skalę i prowadzić do znacznych zakłóceń w zwykłym prowadzeniu działalności społecznej i gospodarczej. Związane z bezpieczeństwem elementy infrastruktury krytycznej, w tym krytycznej infrastruktury cyfrowej, to systemy, które są wykorzystywane do bezpośredniej ochrony fizycznej integralności infrastruktury krytycznej lub zdrowia i bezpieczeństwa osób i mienia, ale które nie są konieczne do funkcjonowania systemu. Awaria lub nieprawidłowe działanie takich elementów mogą bezpośrednio prowadzić do ryzyka dla fizycznej integralności infrastruktury krytycznej, a co za tym idzie, do ryzyka dla zdrowia i bezpieczeństwa osób i mienia. Elementów przeznaczonych wyłącznie do celów cyberbezpieczeństwa nie należy kwalifikować jako związanych z bezpieczeństwem elementów.

Przykładami związanych z bezpieczeństwem elementów takiej infrastruktury krytycznej są systemy monitorowania ciśnienia wody lub systemy sterowania alarmem przeciwpożarowym w centrach przetwarzania danych w chmurze (ang. cloud computing centres).

(56) Wdrażanie systemów AI w edukacji jest ważne, by promować wysokiej jakości kształcenie i szkolenie cyfrowe oraz by umożliwić wszystkim osobom uczącym się i nauczycielom zdobywanie niezbędnych umiejętności i kompetencji cyfrowych, w tym umiejętności korzystania z mediów, i krytycznego myślenia oraz dzielenie się tymi umiejętnościami i kompetencjami, z myślą o aktywnym udziale w gospodarce, społeczeństwie i procesach demokratycznych. Jako systemy AI wysokiego ryzyka należy natomiast zaklasyfikować systemy AI wykorzystywane w obszarze edukacji lub szkolenia zawodowego – w szczególności przeznaczone do celów podejmowania decyzji o dostępie lub przyjęciu do instytucji edukacyjnych i instytucji szkolenia zawodowego lub programów edukacyjnych lub szkolenia zawodowego na wszystkich poziomach lub do przydzielania osób do tych instytucji lub programów, do oceniania wyników nauki osób, do oceniania odpowiedniego poziomu wykształcenia i istotnego oddziaływania na poziom wykształcenia i szkolenia, jaki dana osoba fizyczna otrzyma lub do jakiego będzie mogła mieć dostęp, lub do monitorowania i wykrywania zabronionego zachowania uczniów podczas testów – ponieważ systemy te mogą decydować o przebiegu kształcenia i kariery zawodowej danej osoby, a tym samym mogą wpływać na jej zdolność do zapewnienia sobie źródła utrzymania. Takie systemy, jeżeli są niewłaściwie zaprojektowane i wykorzystywane, mogą być szczególnie inwazyjne i naruszać prawo do kształcenia i szkolenia, a także prawo do niedyskryminacji oraz mogą utrwalać historyczne wzorce dyskryminacji, na przykład wobec kobiet, niektórych grup wiekowych, osób z niepełnosprawnościami lub osób o określonym pochodzeniu rasowym lub etnicznym bądź określonej orientacji seksualnej.

(57) Systemy AI wykorzystywane w obszarze zatrudnienia, zarządzania pracownikami i dostępu do samozatrudnienia, w szczególności do rekrutacji i wyboru kandydatów, do podejmowania decyzji mających wpływ na warunki stosunków pracy, decyzji o awansie i rozwiązaniu umownego stosunku pracy, do spersonalizowanego przydzielania zadań w oparciu o indywidualne zachowania, cechy osobowości lub charakter i do monitorowania lub oceny osób pozostających w umownych stosunkach pracy, należy również zaklasyfikować jako systemy wysokiego ryzyka, ponieważ systemy te mogą w znacznym stopniu wpływać na przyszłe perspektywy zawodowe, źródła utrzymania tych osób i prawa pracownicze. Odpowiednie umowne stosunki pracy powinny w znaczący sposób obejmować pracowników i osoby pracujące za pośrednictwem platform internetowych, o czym mowa w programie prac Komisji na 2021 r. W całym procesie rekrutacji oraz w ramach oceniania, awansowania lub utrzymywania na stanowisku osób pozostających w umownych stosunkach pracy systemy takie mogą utrwalać historyczne wzorce dyskryminacji, na przykład wobec kobiet, niektórych grup wiekowych, osób z niepełnosprawnościami lub osób o określonym pochodzeniu rasowym lub etnicznym lub o określonej orientacji seksualnej. Systemy AI wykorzystywane do monitorowania wydajności i zachowania takich osób mogą również podważać ich prawa podstawowe w zakresie ochrony danych i prywatności.

(58) Innym obszarem, w którym wykorzystanie systemów AI wymaga szczególnej uwagi, jest dostęp do niektórych podstawowych usług i świadczeń prywatnych i publicznych niezbędnych ludziom do pełnego uczestnictwa w życiu społecznym lub do poprawy poziomu życia oraz korzystanie z tych usług i świadczeń. W szczególności osoby fizyczne ubiegające się o podstawowe świadczenia i usługi w ramach pomocy publicznej lub korzystające z takich świadczeń i usług zapewnianych przez organy publiczne, a mianowicie usług opieki zdrowotnej, świadczeń z zabezpieczenia społecznego, usług społecznych zapewniających ochronę w przypadkach takich jak macierzyństwo, choroba, wypadki przy pracy, zależność lub podeszły wiek oraz utrata zatrudnienia, a także z pomocy społecznej i mieszkaniowej, są zazwyczaj zależne od tych świadczeń i usług oraz znajdują się w słabszym położeniu względem odpowiedzialnych organów. Jeżeli systemy AI są wykorzystywane do ustalenia, czy organy powinny przyznać takie świadczenia i usługi, odmówić ich, ograniczyć je, cofnąć lub odzyskać, w tym do stwierdzenia, czy świadczeniobiorcy są w świetle prawa uprawnieni do takich świadczeń lub usług, systemy te mogą mieć znaczący wpływ na źródła utrzymania osób i mogą naruszać ich prawa podstawowe, takie jak prawo do ochrony socjalnej, niedyskryminacji, godności człowieka lub skutecznego środka prawnego i w związku z tym systemy te należy zaklasyfikować jako systemy wysokiego ryzyka. Niniejsze rozporządzenie nie powinno jednak utrudniać rozwoju i stosowania innowacyjnych rozwiązań w administracji publicznej, która może odnieść korzyści z powszechniejszego wykorzystywania zgodnych i bezpiecznych systemów AI, pod warunkiem że systemy te nie stwarzają wysokiego ryzyka dla osób prawnych i fizycznych. Ponadto jako systemy wysokiego ryzyka należy zaklasyfikować systemy AI wykorzystywane do przeprowadzania scoringu kredytowego lub oceny zdolności kredytowej osób fizycznych, ponieważ systemy te decydują o dostępie tych osób do zasobów finansowych lub podstawowych usług, takich jak mieszkalnictwo, energia elektryczna i usługi telekomunikacyjne. Systemy AI wykorzystywane do tych celów mogą prowadzić do dyskryminacji osób lub grup i mogą utrwalać historyczne wzorce dyskryminacji, takie jak dyskryminacja ze względu na pochodzenie rasowe lub etniczne, płeć, niepełnosprawność, wiek, orientację seksualną, lub mogą powodować powstawanie nowych rodzajów dyskryminacji. Za systemy

wysokiego ryzyka na mocy niniejszego rozporządzenia nie należy jednak uznawać systemów AI przewidzianych w prawie Unii do celów wykrywania oszustw w ramach oferowania usług finansowych oraz do celów ostrożnościowych do obliczania wymogów kapitałowych instytucji kredytowych i zakładów ubezpieczeń. Ponadto systemy AI przeznaczone do przeprowadzania oceny ryzyka w przypadku ubezpieczenia zdrowotnego i na życie dla osób fizycznych i ustalania cen tych ubezpieczeń mogą mieć również znaczący wpływ na źródła utrzymania osób, a jeżeli nie są odpowiednio zaprojektowane, rozwinięte i wykorzystywane, mogą naruszać ich prawa podstawowe i prowadzić do poważnych konsekwencji dla życia i zdrowia ludzi, w tym wykluczenia finansowego i dyskryminacji. Wreszcie systemy AI przeznaczone do przeprowadzania oceny i klasyfikowania zgłoszeń alarmowych dokonywanych przez osoby fizyczne lub do wysyłania lub ustalania priorytetów w wysyłaniu służb pierwszej pomocy, w tym policji, straży pożarnej i pomocy medycznej, a także w ramach systemów oceny stanu zdrowia pacjentów w nagłych wypadkach, należy zaklasyfikować jako systemy wysokiego ryzyka, ponieważ służą one do podejmowania decyzji o krytycznym znaczeniu dla życia i zdrowia osób oraz ich mienia.

(59) Ze względu na rolę i odpowiedzialność organów ścigania ich działania związane z niektórymi rodzajami wykorzystania systemów AI charakteryzują się znacznym brakiem równowagi sił i mogą prowadzić do objęcia osoby fizycznej nadzorem, do jej aresztowania lub pozbawienia wolności, jak również do zaistnienia innego niepożądanego wpływu na prawa podstawowe zagwarantowane w Karcie. W szczególności jeżeli system AI nie jest trenowany z wykorzystaniem danych wysokiej jakości, nie spełnia odpowiednich wymogów pod względem skuteczności jego działania, dokładności lub solidności lub nie został odpowiednio zaprojektowany i przetestowany przed wprowadzeniem do obrotu lub oddaniem do użytku w inny sposób, może on wskazywać osoby w sposób dyskryminacyjny lub w inny nieprawidłowy lub niesprawiedliwy sposób. Ponadto korzystanie z istotnych procesowych praw podstawowych, takich jak prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, jak również prawo do obrony i domniemania niewinności, może być utrudnione, w szczególności w przypadku gdy takie systemy AI nie są w wystarczającym stopniu przejrzyste, wyjaśnialne i udokumentowane. W związku z tym szereg systemów AI przeznaczonych do wykorzystania w kontekście ścigania przestępstw, w których dokładność, wiarygodność i przejrzystość są szczególnie ważne dla uniknięcia niepożądanego wpływu, zachowania zaufania publicznego oraz zapewnienia odpowiedzialności i skutecznego dochodzenia roszczeń, należy klasyfikować jako systemy wysokiego ryzyka, o ile ich wykorzystanie jest dozwolone zgodnie z właściwymi przepisami prawa Unii i prawa krajowego. Ze względu na charakter działań i związane z nimi ryzyko do takich systemów AI wysokiego ryzyka należy zaliczyć w szczególności systemy AI przeznaczone do wykorzystywania przez organy ścigania lub w ich imieniu lub przez instytucje, organy i jednostki organizacyjne Unii w ramach wsparcia udzielanego organom ścigania w zakresie oceny ryzyka, że osoba fizyczna stanie się ofiarą przestępstwa, takie jak wariografy i podobne narzędzia, do oceny wiarygodności dowodów podczas prowadzenia postępowań przygotowawczych w sprawie przestępstw lub ich ścigania oraz, o ile nie jest to zakazane na mocy niniejszego rozporządzenia, do oceny ryzyka popełnienia przestępstwa lub ponownego popełnienia przestępstwa przez osobę fizyczną niewyłącznie na podstawie profilowania osób fizycznych lub oceny cech osobowości i charakteru lub wcześniejszego zachowania przestępnego osób fizycznych lub grup, do profilowania w trakcie wykrywania przestępstw, prowadzenia postępowań przygotowawczych w ich sprawie lub ich ścigania. Systemów AI przeznaczonych specjalnie do wykorzystania w postępowaniach administracyjnych prowadzonych przez organy podatkowe i celne, jak również przez jednostki analityki finansowej wykonujące zadania administracyjne dotyczące analizy informacji na podstawie przepisów prawa Unii dotyczących przeciwdziałania praniu pieniędzy, nie należy zaklasyfikować jako systemów AI wysokiego ryzyka wykorzystywanych przez organy ścigania do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania. Wykorzystanie narzędzi sztucznej inteligencji przez organy ścigania i inne odpowiednie organy nie powinno stać się czynnikiem powodującym nierówności lub wykluczenie. Nie należy ignorować wpływu wykorzystania narzędzi AI na prawo podejrzanych do obrony, w szczególności na trudności w uzyskaniu istotnych informacji na temat funkcjonowania tych systemów oraz wynikające z tego trudności w kwestionowaniu dostarczanych przez nie wyników przed sądem, w szczególności przez osoby fizyczne objęte postępowaniem przygotowawczym.

(60) Systemy AI wykorzystywane w zarządzaniu migracją, azylem i kontrolą graniczną mają wpływ na osoby, które często znajdują się w szczególnie trudnej sytuacji i które są zależne od rezultatów działań właściwych organów publicznych. Dokładność, niedyskryminujący charakter i przejrzystość systemów AI wykorzystywanych w tych kontekstach są zatem szczególnie istotne w celu zapewnienia poszanowania praw podstawowych osób, na które AI ma wpływ, w szczególności ich prawa do swobodnego przemieszczania się, niedyskryminacji, ochrony życia prywatnego i danych osobowych, ochrony międzynarodowej i dobrej administracji. O ile wykorzystanie systemów AI jest dozwolone zgodnie z właściwymi przepisami prawa Unii i prawa krajowego, za systemy wysokiego ryzyka należy zatem uznać systemy AI przeznaczone do wykorzystywania przez właściwe organy publiczne lub w ich imieniu lub przez instytucje, organy i jednostki organizacyjne Unii odpowiedzialne za wykonywanie zadań w dziedzinach zarządzania

migracją, azylem i kontrolą graniczną, takie jak wariografy i podobne narzędzia, gdy systemy te stosuje się do oceny niektórych rodzajów ryzyka stwarzanych przez osoby fizyczne wjeżdżające na terytorium państwa członkowskiego lub ubiegające się o wizę lub azyl, do wspierania właściwych organów publicznych przy rozpatrywaniu wniosków o udzielenie azylu, o wydanie wizy i dokumentów pobytowych oraz związanych z nimi skarg w odniesieniu do celu, jakim jest ustalenie kwalifikowalności osób fizycznych ubiegających się o przyznanie określonego statusu, w tym przy powiązanej ocenie wiarygodności dowodów, do celów wykrywania, rozpoznawania lub identyfikacji osób fizycznych w kontekście zarządzania migracją, azylem i kontrolą graniczną, z wyjątkiem weryfikacji dokumentów podróży. Systemy AI w obszarze zarządzania migracją, azylem i kontrolą graniczną objęte niniejszym rozporządzeniem powinny być zgodne z odpowiednimi wymogami proceduralnymi określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 810/2009[32], dyrektywie Parlamentu Europejskiego i Rady 2013/32/UE[33] i w innych właściwych przepisach prawa Unii. Wykorzystanie systemów AI w zarządzaniu migracją, azylem i kontrolą graniczną nie powinno w żadnym wypadku być wykorzystywane przez państwa członkowskie lub instytucje, organy i jednostki organizacyjne Unii jako sposób na obejście ich międzynarodowych zobowiązań wynikających z Konwencji ONZ dotyczącej statusu uchodźców sporządzonej w Genewie dnia 28 lipca 1951 r., zmienionej protokołem z dnia 31 stycznia 1967 r. Nie powinny być one również wykorzystywane w żaden sposób do naruszania zasady non-refoulement ani do odmawiania bezpiecznych i skutecznych legalnych sposobów wjazdu na terytorium Unii, w tym prawa do ochrony międzynarodowej.

(61) Niektóre systemy AI przeznaczone na potrzeby sprawowania wymiaru sprawiedliwości i procesów demokratycznych należy zaklasyfikować jako systemy wysokiego ryzyka, biorąc pod uwagę ich potencjalnie istotny wpływ na demokrację, praworządność, wolności osobiste, a także prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu. W szczególności, aby wyeliminować potencjalne ryzyko stronniczości, błędów i efektu czarnej skrzynki, jako systemy wysokiego ryzyka należy zakwalifikować systemy AI przeznaczone do wykorzystania przez organy wymiaru sprawiedliwości lub w ich imieniu, aby pomóc tym organom w poszukiwaniu i interpretacji faktów i prawa oraz w stosowaniu przepisów prawa do konkretnego stanu faktycznego. Systemy AI przeznaczone do wykorzystania w tych celach przez organy alternatywnego rozstrzygania sporów również należy uznać za systemy wysokiego ryzyka, jeżeli wyniki postępowania w sprawie alternatywnego rozstrzygania sporów wywołują skutki prawne dla stron. Wykorzystanie narzędzi AI może wspierać uprawnienia decyzyjne sędziów lub niezależność sądownictwa, ale nie powinno ich zastępować; podejmowanie ostatecznej decyzji musi pozostać działaniem kierowanym przez człowieka. Kwalifikacja systemów AI jako systemów AI wysokiego ryzyka nie powinna jednak rozciągać się na systemy AI przeznaczone do czysto pomocniczych czynności administracyjnych, które nie mają wpływu na faktyczne sprawowanie wymiaru sprawiedliwości w poszczególnych przypadkach, takich jak anonimizacja lub pseudonimizacja orzeczeń sądowych, dokumentów lub danych, komunikacja między członkami personelu, zadania administracyjne.

(62) Bez uszczerbku dla przepisów ustanowionych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/900[34] oraz aby zapobiec ryzyku nadmiernej zewnętrznej ingerencji w prawo do głosowania zapisane w art. 39 Karty oraz niepożądanemu wpływowi na demokrację i praworządność, systemy AI przeznaczone do wykorzystania, by wpływać na wynik wyborów lub referendum lub na zachowania wyborcze osób fizycznych podczas głosowania w wyborach lub referendach, należy zaklasyfikować jako systemy AI wysokiego ryzyka, z wyjątkiem systemów AI, na których wyniki osoby fizyczne nie są bezpośrednio narażone, takich jak narzędzia wykorzystywane do organizowania, optymalizacji i strukturyzowania kampanii politycznych z administracyjnego i logistycznego punktu widzenia.

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

(64) Aby ograniczyć ryzyko stwarzane przez systemy AI wysokiego ryzyka wprowadzone do obrotu lub oddawane do użytku oraz aby zapewnić wysoki poziom wiarygodności, należy stosować pewne obowiązkowe wymogi do systemów AI wysokiego ryzyka, z uwzględnieniem przeznaczenia systemu AI i kontekstu jego wykorzystania oraz zgodnie z systemem zarządzania ryzykiem, który ma zostać ustanowiony przez dostawcę. Środki przyjęte przez dostawców w celu zapewnienia zgodności z obowiązkowymi wymogami niniejszego rozporządzenia powinny uwzględniać powszechnie uznany stan wiedzy technicznej w zakresie AI, być proporcjonalne i skuteczne do osiągnięcia celów niniejszego rozporządzenia. W oparciu

o nowe ramy prawne, jak wyjaśniono w zawiadomieniu Komisji „Niebieski przewodnik – wdrażanie unijnych przepisów dotyczących produktów 2022", ogólna zasada stanowi, że do jednego produktu można stosować więcej niż jeden akt prawny unijnego prawodawstwa harmonizacyjnego, ponieważ udostępnianie lub oddawanie do użytku może mieć miejsce tylko wtedy, gdy produkt jest zgodny z całością obowiązującego unijnego prawodawstwa harmonizacyjnego. Zagrożenia związane z systemami AI objętymi wymogami niniejszego rozporządzenia dotyczą innych aspektów niż obowiązujące unijne prawodawstwo harmonizacyjne, w związku z czym wymogi niniejszego rozporządzenia uzupełnią obowiązujące unijne prawodawstwo harmonizacyjne. Na przykład maszyny lub wyroby medyczne zawierające system AI mogą stwarzać ryzyko, które nie zostało uwzględnione w zasadniczych wymogach w zakresie zdrowia i bezpieczeństwa ustanowionych w odpowiednim unijnym prawodawstwie harmonizacyjnym, ponieważ to prawo sektorowe nie reguluje ryzyka specyficznego dla systemów AI. Wymaga to jednoczesnego i komplementarnego stosowania różnych aktów ustawodawczych. Aby zapewnić spójność i uniknąć niepotrzebnych obciążeń administracyjnych i niepotrzebnych kosztów, dostawcy produktu, który zawiera co najmniej jeden system AI wysokiego ryzyka, do którego stosuje się wymogi niniejszego rozporządzenia i unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych, wymienionego w załączniku do niniejszego rozporządzenia, powinni mieć swobodę w zakresie decyzji operacyjnych dotyczących sposobu zapewnienia w optymalny sposób zgodności produktu zawierającego co najmniej jeden system AI ze wszystkimi mającymi zastosowanie wymogami unijnego prawodawstwa harmonizacyjnego. Swoboda ta może oznaczać na przykład decyzję dostawcy o włączeniu części niezbędnych procesów testowania i sprawozdawczości, informacji i dokumentacji wymaganych na mocy niniejszego rozporządzenia do już istniejącej dokumentacji i procedur wymaganych na mocy obowiązującego unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych i wymienionego w załączniku do niniejszego rozporządzenia. Nie powinno to w żaden sposób podważać spoczywającego na dostawcy obowiązku zapewnienia zgodności z wszystkimi mającymi zastosowanie wymogami.

(65) System zarządzania ryzykiem powinien obejmować ciągły, iteracyjny proces, który jest planowany i realizowany przez cały cykl życia systemu AI wysokiego ryzyka. Proces ten powinien mieć na celu identyfikację i ograniczenie istotnego ryzyka, jakie systemy AI stwarzają dla zdrowia, bezpieczeństwa i praw podstawowych. System zarządzania ryzykiem powinien podlegać regularnym przeglądom i aktualizacji, aby zapewnić jego stałą skuteczność oraz uzasadnienie i dokumentację wszelkich istotnych decyzji i działań podjętych zgodnie z niniejszym rozporządzeniem. Proces ten powinien zapewniać, aby dostawca identyfikował ryzyko lub niepożądany wpływ oraz wdrażał środki ograniczające znane i racjonalnie przewidywalne ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych związane z systemami AI w świetle ich przeznaczenia i dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, w tym możliwego ryzyka wynikającego z interakcji między systemem AI a środowiskiem, w którym ten system działa. W systemie zarządzania ryzykiem należy przyjąć najbardziej odpowiednie – w świetle aktualnego stanu wiedzy technicznej w dziedzinie AI – środki zarządzania ryzykiem. Przy określaniu najbardziej odpowiednich środków zarządzania ryzykiem dostawca powinien udokumentować i wyjaśnić dokonane wybory oraz, w stosownych przypadkach, zaangażować ekspertów i zewnętrzne zainteresowane strony. Identyfikując dające się racjonalnie przewidzieć niewłaściwe wykorzystanie systemów AI wysokiego ryzyka, dostawca powinien uwzględnić przypadki wykorzystania systemów AI, w odniesieniu do których można zasadnie oczekiwać, że będą one wynikać z łatwo przewidywalnego zachowania ludzkiego w kontekście szczególnych cech i wykorzystania danego systemu AI, chociaż takich przypadków wykorzystania nie przewidziano w przeznaczeniu danego systemu ani w jego instrukcji obsługi. Wszelkie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu AI wysokiego ryzyka zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, mogące powodować ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych, powinny zostać uwzględnione w instrukcji obsługi dostarczonej przez dostawcę. Ma to na celu zapewnienie, aby podmiot stosujący był ich świadomy i uwzględniał je przy korzystaniu z systemu AI wysokiego ryzyka. Określenie i wdrożenie – na podstawie niniejszego rozporządzenia – środków ograniczających ryzyko w odniesieniu do dającego się przewidzieć niewłaściwego wykorzystania nie powinno wymagać od dostawcy wprowadzenia szczególnego dodatkowego szkolenia, by zaradzić temu dającemu się przewidzieć niewłaściwemu wykorzystaniu. Zachęca się jednak dostawców do rozważenia takich dodatkowych środków szkoleniowych w celu ograniczenia dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, o ile będzie to konieczne i stosowne.

(66) Do systemów AI wysokiego ryzyka należy stosować wymogi dotyczące zarządzania ryzykiem, jakości i istotności wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji podmiotom stosującym, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Wymogi te są konieczne, aby skutecznie ograniczyć ryzyko dla zdrowia, bezpieczeństwa i praw podstawowych. Z uwagi na brak innych racjonalnie dostępnych

środków, które powodowałyby mniejsze ograniczenia w handlu, wymogi te nie stanowią nieuzasadnionych ograniczeń w handlu.

(67) Wysokiej jakości dane i dostęp do wysokiej jakości danych odgrywają kluczową rolę w ustanawianiu struktury i zapewnianiu skuteczności działania wielu systemów AI, w szczególności w przypadku stosowania technik obejmujących trenowanie modeli, w celu zapewnienia, aby system AI wysokiego ryzyka działał zgodnie z przeznaczeniem i bezpiecznie oraz aby nie stał się źródłem zakazanej przez prawo Unii dyskryminacji. Wysokiej jakości zbiory danych treningowych, walidacyjnych i testowych wymagają wdrożenia odpowiednich praktyk w zakresie administrowania i zarządzania danymi. Zbiory danych treningowych, walidacyjnych i testowych, w tym etykiety, powinny być adekwatne, wystarczająco reprezentatywne oraz w jak największym stopniu wolne od błędów i kompletne z punktu widzenia przeznaczenia systemu. Aby ułatwić zapewnienie zgodności z prawem Unii o ochronie danych, takim jak rozporządzenie (UE) 2016/679, praktyki w zakresie administrowania i zarządzania danymi powinny przewidywać, w przypadku danych osobowych, zapewnianie przejrzystości pierwotnego celu zbierania danych. Te zbiory danych powinny również charakteryzować się odpowiednimi właściwościami statystycznymi, w tym w odniesieniu do osób lub grup osób, wobec których system AI wysokiego ryzyka ma być wykorzystywany, ze szczególnym uwzględnieniem ograniczania ewentualnej stronniczości w zbiorach danych, która może mieć wpływ na zdrowie i bezpieczeństwo osób, negatywnie oddziaływać na prawa podstawowe lub prowadzić do dyskryminacji zakazanej na mocy prawa Unii, zwłaszcza w przypadku gdy dane wyjściowe wpływają na dane wejściowe wykorzystywane na potrzeby przyszłych operacji (sprzężenie zwrotne, ang. feedback loops). Stronniczość może być na przykład nieodłączną cechą źródłowych zbiorów danych, szczególnie jeżeli używa się danych historycznych lub wygenerowanych na etapie wdrażania systemów w warunkach rzeczywistych. Na wyniki generowane przez systemy AI może wpływać taka nieodłączna stronniczość, która z zasady stopniowo zwiększa się, a tym samym utrwala i pogłębia istniejącą dyskryminację, zwłaszcza w odniesieniu do osób należących do grup szczególnie wrażliwych, w tym grup rasowych lub etnicznych. Wymóg, aby zbiory danych były w jak największym stopniu kompletne i wolne od błędów, nie powinien wpływać na stosowanie technik ochrony prywatności w kontekście wdrażania i testowania systemów AI. W szczególności zbiory danych powinny uwzględniać – w zakresie wymaganym z uwagi na ich przeznaczenie – cechy, właściwości lub elementy, które są specyficzne dla określonego otoczenia geograficznego, kontekstualnego, behawioralnego lub funkcjonalnego, w którym dany system AI ma być wykorzystywany. Zgodność z wymogami związanymi z zarządzaniem danymi można zapewnić, korzystając z usług stron trzecich, które oferują certyfikowane usługi w zakresie zgodności, w tym weryfikację zarządzania danymi i integralności zbioru danych oraz praktyki w zakresie trenowania, walidacji i testowania danych, o ile zapewniona jest zgodność z wymogami dotyczącymi danych określonymi w niniejszym rozporządzeniu.

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

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

(70) W celu ochrony praw innych osób przed dyskryminacją, która może wynikać ze stronniczości systemów AI, dostawcy powinni wyjątkowo, w zakresie, w jakim jest to bezwzględnie konieczne do celów zapewnienia wykrywania i korygowania stronniczości w odniesieniu do systemów AI wysokiego

ryzyka – z zastrzeżeniem odpowiednich zabezpieczeń w zakresie podstawowych praw i wolności osób fizycznych oraz po spełnieniu wszystkich mających zastosowanie warunków ustanowionych w niniejszym rozporządzeniu, w uzupełnieniu warunków ustanowionych w rozporządzeniach (UE) 2016/679 i (UE) 2018/1725 oraz w dyrektywie (UE) 2016/680 – mieć możliwość przetwarzania również szczególnych kategorii danych osobowych w związku z istotnym interesem publicznym w rozumieniu art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679 i art. 10 ust. 2 lit. g) rozporządzenia (UE) 2018/1725.

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

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

(73) Systemy AI wysokiego ryzyka należy projektować i rozwijać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie, zapewniać, by ich wykorzystanie było zgodne z przeznaczeniem oraz zapewniać, aby skutki ich wykorzystania były uwzględniane w całym cyklu życia systemu. W tym celu przed wprowadzeniem systemu do obrotu lub oddaniem go do użytku dostawca systemu powinien określić odpowiednie środki związane z nadzorem ze strony człowieka. W szczególności, w stosownych przypadkach, takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka – operatora systemu, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru ze strony człowieka, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji. W stosownych przypadkach istotne jest także zapewnienie, aby systemy AI wysokiego ryzyka obejmowały mechanizmy udzielania wskazówek i informacji osobom fizycznym, którym powierzono nadzór ze strony człowieka, aby mogły one podejmować świadome decyzje, czy, kiedy i w jaki sposób należy interweniować w celu uniknięcia negatywnych konsekwencji lub ryzyka lub zatrzymać system, jeżeli nie działa on zgodnie z przeznaczeniem. Zważywszy na istotne konsekwencje dla osób w przypadku nieprawidłowego dopasowania przez niektóre systemy identyfikacji biometrycznej, należy wprowadzić wymóg sprawowania w odniesieniu

do tych systemów wzmocnionego nadzoru ze strony człowieka, tak aby podmiot stosujący nie mógł podejmować żadnych działań ani decyzji na podstawie identyfikacji wynikającej z systemu, dopóki nie została ona odrębnie zweryfikowana i potwierdzona przez co najmniej dwie osoby fizyczne. Osoby te mogą pochodzić z różnych podmiotów i mogą to być osoby obsługujące system lub z niego korzystające. Wymóg ten nie powinien powodować niepotrzebnych obciążeń ani opóźnień i powinno wystarczyć, że odrębne weryfikacje dokonywane przez różne osoby będą automatycznie rejestrowane w wygenerowanych przez system rejestrach zdarzeń. Biorąc pod uwagę specyfikę obszarów ścigania przestępstw, migracji, kontroli granicznej i azylu, wymóg ten nie powinien mieć zastosowania, jeżeli na mocy prawa Unii lub prawa krajowego stosowanie tego wymogu uznaje się za nieproporcjonalne.

(74) Systemy AI wysokiego ryzyka powinny działać w sposób spójny w całym cyklu życia i charakteryzować się odpowiednim poziomem dokładności, solidności i cyberbezpieczeństwa – w świetle ich przeznaczenia i zgodnie z powszechnie uznawanym stanem wiedzy technicznej. Komisję oraz odpowiednie organizacje i zainteresowane strony zachęca się, by należycie uwzględniały ograniczanie ryzyka i negatywnych skutków związanych z systemem AI. Oczekiwany poziom wskaźników skuteczności działania należy zadeklarować w załączonej instrukcji obsługi. Dostawców wzywa się, by przekazywali te informacje podmiotom stosującym w jasny i łatwo zrozumiały sposób, wolny od dwuznaczności i stwierdzeń wprowadzających w błąd. Prawo Unii dotyczące metrologii prawnej, w tym dyrektywy Parlamentu Europejskiego i Rady 2014/31/UE[35] i 2014/32/UE[36], ma na celu zapewnienie dokładności pomiarów oraz wspieranie przejrzystości i uczciwości transakcji handlowych. W tym kontekście, we współpracy z odpowiednimi zainteresowanymi stronami i organizacjami, takimi jak organy ds. metrologii i organy ds. analizy porównawczej, Komisja powinna w stosownych przypadkach zachęcać do opracowywania poziomów odniesienia i metod pomiaru dotyczących systemów AI. Komisja powinna przy tym współpracować z partnerami międzynarodowymi pracującymi nad metrologią i odpowiednimi wskaźnikami pomiarowymi związanymi z AI oraz uwzględniać ich działania.

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

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

(77) Bez uszczerbku dla wymogów związanych z solidnością i dokładnością określonych w niniejszym rozporządzeniu systemy AI wysokiego ryzyka, które wchodzą w zakres stosowania rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, zgodnie z tym rozporządzeniem mogą wykazać zgodność z wymogami w zakresie cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu w drodze spełnienia zasadniczych wymogów w zakresie cyberbezpieczeństwa ustanowionych w tym rozporządzeniu. W przypadku gdy systemy AI wysokiego ryzyka spełniają zasadnicze wymogi rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, należy uznać, że wykazują zgodność z wymogami w zakresie cyberbezpieczeństwa ustanowionymi w niniejszym rozporządzeniu w zakresie, w jakim spełnienie tych wymogów wykazano w deklaracji zgodności UE lub w jej częściach wydanych zgodnie z tym rozporządzeniem. W tym celu ocena ryzyka dotyczącego cyberbezpieczeństwa związanego z produktem z elementami cyfrowymi, które zaklasyfikowano jako system AI wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, przeprowadzana na podstawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi,

powinna uwzględniać ryzyko dla cyberodporności systemu AI w odniesieniu do podejmowanych przez nieupoważnione osoby trzecie prób zmiany jego wykorzystania, zachowania lub skuteczności działania, w tym uwzględniać charakterystyczne dla AI słabe punkty, takie jak ryzyko zatruwania danych lub ataki kontradyktoryjne, a także, w stosownych przypadkach, uwzględniać ryzyko dla praw podstawowych zgodnie z wymogami niniejszego rozporządzenia.

(78) Procedura oceny zgodności przewidziana w niniejszym rozporządzeniu powinna mieć zastosowanie do zasadniczych wymogów w zakresie cyberbezpieczeństwa produktu z elementami cyfrowymi objętego rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zaklasyfikowanego jako system AI wysokiego ryzyka na podstawie niniejszego rozporządzenia. Zasada ta nie powinna jednak powodować zmniejszenia niezbędnego poziomu ufności w odniesieniu do produktów krytycznych z elementami cyfrowymi objętych rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi. W związku z tym, na zasadzie odstępstwa od tej zasady, systemy AI wysokiego ryzyka, które wchodzą w zakres niniejszego rozporządzenia i są również kwalifikowane jako ważne i krytyczne produkty z elementami cyfrowymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i do których ma zastosowanie procedura oceny zgodności oparta na kontroli wewnętrznej określona w załączniku do niniejszego rozporządzenia, podlegają przepisom dotyczącym oceny zgodności zawartym w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi w zakresie, w jakim dotyczy to zasadniczych wymogów w zakresie cyberbezpieczeństwa określonych w tym rozporządzeniu. W tym przypadku do wszystkich pozostałych aspektów objętych niniejszym rozporządzeniem należy stosować odpowiednie przepisy dotyczące oceny zgodności opierającej się na kontroli wewnętrznej określone w załączniku do niniejszego rozporządzenia. By wykorzystać wiedzę teoretyczną i fachową ENISA w zakresie polityki cyberbezpieczeństwa i w oparciu o zadania powierzone ENISA na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881[37], Komisja powinna współpracować z ENISA w kwestiach związanych z cyberbezpieczeństwem systemów AI.

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

(80) Jako sygnatariusze Konwencji ONZ o prawach osób niepełnosprawnych Unia i państwa członkowskie są prawnie zobowiązane do ochrony osób z niepełnosprawnościami przed dyskryminacją i do propagowania ich równości, do zapewnienia im dostępu na równych zasadach z innymi osobami do technologii i systemów informacyjno-komunikacyjnych oraz do zapewnienia poszanowania ich prywatności. Z uwagi na rosnące znaczenie i wykorzystanie systemów sztucznej inteligencji stosowanie zasad projektowania uniwersalnego do wszystkich nowych technologii i usług powinno zapewniać pełny i równy dostęp dla wszystkich osób, których potencjalnie dotyczą technologie AI lub które je stosują, w tym osób z niepełnosprawnościami, w sposób uwzględniający w pełni ich przyrodzoną godność i różnorodność. Istotne jest zatem, aby dostawcy zapewniali pełną zgodność z wymogami dostępności, w tym z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/2102[38] i dyrektywą (UE) 2019/882. Dostawcy powinni zapewnić zgodność z tymi wymogami już na etapie projektowania. W związku z tym w projektowaniu systemu AI wysokiego ryzyka należy w jak największym stopniu uwzględnić niezbędne środki.

(81) Dostawca powinien ustanowić solidny system zarządzania jakością, zapewnić przeprowadzenie wymaganej procedury oceny zgodności, sporządzić odpowiednią dokumentację i ustanowić solidny system monitorowania po wprowadzeniu do obrotu. Dostawcy systemów AI wysokiego ryzyka, którzy podlegają obowiązkom dotyczącym systemów zarządzania jakością na mocy odpowiednich sektorowych przepisów prawa Unii, powinni mieć możliwość włączenia elementów systemu zarządzania jakością przewidzianego w niniejszym rozporządzeniu do istniejącego systemu zarządzania jakością przewidzianego w innych sektorowych przepisach prawa Unii. Komplementarność między niniejszym rozporządzeniem a obowiązującymi sektorowymi przepisami prawa Unii powinna być również brana pod uwagę w przyszłych działaniach normalizacyjnych lub wytycznych przyjmowanych przez Komisję. Organy publiczne, które oddają do użytku systemy AI wysokiego ryzyka do celów własnych, mogą – w ramach przyjętego, odpowiednio, na poziomie krajowym lub regionalnym systemu zarządzania jakością – przyjąć i wdrożyć zasady dotyczące systemu zarządzania jakością, z uwzględnieniem specyfiki sektora oraz kompetencji i organizacji danego organu publicznego.

(82) W celu umożliwienia egzekwowania przepisów niniejszego rozporządzenia i stworzenia równych warunków działania dla operatorów, a także uwzględniając różne formy udostępniania produktów cyfrowych, należy zapewnić, aby w każdych okolicznościach osoba, która ma miejsce zamieszkania lub siedzibę w Unii, była w stanie przekazać organom wszystkie niezbędne informacje dotyczące zgodności danego systemu AI. W związku z tym dostawcy mający miejsce zamieszkania lub siedzibę w państwach trzecich

przed udostępnieniem swoich systemów AI w Unii powinni ustanowić – na podstawie pisemnego pełnomocnictwa – upoważnionego przedstawiciela mającego miejsce zamieszkania lub siedzibę w Unii. Ten upoważniony przedstawiciel odgrywa kluczową rolę w zapewnianiu zgodności systemów AI wysokiego ryzyka wprowadzanych do obrotu lub oddawanych do użytku w Unii przez dostawców, którzy nie mają miejsca zamieszkania lub siedziby w Unii, oraz w pełnieniu funkcji ich osoby kontaktowej mającej miejsce zamieszkania lub siedzibę w Unii.

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

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

(85) Systemy AI ogólnego przeznaczenia mogą być wykorzystywane jako samodzielne systemy AI wysokiego ryzyka lub stanowić element innych systemów AI wysokiego ryzyka. W związku z tym z uwagi na ich szczególny charakter i aby zapewnić sprawiedliwy podział odpowiedzialności w całym łańcuchu wartości AI, dostawcy takich systemów, niezależnie od tego, czy ich mogą być one wykorzystywane jako systemy AI wysokiego ryzyka przez innych dostawców czy jako elementy systemów AI wysokiego ryzyka, powinni ściśle współpracować – o ile niniejsze rozporządzenie nie stanowi inaczej – z dostawcami odpowiednich systemów AI wysokiego ryzyka, aby umożliwić im spełnianie odpowiednich obowiązków ustanowionych w niniejszym rozporządzeniu, oraz z właściwymi organami ustanowionymi na podstawie niniejszego rozporządzenia.

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

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

(88) W całym łańcuchu wartości AI wiele podmiotów często dostarcza systemy AI, narzędzia i usługi, ale również elementy lub procesy, które są włączane przez dostawcę do systemu AI w różnych celach, w tym trenowania modelu, retrenowania modelu, testowania i oceny modelu, integracji z oprogramowaniem lub innych aspektów rozwoju modelu. Podmioty te mają do odegrania ważną rolę w łańcuchu wartości w stosunku do dostawcy systemu AI wysokiego ryzyka, z którym to systemem zintegrowane są ich systemy AI, narzędzia, usługi, elementy lub procesy; podmioty te powinny zapewnić temu dostawcy na podstawie pisemnej umowy niezbędne informacje, zdolności, dostęp techniczny i inną pomoc

w oparciu o powszechnie uznany stan wiedzy technicznej, aby umożliwić dostawcy pełne spełnienie obowiązków ustanowionych w niniejszym rozporządzeniu, bez uszczerbku dla ich własnych praw własności intelektualnej lub tajemnic przedsiębiorstwa.

(89) Strony trzecie udostępniające publicznie narzędzia, usługi, procesy lub elementy AI, inne niż modele AI ogólnego przeznaczenia, nie powinny być zobowiązane do zapewnienia zgodności z wymogami dotyczącymi odpowiedzialności w całym łańcuchu wartości AI, w szczególności wobec dostawcy, który je wykorzystał lub zintegrował, jeżeli te narzędzia, usługi, procesy lub elementy AI są udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania. Należy zachęcać twórców narzędzi, usług, procesów lub elementów AI, innych niż modele AI ogólnego przeznaczenia, które są udostępniane na bezpłatnej licencji otwartego oprogramowania, do wdrażania powszechnie przyjętych praktyk w zakresie dokumentacji, takich jak karta modelu i karta charakterystyki, jako sposobu na przyspieszenie wymiany informacji w całym łańcuchu wartości AI, co umożliwi promowanie godnych zaufania systemów AI w Unii.

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

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

(92) Niniejsze rozporządzenie pozostaje bez uszczerbku dla obowiązków pracodawców w zakresie informowania pracowników lub ich przedstawicieli i konsultowania się z nimi na podstawie prawa Unii o prawa krajowego oraz unijnej lub krajowej praktyki, w tym dyrektywy 2002/14/WE Parlamentu Europejskiego i Rady[39], na temat decyzji o oddaniu do użytku lub korzystaniu z systemów AI. Nadal konieczne jest zapewnienie pracownikom i ich przedstawicielom informacji na temat planowanego wdrożenia systemów AI wysokiego ryzyka w miejscu pracy, w przypadku gdy warunki dotyczące tych obowiązków w zakresie informowania lub informowania i przeprowadzania konsultacji określone w innych instrumentach prawnych nie są spełnione. Ponadto takie prawo do informacji ma charakter pomocniczy i konieczny w stosunku do leżącego u podstaw niniejszego rozporządzenia celu, jakim jest ochrona praw podstawowych. W związku z tym w niniejszym rozporządzeniu należy ustanowić wymóg informowania w tym zakresie, nie naruszając żadnych istniejących praw pracowników.

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

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

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

(96) Aby skutecznie zapewnić ochronę praw podstawowych, podmioty stosujące systemy AI wysokiego ryzyka będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne i podmioty stosujące niektóre systemy AI wysokiego ryzyka wymienione w załączniku do niniejszego rozporządzenia, tacy jak podmioty bankowe lub ubezpieczeniowe, powinni przed wprowadzeniem tych systemów do użytku przeprowadzić ocenę skutków dla praw podstawowych. Usługi o charakterze publicznym ważne dla osób fizycznych mogą być również świadczone przez podmioty prywatne. Podmioty prywatne świadczące takie usługi publiczne działają w powiązaniu z zadaniami świadczonymi w interesie publicznym, takimi jak edukacja, opieka zdrowotna, usługi społeczne, mieszkalnictwo, sprawowanie wymiaru sprawiedliwości. Celem oceny skutków dla praw podstawowych jest zidentyfikowanie przez podmiot stosujący konkretnych rodzajów ryzyka dla praw osób fizycznych lub grup osób fizycznych, na które AI może mieć wpływ, oraz określenie środków, które należy podjąć w przypadku urzeczywistnienia się tego ryzyka. Ocena skutków powinna być przeprowadzana przed wdrożeniem systemu AI wysokiego ryzyka i powinna być aktualizowana, gdy podmiot stosujący uzna, że którykolwiek z istotnych czynników uległ zmianie. W ocenie skutków należy określić odpowiednie procesy podmiotu stosującego, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem; powinna ona przedstawiać informacje o okresie, w którym system ma być wykorzystywany, i o częstotliwości jego wykorzystania, a także opis konkretnych kategorii osób fizycznych i grup, na które AI może mieć wpływ w tym konkretnym kontekście wykorzystania. Ocena powinna również obejmować określenie szczególnego ryzyka szkody, które może mieć wpływ na prawa podstawowe tych osób lub grup. Przeprowadzając tę ocenę, podmiot stosujący powinien uwzględnić informacje istotne dla właściwej oceny skutków, w tym między innymi informacje podane przez dostawcę systemu AI wysokiego ryzyka w instrukcji obsługi. W świetle zidentyfikowanego ryzyka podmioty stosujące powinny określić środki, które należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym na przykład rozwiązania dotyczące zarządzania w tym konkretnym kontekście wykorzystania, np. dotyczące nadzoru ze strony człowieka zgodnie z instrukcją obsługi lub procedury rozpatrywania skarg i dochodzenia roszczeń, ponieważ mogą one odegrać zasadniczą rolę w ograniczaniu ryzyka dla praw podstawowych w konkretnych przypadkach wykorzystania. Po przeprowadzeniu tej oceny skutków podmiot stosujący powinien powiadomić odpowiedni organ nadzoru rynku. W stosownych przypadkach w celu zebrania odpowiednich informacji niezbędnych do przeprowadzenia oceny skutków podmioty stosujące system AI wysokiego ryzyka, w szczególności gdy systemy AI są wykorzystywane w sektorze publicznym, mogą angażować odpowiednie zainteresowane strony, w tym przedstawicieli grup osób, na które system AI może mieć wpływ, niezależnych ekspertów i organizacje społeczeństwa obywatelskiego w przeprowadzanie takich ocen skutków i opracowywanie środków, które należy wprowadzić w przypadku urzeczywistnienia się ryzyka. Europejski Urząd ds. Sztucznej Inteligencji (zwany dalej „Urzędem ds. AI") powinien opracować wzór kwestionariusza, by ułatwić zapewnienie zgodności przez podmioty stosujące i zmniejszyć obciążenia administracyjne dla tych podmiotów.

(97) Należy jasno zdefiniować pojęcie modeli AI ogólnego przeznaczenia i oddzielić je od pojęcia systemów AI, aby zapewnić pewność prawa. Definicja powinna opierać się na kluczowych cechach funkcjonalnych modelu AI ogólnego przeznaczenia, w szczególności na ogólnym charakterze i zdolności do kompetentnego wykonywania szerokiego zakresu różnych zadań. Modele te są zazwyczaj trenowane w oparciu o dużą ilość danych za pomocą różnych metod, takich jak uczenie się samodzielnie nadzorowane, nienadzorowane lub uczenie przez wzmacnianie. Modele AI ogólnego przeznaczenia mogą być wprowadzane

do obrotu na różne sposoby, w tym za pośrednictwem bibliotek, interfejsów programowania aplikacji (API), przez bezpośrednie pobieranie lub w wersji fizycznej. Modele te mogą być dalej zmieniane lub dostosowywane jako baza do tworzenia nowych modeli. Chociaż modele AI są zasadniczymi elementami systemów AI, nie stanowią same w sobie systemów AI. Aby model AI mógł stać się systemem AI należy dodać do niego dodatkowe elementy, takie jak na przykład interfejs użytkownika. Modele AI są zwykle zintegrowane z systemami AI i stanowią ich część. Niniejsze rozporządzenie ustanawia przepisy szczególne dotyczące modeli AI ogólnego przeznaczenia oraz modeli AI ogólnego przeznaczenia, które stwarzają ryzyko systemowe, a przepisy te powinny być stosowane również wtedy, gdy modele te są zintegrowane z systemem AI lub stanowią jego część. Należy rozumieć, że obowiązki dostawców modeli AI ogólnego przeznaczenia powinny mieć zastosowanie od momentu wprowadzenia do obrotu modeli AI ogólnego przeznaczenia. W przypadku gdy dostawca modelu AI ogólnego przeznaczenia zintegruje własny model z własnym systemem AI, który jest udostępniany na rynku lub oddany do użytku, model ten należy uznać za wprowadzony do obrotu i w związku z tym ustanowione w niniejszym rozporządzeniu obowiązki dotyczące modeli powinny nadal mieć zastosowanie obok obowiązków dotyczących systemów AI. Obowiązki ustanowione w odniesieniu do modeli nie powinny w żadnym przypadku mieć zastosowania, jeżeli model własny jest stosowany w czysto wewnętrznych procesach, które nie są niezbędne do dostarczania produktu lub usługi osobom trzecim, a prawa osób fizycznych nie są naruszone. Biorąc pod uwagę ich potencjalne znacząco negatywne skutki, modele AI ogólnego przeznaczenia z ryzykiem systemowym powinny zawsze podlegać odpowiednim obowiązkom ustanowionym w niniejszym rozporządzeniu. Definicja nie powinna obejmować modeli AI wykorzystywanych przed wprowadzeniem ich do obrotu wyłącznie do celów działalności badawczo-rozwojowej i tworzenia prototypów. Pozostaje to bez uszczerbku dla obowiązku zapewnienia zgodności z niniejszym rozporządzeniem w przypadku wprowadzenia do obrotu danego modelu w następstwie takiej działalności.

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

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

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

(101) Dostawcy modeli AI ogólnego przeznaczenia odgrywają szczególną rolę i ponoszą szczególną odpowiedzialność w całym łańcuchu wartości AI, ponieważ modele, które dostarczają, mogą stanowić podstawę szeregu systemów niższego szczebla, często dostarczanych przez dostawców niższego szczebla, które to systemy wymagają dobrego zrozumienia modeli i ich zdolności, zarówno by umożliwić integrację takich modeli z ich produktami, jak i by spełniać obowiązki ustanowione w niniejszym rozporządzeniu lub innych przepisach. W związku z tym należy ustanowić proporcjonalne środki w zakresie przejrzystości, w tym sporządzanie i aktualizowanie dokumentacji oraz dostarczanie informacji na temat modelu AI ogólnego przeznaczenia do wykorzystania przez dostawców niższego szczebla. Dostawca modelu AI ogólnego przeznaczenia powinien przygotować i aktualizować dokumentację techniczną w celu ud stępnienia jej na wniosek Urzędowi ds. AI i właściwym organom krajowym. Minimalny zbiór elementów do uwzględnienia w takiej dokumentacji należy określić w szczególnych załącznikach do niniejszego rozporządzenia. Komisja powinna być uprawniona do zmiany tych załączników w drodze aktów delegowanych w świetle postępu technicznego.

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

(103) Elementy AI na bezpłatnej licencji otwartego oprogramowania obejmują oprogramowanie i dane, w tym modele i modele AI ogólnego przeznaczenia, narzędzia, usługi lub procesy systemu AI. Elementy AI

na bezpłatnej licencji otwartego oprogramowania mogą być dostarczane za pośrednictwem różnych kanałów, w tym rozwijane w otwartych repozytoriach. Do celów niniejszego rozporządzenia elementy AI, które są dostarczane odpłatnie lub w inny sposób monetyzowane, w tym poprzez zapewnianie wsparcia technicznego lub innych usług związanych z elementem AI, w tym poprzez platformy oprogramowania, lub wykorzystywanie danych osobowych z powodów innych niż wyłącznie poprawa bezpieczeństwa, kompatybilności lub interoperacyjności oprogramowania, z wyjątkiem transakcji między mikroprzedsiębiorstwami, nie powinny korzystać ze zwolnień przewidzianych w odniesieniu do bezpłatnych i otwartych elementów AI. Fakt udostępniania elementów AI w otwartych repozytoriach nie powinien sam w sobie stanowić monetyzacji.

(104) Dostawcy modeli AI ogólnego przeznaczenia, które są udostępniane na podstawie bezpłatnej licencji otwartego oprogramowania i których parametry, w tym wagi, informacje o architekturze modelu oraz informacje na temat korzystania z modelu, są udostępniane publicznie, powinni podlegać zwolnieniom w odniesieniu do wymogów związanych z przejrzystością nałożonych na modele AI ogólnego przeznaczenia, chyba że można uznać, że modele te stwarzają ryzyko systemowe, w którym to przypadku fakt, że model jest przejrzysty i że towarzyszy mu licencja otwartego oprogramowania, nie powinien być uznawany za wystarczający powód zwolnienia ze spełnienia obowiązków ustanowionych w niniejszym rozporządzeniu. W każdym razie, biorąc pod uwagę, że udostępnianie modeli AI ogólnego przeznaczenia na podstawie bezpłatnej licencji otwartego oprogramowania niekoniecznie prowadzi do ujawnienia istotnych informacji na temat zbioru danych wykorzystywanego do trenowania lub dostrajania modelu oraz na temat sposobu zapewnienia tym samym zgodności z prawem autorskim, przewidziane w odniesieniu do modeli AI ogólnego przeznaczenia zwolnienie z obowiązku spełnienia wymogów związanych z przejrzystością nie powinno dotyczyć obowiązku sporządzenia streszczenia dotyczącego treści wykorzystywanych do trenowania modeli oraz obowiązku wprowadzenia polityki w celu zapewnienie zgodności z unijnym prawem autorskim, w szczególności w celu zidentyfikowania i zastosowania się do zastrzeżenia praw zgodnie z art. 4 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790[40].

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

(106) Dostawcy wprowadzający modele AI ogólnego przeznaczenia do obrotu w Unii powinni zapewnić, aby ustanowione w niniejszym rozporządzeniu odpowiednie obowiązki zostały spełnione. W tym celu dostawcy modeli AI ogólnego przeznaczenia powinni wprowadzić politykę w celu zapewnienia zgodności z prawem Unii dotyczącym prawa autorskiego i praw pokrewnych, w szczególności w celu identyfikacji i zastosowania się do zastrzeżenia praw wyrażonego przez podmioty uprawnione zgodnie z art. 4 ust. 3 dyrektywy (UE) 2019/790. Każdy dostawca wprowadzający do obrotu w Unii model AI ogólnego przeznaczenia powinien spełniać ten obowiązek, niezależnie od jurysdykcji, w której mają miejsce czynności regulowane prawem autorskim stanowiące podstawę trenowania tych modeli AI ogólnego przeznaczenia. Jest to konieczne do zapewnienia równych warunków działania dostawcom modeli AI ogólnego przeznaczenia, tak aby żaden dostawca nie mógł uzyskać przewagi konkurencyjnej na rynku Unii poprzez stosowanie niższych standardów praw autorskich niż normy przewidziane w Unii.

(107) W celu zwiększenia przejrzystości dotyczącej danych wykorzystywanych do pretrenowania i trenowania modeli AI ogólnego przeznaczenia, w tym w zakresie tekstów i danych chronionych prawem autorskim, właściwe jest, aby dostawcy takich modeli sporządzali i udostępniali publicznie wystarczająco szczegółowe streszczenie na temat treści wykorzystywanych do trenowania modelu AI ogólnego przeznaczenia. Przy należytym uwzględnieniu potrzeby ochrony tajemnic przedsiębiorstwa i poufnych informacji handlowych streszczenie to nie powinno skupiać się na szczegółach technicznych, lecz mieć zasadniczo kompleksowy charakter, aby ułatwić stronom mającym uzasadniony interes, w tym posiadaczom praw autorskich, wykonywanie i egzekwowanie ich praw wynikających z prawa Unii; streszczenie to powinno

więc na przykład wymieniać główne zbiory danych, które wykorzystano do trenowania modelu, takie jak duże prywatne lub publiczne bazy lub archiwa danych, oraz powinno zawierać opisowe wyjaśnienie innych wykorzystanych źródeł danych. Urząd ds. AI powinien zapewnić wzór streszczenia, który powinien być prosty i skuteczny oraz umożliwiać dostawcy przedstawienie wymaganego streszczenia w formie opisowej.

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

(109) Spełnianie obowiązków mających zastosowanie do dostawców modeli AI ogólnego przeznaczenia powinno być współmierne i proporcjonalne do rodzaju dostawcy modeli, z wyłączeniem konieczności ich spełnienia przez osoby, które rozwijają lub wykorzystują modele do celów pozazawodowych lub badań naukowych – osoby te należy jednak zachęcać do dobrowolnego spełniania tych wymogów. Bez uszczerbku dla unijnego prawa autorskiego spełnianie tych obowiązków powinno odbywać się przy należytym uwzględnieniu wielkości dostawcy i umożliwiać uproszczone sposoby spełnienia tych obowiązków przez MŚP, w tym przedsiębiorstwa typu startup, które nie powinny wiązać się z nadmiernymi kosztami i zniechęcać do korzystania z takich modeli. W przypadku zmiany lub dostrajania modelu obowiązki dostawców modeli AI ogólnego przeznaczenia powinny być ograniczone do tej zmiany lub dostrajania modelu, na przykład poprzez uzupełnienie już istniejącej dokumentacji technicznej o informacje na temat zmiany, w tym nowych źródeł danych treningowych, w celu spełnienia obowiązków związanych z łańcuchem wartości przewidzianych w niniejszym rozporządzeniu.

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

(111) Należy ustanowić metodykę klasyfikacji modeli AI ogólnego przeznaczenia jako modeli AI ogólnego przeznaczenia z ryzykiem systemowym. Ponieważ ryzyko systemowe wynika ze szczególnie wysokich zdolności, należy uznać, że model AI ogólnego przeznaczenia stwarza ryzyko systemowe, jeżeli wykazuje on zdolności dużego oddziaływania, oceniane na podstawie odpowiednich narzędzi technicznych i metodologii, lub jeżeli ze względu na swój zasięg ma znaczący wpływ na rynek wewnętrzny. Zdolności dużego oddziaływania w przypadku modeli AI ogólnego przeznaczenia oznaczają zdolności, które dorównują zdolnościom zapisanym w najbardziej zaawansowanych modelach AI ogólnego przeznaczenia lub je przewyższają. Pełny zakres zdolności danego modelu można lepiej zrozumieć po jego wprowadzeniu do obrotu lub w momencie, w którym podmioty stosujące wchodzą w interakcję z modelem. Zgodnie z aktualnym stanem wiedzy technicznej w momencie wejścia w życie niniejszego rozporządzenia jednym ze sposób przybliżonego określenia zdolności modelu jest łączna liczba obliczeń wykorzystanych do trenowania modelu AI ogólnego zastosowania mierzona w operacjach zmiennoprzecinkowych. Łączna liczba obliczeń wykorzystanych do trenowania obejmuje obliczenia stosowane w odniesieniu

do wszystkich działań i metod, które mają na celu zwiększenie zdolności modelu przed wdrożeniem, takich jak pretrenowanie, generowanie danych syntetycznych i dostrajanie. W związku z tym należy określić próg minimalny operacjach zmiennoprzecinkowych, który, jeżeli zostanie spełniony przez model AI ogólnego przeznaczenia, stwarza domniemanie, że model ten jest modelem AI ogólnego przeznaczenia z ryzykiem systemowym. Próg ten powinien być z czasem dostosowywany w celu odzwierciedlenia zmian technologicznych i przemysłowych, takich jak ulepszenia algorytmiczne lub większa wydajność sprzętu, i powinien zostać uzupełniony o poziomy odniesienia i wskaźniki dotyczące zdolności modelu. W tym celu Urząd ds. AI powinien współpracować ze środowiskiem naukowym, przemysłem, społeczeństwem obywatelskim i innymi ekspertami. Progi, a także narzędzia i poziomy odniesienia na potrzeby oceny zdolności dużego oddziaływania powinny zapewniać mocne podstawy przewidywania ogólnego charakteru, zdolności i związanego z nimi ryzyka systemowego modeli AI ogólnego przeznaczenia; mogą one uwzględniać sposób, w jaki model zostanie wprowadzony do obrotu lub liczbę użytkowników, na które model ten może mieć wpływ. Aby uzupełnić ten system, Komisja powinna mieć możliwość podejmowania indywidualnych decyzji w sprawie uznania modelu AI ogólnego przeznaczenia za model AI ogólnego przeznaczenia z ryzykiem systemowym, jeżeli okaże się, że zdolności lub wpływ takiego modelu są równoważne z tymi, na które wskazuje ustalony próg. Decyzję tę należy podjąć na podstawie ogólnej oceny kryteriów do celów uznawania modelu AI ogólnego przeznaczenia za model z ryzykiem systemowym, określonych w załączniku do niniejszego rozporządzenia, takich jak jakość lub wielkość zbioru danych treningowych, liczba użytkowników biznesowych i końcowych, format danych wejściowych i wyjściowych modelu, poziom autonomii i skalowalności lub narzędzia, do których ma dostęp. Na uzasadniony wniosek dostawcy, którego model został uznany za model AI ogólnego przeznaczenia z ryzykiem systemowym, Komisja powinna odnieść się do tego wniosku i może podjąć decyzję o ponownej ocenie, czy model AI ogólnego przeznaczenia nadal można uznać za stwarzający ryzyko systemowe.

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

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

(114) Dostawcy modeli AI ogólnego przeznaczenia stwarzających ryzyko systemowe powinni podlegać nie tylko obowiązkom nałożonym na dostawców modeli AI ogólnego przeznaczenia, ale także obowiązkom mającym na celu identyfikację i ograniczenie ryzyka systemowego oraz zapewnienie odpowiedniego poziomu ochrony cyberbezpieczeństwa, niezależnie od tego, czy modele te są dostarczane jako samodzielne modele czy wbudowane w system AI lub w produkt. Aby osiągnąć te cele, w niniejszym rozporządzeniu należy zobowiązać dostawców do przeprowadzania niezbędnych ocen modeli, w szczególności przed ich pierwszym wprowadzeniem do obrotu, w tym przeprowadzania wobec modeli i dokumentowania testów kontradyktoryjnych, również, w stosownych przypadkach, w drodze wewnętrznych lub niezależnych testów zewnętrznych. Ponadto dostawcy modeli AI ogólnego przeznaczenia z ryzykiem systemowym powinni stale oceniać i ograniczać ryzyko systemowe, w tym na przykład poprzez

wprowadzanie strategii zarządzania ryzykiem, takich jak procesy rozliczalności i zarządzania, wdrażanie monitorowania po wprowadzeniu do obrotu, podejmowanie odpowiednich środków w całym cyklu życia modelu oraz współpracę z odpowiednimi podmiotami w całym łańcuchu wartości AI.

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

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

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

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

(119) Biorąc pod uwagę szybkie tempo innowacji i rozwój technologiczny usług cyfrowych objętych różnymi instrumentami prawa Unii, w szczególności mając na uwadze wykorzystanie tych usług oraz zrozumienie,

kto jest ich odbiorcą, systemy AI podlegające niniejszemu rozporządzeniu mogą być dostarczane jako usługi pośrednie lub ich części w rozumieniu rozporządzenia (UE) 2022/2065, które należy postrzegać w sposób neutralny pod względem technologicznym. Na przykład systemy AI mogą być wykorzystywane w roli wyszukiwarek internetowych, w szczególności w zakresie, w jakim system AI, taki jak chatbot internetowy, zasadniczo przeprowadza wyszukiwanie wszystkich stron internetowych, a następnie włącza wyniki do swojej istniejącej wiedzy i wykorzystuje zaktualizowaną wiedzę do wygenerowania jednego wyniku, który łączy różne źródła informacji.

(120) Ponadto obowiązki nałożone w niniejszym rozporządzeniu na dostawców i podmioty stosujące niektóre systemy AI, by umożliwić wykrywanie i ujawnianie, że wyniki tych systemów są sztucznie wygenerowane lub zmanipulowane, są szczególnie istotne dla ułatwienia skutecznego wdrożenia rozporządzenia (UE) 2022/2065. Dotyczy to w szczególności obowiązków dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych w zakresie identyfikowania i ograniczania ryzyka systemowego, które może wynikać z rozpowszechniania treści sztucznie wygenerowanych lub zmanipulowanych, w szczególności ryzyka faktycznych lub przewidywalnych negatywnych skutków dla procesów demokratycznych, dyskursu obywatelskiego i procesów wyborczych, w tym poprzez stosowanie dezinformacji.

(121) Kluczową rolę w dostarczaniu dostawcom rozwiązań technicznych – zgodnie z aktualnym stanem wiedzy technicznej – w celu zapewnienia zgodności z niniejszym rozporządzeniem powinna odgrywać normalizacja, tak aby promować innowacje oraz konkurencyjność i wzrost gospodarczy na jednolitym rynku. Zgodność z normami zharmonizowanymi określonymi w art. 2 pkt 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012[41], które z założenia mają odzwierciedlać stan wiedzy technicznej, powinna stanowić dla dostawców sposób wykazania zgodności z wymogami niniejszego rozporządzenia. Przy opracowywaniu norm należy zatem zachęcać do zrównoważonej reprezentacji interesów wszystkich zainteresowanych stron, w szczególności MŚP, organizacji konsumenckich oraz zainteresowanych stron działających na rzecz ochrony środowiska i społeczeństwa zgodnie z art. 5 i 6 rozporządzenia (UE) nr 1025/2012. Aby ułatwić osiąganie zgodności, wnioski o normalizację powinny być wydawane przez Komisję bez zbędnej zwłoki. Przygotowując wniosek o normalizację, Komisja powinna skonsultować się z forum doradczym i Radą ds. AI, aby zebrać odpowiednią wiedzę fachową. Jednakże w przypadku braku odpowiednich odniesień do norm zharmonizowanych Komisja powinna mieć możliwość ustanowienia, w drodze aktów wykonawczych i po konsultacji z forum doradczym, wspólnych specyfikacji dotyczących niektórych wymogów określonych w niniejszym rozporządzeniu. Ta wspólna specyfikacja powinna stanowić wyjątkowe rozwiązanie awaryjne ułatwiające dostawcy spełnienie wymogów niniejszego rozporządzenia, w przypadku gdy wniosek o normalizację nie został zaakceptowany przez żadną z europejskich organizacji normalizacyjnych lub gdy odpowiednie normy zharmonizowane w niewystarczającym stopniu uwzględniają obawy dotyczące praw podstawowych lub gdy normy zharmonizowane nie są zgodne z wnioskiem, lub gdy występują opóźnienia w przyjęciu odpowiedniej normy zharmonizowanej. Jeżeli opóźnienie w przyjęciu normy zharmonizowanej wynika ze złożoności technicznej danej normy, Komisja powinna to uwzględnić, zanim zacznie rozważać ustanowienie wspólnych specyfikacji. Przy opracowywaniu wspólnych specyfikacji zachęca się Komisję do współpracy z partnerami międzynarodowymi i międzynarodowymi organami normalizacyjnymi.

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

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

(124) Aby zminimalizować obciążenie dla operatorów i uniknąć ewentualnego powielania działań, zgodność z wymogami niniejszego rozporządzenia w przypadku systemów AI wysokiego ryzyka powiązanych z produktami, które są objęte zakresem stosowania obowiązującego unijnego prawodawstwa harmonizacyjnego opartego na nowych ramach prawnych, należy oceniać w ramach oceny zgodności przewidzianej już w tym prawodawstwie. Stosowanie wymogów niniejszego rozporządzenia nie powinno zatem

wpływać na szczególną logikę, metodykę lub ogólną strukturę oceny zgodności określone w unijnym prawodawstwie harmonizacyjnym.

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

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

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

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

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

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

(131) Aby ułatwić pracę Komisji i państw członkowskich w dziedzinie AI, jak również zwiększyć przejrzystość wobec ogółu społeczeństwa, dostawców systemów AI wysokiego ryzyka innych niż te, które są powiązane z produktami objętymi zakresem stosowania odpowiedniego obowiązującego unijnego prawodawstwa harmonizacyjnego, a także dostawców, którzy uznają, że w związku z odstępstwem system AI wymieniony w wykazie przypadków wykorzystania stanowiących wysokie ryzyko zamieszczonym w załączniku do niniejszego rozporządzenia nie jest systemem wysokiego ryzyka, należy zobowiązać,

by dokonali swojej rejestracji oraz rejestracji informacji na temat swoich systemów AI w bazie danych UE, która zostanie utworzona i będzie zarządzana przez Komisję. Przed wykorzystaniem systemu AI wymienionego w wykazie przypadków wykorzystania stanowiących wysokie ryzyko zamieszczonym w załączniku do niniejszego rozporządzenia będące publicznymi organami, agencjami lub jednostkami organizacyjnymi podmioty stosujące systemy AI wysokiego ryzyka powinny dokonać swojej rejestracji w tej bazie danych i wybrać system, który zamierzają wykorzystywać. Inne podmioty stosujące powinny być uprawnione do uczynienia tego dobrowolnie. Ta sekcja bazy danych UE powinna być publicznie dostępna, nieodpłatna, informacje powinny być łatwe do odnalezienia, zrozumiałe i nadające się do odczytu maszynowego. Ta baza danych UE powinna być również przyjazna dla użytkownika, na przykład poprzez zapewnienie funkcji wyszukiwania, w tym za pomocą słów kluczowych, co umożliwi ogółowi społeczeństwa znalezienie istotnych informacji przedkładanych przy rejestracji systemów AI wysokiego ryzyka, oraz informacji na temat przypadków wykorzystywania systemów AI wysokiego ryzyka, określonych w załączniku do niniejszego rozporządzenia, któremu odpowiadają poszczególne systemy AI wysokiego ryzyka. W unijnej bazie danych UE powinno się też rejestrować wszelkie istotne zmiany systemów sztucznej inteligencji wysokiego ryzyka. W przypadku systemów AI wysokiego ryzyka w obszarze ścigania przestępstw, zarządzania migracją, azylem i kontrolą graniczną obowiązkowej rejestracji należy dokonać w bezpiecznej niepublicznej sekcji bazy danych. Dostęp do tej bezpiecznej niepublicznej sekcji powinna posiadać tylko i wyłącznie Komisja i organy nadzoru rynku w odniesieniu do ich krajowej sekcji bazy danych UE. Systemy AI wysokiego ryzyka w obszarze infrastruktury krytycznej powinny być rejestrowane wyłącznie na poziomie krajowym. Komisja powinna być administratorem bazy danych UE zgodnie z rozporządzeniem (UE) 2018/1725. Aby zapewnić pełną funkcjonalność bazy danych UE po jej wdrożeniu, procedura ustanawiania bazy danych powinna obejmować rozwijanie przez Komisję specyfikacji funkcjonalnych oraz sprawozdanie z niezależnego audytu. Wykonując swoje zadania jako administrator danych bazy danych UE, Komisja powinna wziąć pod uwagę ryzyko dotyczące cyberbezpieczeństwa. Aby zmaksymalizować dostępność i wykorzystywanie bazy danych UE przez społeczeństwo, baza danych UE, w tym udostępniane za jej pośrednictwem informacje, powinna być zgodna z wymogami określonymi w dyrektywie (UE) 2019/882.

(132) Niektóre systemy AI przeznaczone do wchodzenia w interakcję z osobami fizycznymi lub generowania treści mogą stwarzać szczególne ryzyko podawania się za inną osobę lub wprowadzania w błąd, niezależnie od tego, czy kwalifikują się jako systemy wysokiego ryzyka, czy też nie. W pewnych okolicznościach wykorzystanie tych systemów powinno zatem podlegać szczególnym obowiązkom w zakresie przejrzystości bez uszczerbku dla wymogów i obowiązków określonych dla systemów AI wysokiego ryzyka, przy zastosowaniu ukierunkowanych wyjątków, aby uwzględnić szczególne potrzeby w zakresie ścigania przestępstw. W szczególności osoby fizyczne powinny być powiadamiane o tym, że wchodzą w interakcję z systemem AI, chyba że jest to oczywiste z punktu widzenia osoby fizycznej, która jest dostatecznie poinformowana, uważna i ostrożna, z uwzględnieniem okoliczności i kontekstu korzystania. Przy spełnianiu takiego obowiązku należy uwzględniać cechy osób fizycznych należących do grup szczególnie wrażliwych ze względu na wiek lub niepełnosprawność – w zakresie, w jakim system AI ma również wchodzić w interakcję z tymi grupami. Ponadto osoby fizyczne powinny być powiadamiane, jeżeli są poddawane działaniu systemów AI, które poprzez przetwarzanie ich danych biometrycznych mogą zidentyfikować lub wywnioskować emocje lub zamiary tych osób lub przypisać je do określonych kategorii. Te określone kategorie mogą dotyczyć takich aspektów jak płeć, wiek, kolor włosów, kolor oczu, tatuaże, cechy osobowości, pochodzenie etniczne, osobiste preferencje i zainteresowania. Tego rodzaju informacje i powiadomienia należy przekazywać w formatach dostępnych dla osób z niepełnosprawnościami.

(133) Różne systemy AI mogą generować duże ilości treści syntetycznych, które stają się coraz trudniejsze do odróżnienia od treści generowanych przez człowieka i treści autentycznych. Szeroka dostępność i coraz większe zdolności tych systemów mają znaczący wpływ na integralność ekosystemu informacyjnego i zaufanie do niego, stwarzając nowe rodzaje ryzyka polegające na podawaniu informacji wprowadzających w błąd i na manipulacji na dużą skalę, oszustwach, podszywaniu się pod inne osoby i wprowadzaniu w błąd konsumentów. W świetle tych skutków, a także szybkiego tempa technologicznego oraz zapotrzebowania na nowe metody i techniki śledzenia pochodzenia informacji należy zobowiązać dostawców tych systemów do wbudowania rozwiązań technicznych, które umożliwiają oznakowanie w formacie nadającym się do odczytu maszynowego i wykrywanie, że wyniki zostały wygenerowane lub zmanipulowane przez system AI, a nie przez człowieka. Takie techniki i metody powinny być wystarczająco niezawodne, interoperacyjne, skuteczne i solidne, o ile jest to technicznie wykonalne, z uwzględnieniem dostępnych technik lub kombinacji takich technik, takich jak znaki wodne, identyfikacja metadanych, metody kryptograficzne służące do potwierdzania pochodzenia i autentyczności treści, metody rejestracji zdarzeń, odciski palców lub inne techniki, stosownie do przypadku. Przy spełnianiu tego obowiązku dostawcy powinni uwzględniać specyfikę i ograniczenia różnych rodzajów treści oraz istotne postępy technologiczne i rynkowe w tym obszarze, które odzwierciedla powszechnie uznany

stan wiedzy technicznej. Takie techniki i metody można wdrażać na poziomie danego systemu AI lub na poziomie modelu AI, w tym modeli AI ogólnego przeznaczenia generujących treści, a tym samym ułatwiać spełnianie tego obowiązku przez dostawcę niższego szczebla danego systemu AI. Aby zachować proporcjonalność, należy przewidzieć, że ten obowiązek oznakowania nie powinien obejmować systemów AI pełniących przede wszystkim funkcję wspomagającą w zakresie standardowej edycji lub systemów AI, które nie zmieniają w istotny sposób przekazywanych przez podmiot stosujący danych wejściowych ani ich semantyki.

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

(135) Bez uszczerbku dla obowiązkowego charakteru i pełnego stosowania obowiązków w zakresie przejrzystości Komisja może również zachęcać do opracowywania kodeksów praktyk na poziomie Unii i ułatwiać ich opracowywanie, aby ułatwić skuteczne wykonywanie obowiązków dotyczących wykrywania i oznakowania treści, które zostały sztucznie wygenerowane lub zmanipulowane, w tym aby wspierać praktyczne rozwiązania dotyczące udostępniania, stosownie do przypadku, mechanizmów wykrywania i ułatwiania współpracy z innymi podmiotami w całym łańcuchu wartości, które rozpowszechniają treści lub sprawdzają ich autentyczność i pochodzenie, aby umożliwić ogółowi społeczeństwa skuteczne rozróżnianie treści wygenerowanych przez AI.

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

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

(138) AI jest szybko rozwijającą się grupą technologii, wymagającą nadzoru regulacyjnego oraz bezpiecznej i kontrolowanej przestrzeni do przeprowadzania doświadczeń, przy jednoczesnym zapewnieniu odpowiedzialnej innowacji oraz uwzględnieniu odpowiednich zabezpieczeń i środków ograniczających ryzyko. Aby zapewnić ramy prawne wspierające innowacje, nieulegające dezaktualizacji i uwzględniające przełomowe technologie, państwa członkowskie powinny zapewnić, by ich właściwe organy krajowe

ustanowiły co najmniej jedną piaskownicę regulacyjną w zakresie AI na poziomie krajowym, aby ułatwić rozwijanie i testowanie innowacyjnych systemów AI pod ścisłym nadzorem regulacyjnym przed ich wprowadzeniem do obrotu lub oddaniem do użytku w inny sposób. Państwa członkowskie mogłyby również spełnić ten obowiązek, uczestnicząc w już istniejących piaskownicach regulacyjnych lub ustanawiając piaskownicę wspólnie z co najmniej jednym właściwym organem innego państwa członkowskiego, o ile udział ten zapewnia uczestniczącym państwom członkowskim równoważny poziom zasięgu krajowego. Piaskownice regulacyjne w zakresie AI mogą być tworzone w formie fizycznej, cyfrowej lub hybrydowej i mogą obejmować zarówno produkty fizyczne, jak i cyfrowe. Organy ustanawiające piaskownice regulacyjne w zakresie AI powinny również zapewnić, aby dysponowały one odpowiednimi do ich funkcjonowania zasobami, w tym zasobami finansowymi i ludzkimi.

(139) Piaskownice regulacyjne w zakresie AI powinny mieć na celu: wspieranie innowacji w zakresie AI poprzez ustanowienie kontrolowanego środowiska doświadczalnego i testowego w fazie rozwojowej i przed wprowadzeniem do obrotu, z myślą o zapewnieniu zgodności innowacyjnych systemów AI z niniejszym rozporządzeniem oraz z innymi odpowiednimi przepisami prawa Unii i prawa krajowego. Ponadto piaskownice regulacyjne w zakresie AI powinny mieć na celu zwiększenie pewności prawa dla innowatorów, a także usprawnienie nadzoru ze strony właściwych organów oraz podnoszenie poziomu ich wiedzy na temat możliwości, pojawiających się rodzajów ryzyka oraz skutków związanych ze stosowaniem AI, ułatwienie organom i przedsiębiorstwom uczenia się działań regulacyjnych, w tym z myślą o przyszłym dostosowaniu ram prawnych, wspieranie współpracy i wymiany najlepszych praktyk z organami zaangażowanymi w piaskownicę regulacyjną w zakresie AI oraz przyspieszenie dostępu do rynków, w tym poprzez usuwanie barier dla MŚP, w tym przedsiębiorstw typu startup. Piaskownice regulacyjne w zakresie AI powinny być powszechnie dostępne w całej Unii, a szczególną uwagę należy zwrócić na ich dostępność dla MŚP, w tym dla przedsiębiorstw typu startup. Uczestnictwo w piaskownicy regulacyjnej w zakresie AI powinno koncentrować się na kwestiach, które powodują niepewność prawa dla dostawców i potencjalnych dostawców w zakresie innowacji i eksperymentowania z AI w Unii oraz powinno przyczyniać się do opartego na dowodach uczenia się działań regulacyjnych. Nadzór nad systemami AI w piaskownicy regulacyjnej w zakresie AI powinien zatem obejmować ich rozwój, trenowanie, testowanie i walidację przed wprowadzeniem tych systemów do obrotu lub oddaniem do użytku, a także pojęcie i występowanie istotnych zmian, które mogą wymagać nowej procedury oceny zgodności. Wykrycie jakiegokolwiek znaczącego ryzyka na etapie rozwoju i testowania takich systemów AI powinno powodować konieczność właściwego ograniczenia tego ryzyka, a w przypadku niepowodzenia w tym zakresie – skutkować zawieszeniem procesu rozwoju i testowania systemu. W stosownych przypadkach właściwe organy krajowe ustanawiające piaskownice regulacyjne w zakresie AI powinny współpracować z innymi odpowiednimi organami, w tym organami nadzorującymi ochronę praw podstawowych, i powinny umożliwiać zaangażowanie innych podmiotów funkcjonujących w ekosystemie AI, takich jak krajowe lub europejskie organizacje normalizacyjne, jednostki notyfikowane, ośrodki testowo-doświadczalne, laboratoria badawczo-doświadczalne, europejskie centra innowacji cyfrowych oraz organizacje zrzeszające odpowiednie zainteresowane strony i społeczeństwo obywatelskie. Aby zapewnić jednolite wdrożenie w całej Unii oraz osiągnąć korzyści skali, należy ustanowić wspólne przepisy regulujące uruchamianie piaskownic regulacyjnych w zakresie AI oraz ramy współpracy między odpowiednimi organami uczestniczącymi w nadzorze nad piaskownicami regulacyjnymi. Piaskownice regulacyjne w zakresie AI ustanowione na mocy niniejszego rozporządzenia powinny pozostawać bez uszczerbku dla innych przepisów, które umożliwiają ustanawianie innych piaskownic mających na celu zapewnienie zgodności z przepisami prawa innymi niż niniejsze rozporządzenie. W stosownych przypadkach odpowiednie właściwe organy odpowiedzialne za inne piaskownice regulacyjne powinny przeanalizować korzyści płynące ze stosowania tych piaskownic również do celów zapewnienia zgodności systemów AI z niniejszym rozporządzeniem. Po osiągnięciu porozumienia pomiędzy właściwymi organami krajowymi oraz uczestnikami piaskownicy regulacyjnej w zakresie AI w ramach takiej piaskownicy regulacyjnej można również prowadzić i nadzorować testy w warunkach rzeczywistych.

(140) Niniejsze rozporządzenie powinno zapewniać dostawcom i potencjalnym dostawcom uczestniczącym w piaskownicy regulacyjnej w zakresie AI podstawę prawną do wykorzystywania danych osobowych zebranych w innych celach do rozwoju – w ramach piaskownicy regulacyjnej w zakresie AI – określonych systemów AI w interesie publicznym, tylko pod określonymi warunkami, zgodnie z art. 6 ust. 4 i art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679 i art. 5, 6 i 10 rozporządzenia (UE) 2018/1725 i nie naruszając przepisów art. 4 ust. 2 i art. 10 dyrektywy (UE) 2016/680. Nadal mają zastosowanie wszystkie pozostałe obowiązki administratorów danych i prawa osób, których dane dotyczą, wynikające z rozporządzeń (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywy (UE) 2016/680. W szczególności niniejsze rozporządzenie nie powinno stanowić podstawy prawnej w rozumieniu art. 22 ust. 2 lit. b) rozporządzenia (UE) 2016/679 i art. 24 ust. 2 lit. b) rozporządzenia (UE) 2018/1725. Dostawcy i potencjalni dostawcy w piaskownicy regulacyjnej w zakresie AI powinni zapewnić odpowiednie zabezpieczenia i współpracować

z właściwymi organami, w tym przestrzegać wytycznych tych organów, a także podejmować w dobrej wierze bezzwłoczne działania w celu właściwego ograniczenia wszelkiego zidentyfikowanego znaczącego ryzyka dla bezpieczeństwa, zdrowia i praw podstawowych, jakie może powstać w trakcie rozwoju produktów oraz prowadzenia działań testowych i doświadczalnych w ramach takiej piaskownicy regulacyjnej.

(141) Aby przyspieszyć proces rozwoju i wprowadzania do obrotu systemów AI wysokiego ryzyka wymienionych w załączniku do niniejszego rozporządzenia, ważne jest, aby dostawcy lub potencjalni dostawcy takich systemów mogli korzystać ze specjalnego mechanizmu testowania tych systemów w warunkach rzeczywistych, bez udziału w piaskownicy regulacyjnej w zakresie AI. Jednak w takich przypadkach oraz uwzględniając potencjalne konsekwencje takiego testowania dla osób fizycznych, należy zapewnić, by niniejsze rozporządzenie wprowadzało odpowiednie i wystarczające zabezpieczenia i warunki dotyczące dostawców lub potencjalnych dostawców. Takie zabezpieczenia powinny obejmować między innymi wymóg udzielenia świadomej zgody przez osoby fizyczne, które mają brać udział w testach w warunkach rzeczywistych, z wyjątkiem organów ścigania, gdy konieczność wystąpienia o świadomą zgodę uniemożliwiłaby testowanie systemu AI. Zgoda podmiotów testów na udział w takich testach na podstawie niniejszego rozporządzenia ma odrębny charakter i pozostaje bez uszczerbku dla zgody osób, których dane dotyczą, na przetwarzanie ich danych osobowych na podstawie odpowiedniego prawa o ochronie danych. Ważne jest również, aby zminimalizować ryzyko i umożliwić nadzór ze strony właściwych organów, a zatem zobowiązać potencjalnych dostawców do: przedstawienia właściwemu organowi nadzoru rynku planu testów w warunkach rzeczywistych, rejestrowania testów w specjalnych sekcjach bazy danych UE (z pewnymi ograniczonymi wyjątkami), ustalenia ograniczeń co do okresu, w jakim można przeprowadzać testy, oraz wymagania dodatkowych zabezpieczeń w odniesieniu do osób należących do grup szczególnie wrażliwych, a także pisemnej umowy określającej role i obowiązki potencjalnych dostawców i podmiotów stosujących oraz skutecznego nadzoru ze strony kompetentnego personelu zaangażowanego w testy w warunkach rzeczywistych. Ponadto należy przewidzieć dodatkowe zabezpieczenia w celu zapewnienia, aby predykcje, zalecenia lub decyzje systemu AI mogły zostać skutecznie odwrócone i nie były brane pod uwagę oraz aby dane osobowe były chronione i usuwane, gdy uczestnicy wycofają swoją zgodę na udział w testach, bez uszczerbku dla ich praw jako osób, których dane dotyczą, wynikających z prawa Unii o ochronie danych. W odniesieniu do przekazywania danych należy także przewidzieć, by dane zebrane i przetwarzane do celów testów w warunkach rzeczywistych przekazywano do państw trzecich wyłącznie pod warunkiem wdrożenia odpowiednich zabezpieczeń mających zastosowanie na podstawie prawa Unii, w szczególności zgodnie z podstawami przekazywania danych osobowych na mocy prawa Unii dotyczącego ochrony danych osobowych, a w odniesieniu do danych nieosobowych wprowadzono odpowiednie zabezpieczenia zgodnie z prawem Unii, takim jak rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868[42] i (UE) 2023/2854[43].

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

(143) W celu promowania i ochrony innowacji ważne jest szczególne uwzględnienie interesów MŚP, w tym przedsiębiorstw typu startup, które są dostawcami systemów AI lub podmiotami stosującymi systemy AI. W tym celu państwa członkowskie powinny opracować inicjatywy skierowane do tych operatorów, w tym inicjatywy służące podnoszeniu świadomości i przekazywaniu informacji. Państwa członkowskie powinny zapewniać MŚP, w tym przedsiębiorstwom typu startup, mającym siedzibę statutową lub oddział w Unii, priorytetowy dostęp do piaskownic regulacyjnych w zakresie AI, pod warunkiem że przedsiębiorstwa te spełniają warunki kwalifikowalności i kryteria wyboru – w sposób, który nie uniemożliwia innym dostawcom i potencjalnym dostawcom dostępu do piaskownic, pod warunkiem spełnienia przez nich tych samych warunków i kryteriów. Państwa członkowskie powinny korzystać z istniejących kanałów komunikacji, a w stosownych przypadkach utworzyć nowy specjalny kanał komunikacji z MŚP, w tym przedsiębiorstwami typu startup, podmiotami stosującymi, innymi innowacyjnymi podmiotami, a w stosownych przypadkach, z lokalnymi organami publicznymi, aby wspierać MŚP w rozwoju poprzez udzielanie im wskazówek i odpowiadanie na ich pytania dotyczące wykonywania niniejszego rozporządzenia. W stosownych przypadkach kanały powinny ze sobą współpracować, by uzyskać synergię i zapewnić spójność wskazówek dla MŚP, w tym przedsiębiorstw typu startup, i podmiotów

stosujących. Dodatkowo państwa członkowskie powinny ułatwiać udział MŚP i innych odpowiednich zainteresowanych stron w procesie opracowywania norm. Ponadto przy ustalaniu przez jednostki notyfikowane wysokości opłat z tytułu oceny zgodności należy uwzględnić szczególne interesy i potrzeby dostawców, którzy są MŚP, w tym przedsiębiorstwami typu startup. Komisja powinna regularnie oceniać koszty certyfikacji i zapewnienia zgodności ponoszone przez MŚP, w tym przedsiębiorstwa typu startup, w drodze przejrzystych konsultacji oraz współpracować z państwami członkowskimi na rzecz obniżenia tych kosztów. Przykładowo koszty tłumaczeń związane z prowadzeniem obowiązkowej dokumentacji i komunikacji z organami mogą stanowić istotny koszt dla dostawców i innych operatorów, w szczególności tych działających na mniejszą skalę. Państwa członkowskie powinny w miarę możliwości zapewnić, aby jednym z języków wskazanych i akceptowanych przez nie do celów dokumentacji prowadzonej przez odpowiednich dostawców oraz komunikacji z operatorami był język powszechnie rozumiany przez możliwie największą liczbę podmiotów stosujących w wymiarze transgranicznym. Aby zaspokoić szczególne potrzeby MŚP, w tym przedsiębiorstw typu startup, Komisja powinna na wniosek Rady ds. AI zapewnić ujednolicone wzory w obszarach objętych niniejszym rozporządzeniem. Ponadto Komisja powinna w uzupełnieniu wysiłków państw członkowskich dostarczyć jednolitą platformę informacyjną zawierającą łatwe w użyciu informacje dotyczące niniejszego rozporządzenia dla wszystkich dostawców i podmiotów stosujących, organizować odpowiednie kampanie informacyjne w celu podnoszenia świadomości na temat obowiązków wynikających z niniejszego rozporządzenia oraz oceniać i promować zbieżność najlepszych praktyk w procedurach udzielania zamówień publicznych w odniesieniu do systemów AI. Średnie przedsiębiorstwa, które do niedawna kwalifikowały się jako małe przedsiębiorstwa w rozumieniu załącznika do zalecenia Komisji 2003/361/WE[44], powinny mieć dostęp do tych środków wsparcia, ponieważ w niektórych przypadkach te nowe średnie przedsiębiorstwa mogą nie posiadać zasobów prawnych i szkoleniowych niezbędnych do zapewnienia właściwego zrozumienia i zapewnienia zgodności z niniejszym rozporządzeniem.

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

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

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

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

(148) W niniejszym rozporządzeniu należy ustanowić ramy zarządzania, które umożliwiają koordynację i wspieranie stosowania niniejszego rozporządzenia na poziomie krajowym, a także budowanie zdolności na poziomie Unii i zaangażowanie zainteresowanych stron w dziedzinę AI. Skuteczne wdrożenie i egzekwowanie niniejszego rozporządzenia wymaga ram zarządzania, które umożliwią koordynację i gromadzenie centralnej wiedzy fachowej na poziomie Unii. Misją Urzędu ds. AI, który został ustanowiony decyzją Komisji[45], jest rozwijanie unijnej wiedzy fachowej i unijnych zdolności w dziedzinie AI oraz przyczynianie się do wdrażania prawa Unii dotyczącego AI. Państwa członkowskie powinny ułatwiać Urzędowi ds. AI wykonywanie zadań z myślą o wspieraniu rozwoju unijnej wiedzy fachowej i unijnych zdolności oraz wzmacnianiu funkcjonowania jednolitego rynku cyfrowego. Ponadto należy ustanowić Radę ds. AI składającą się z przedstawicieli państw członkowskich, panel naukowy w celu zaangażowania

środowiska naukowego oraz forum doradcze w celu wnoszenia przez zainteresowane strony wkładu w wykonywanie niniejszego rozporządzenia na poziomie Unii i poziomie krajowym. Rozwój unijnej wiedzy fachowej i unijnych zdolności powinien również obejmować wykorzystanie istniejących zasobów i wiedzy fachowej, w szczególności poprzez synergię ze strukturami zbudowanymi w kontekście egzekwowania innych przepisów na poziomie Unii oraz synergię z powiązanymi inicjatywami na poziomie Unii, takimi jak Wspólne Przedsięwzięcie EuroHPC i ośrodki testowo-doświadczalne w dziedzinie AI w ramach programu „Cyfrowa Europa".

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

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

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

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

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

innych partnerów na poziomie państw członkowskich i na poziomie Unii, każde państwo członkowskie powinno wyznaczyć organ nadzoru rynku, który pełniłby funkcję pojedynczego punktu kontaktowego.

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

(155) W celu zapewnienia, aby dostawcy systemów AI wysokiego ryzyka mogli wykorzystywać doświadczenia związane ze stosowaniem systemów AI wysokiego ryzyka do ulepszenia swoich systemów oraz procesu projektowania i rozwoju lub byli w stanie odpowiednio szybko podejmować wszelkie możliwe działania naprawcze, każdy dostawca powinien wdrożyć system monitorowania po wprowadzeniu do obrotu. W stosownych przypadkach monitorowanie po wprowadzeniu do obrotu powinno obejmować analizę interakcji z innymi systemami AI, w tym z innymi urządzeniami i oprogramowaniem. Monitorowanie po wprowadzeniu do obrotu nie obejmuje wrażliwych danych operacyjnych podmiotów stosujących, które są organami ścigania. System ten ma również zasadnicze znaczenie dla zapewnienia skuteczniejszego i terminowego przeciwdziałania możliwym pojawiającym się ryzykom związanym z systemami AI, które nadal „uczą się" po wprowadzeniu do obrotu lub oddaniu do użytku. W tym kontekście dostawcy powinni być również zobowiązani do wdrożenia systemu zgłaszania odpowiednim organom wszelkich poważnych incydentów zaistniałych w związku z wykorzystaniem ich systemów AI, tj. incydentu lub nieprawidłowego działania prowadzącego do śmierci lub poważnej szkody dla zdrowia, poważnych i nieodwracalnych zakłóceń w zarządzaniu infrastrukturą krytyczną i jej działaniu, naruszeń obowiązków ustanowionych w prawie Unii, których celem jest ochrona praw podstawowych, lub poważnych szkód majątkowych lub środowiskowych.

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

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

(158) Przepisy prawa Unii dotyczące usług finansowych obejmują zasady i wymogi dotyczące zarządzania wewnętrznego i zarządzania ryzykiem, które mają zastosowanie do regulowanych instytucji finansowych podczas świadczenia tych usług, w tym wówczas, gdy korzystają one z systemów AI. Aby zapewnić spójne stosowanie i egzekwowanie obowiązków ustanowionych w niniejszym rozporządzeniu oraz odpowiednich zasad i wymogów ustanowionych w unijnych aktach prawnych dotyczących usług finansowych, właściwe organy do celów nadzoru nad tymi aktami prawnymi i ich egzekwowania, w szczególności właściwe organy zdefiniowane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 575/2013[46] oraz dyrektywach Parlamentu Europejskiego i Rady 2008/48/WE[47], 2009/138/WE[48], 2013/36/UE[49], 2014/17/UE[50] i (UE) 2016/97[51], należy wyznaczyć w ramach ich odpowiednich kompetencji

jako właściwe organy do celów nadzoru nad wykonywaniem niniejszego rozporządzenia, w tym do celów działań w zakresie nadzoru rynku, w odniesieniu do systemów AI dostarczanych lub wykorzystywanych przez objęte regulacją i nadzorem instytucje finansowe, chyba że państwa członkowskie zdecydują się wyznaczyć inny organ do wypełniania tych zadań związanych z nadzorem rynku. Te właściwe organy powinny mieć wszystkie uprawnienia wynikające z niniejszego rozporządzenia i rozporządzenia (UE) 2019/1020 w celu egzekwowania wymogów i obowiązków ustanowionych w niniejszym rozporządzeniu, w tym uprawnienia do prowadzenia działań *ex post* w zakresie nadzoru rynku, które można w stosownych przypadkach włączyć do ich istniejących mechanizmów i procedur nadzorczych na podstawie odpowiednich przepisów prawa Unii dotyczących usług finansowych. Należy przewidzieć, że – działając w charakterze organów nadzoru rynku na podstawie niniejszego rozporządzenia – krajowe organy odpowiedzialne za nadzór nad instytucjami kredytowymi uregulowanymi w dyrektywie 2013/36/UE, które uczestniczą w jednolitym mechanizmie nadzorczym ustanowionym rozporządzeniem Rady (UE) nr 1024/2013[52], powinny niezwłocznie przekazywać Europejskiemu Bankowi Centralnemu wszelkie informacje zidentyfikowane w trakcie prowadzonych przez siebie działań w zakresie nadzoru rynku, które potencjalnie mogą mieć znaczenie dla Europejskiego Banku Centralnego z punktu widzenia określonych w tym rozporządzeniu zadań EBC dotyczących nadzoru ostrożnościowego. Aby dodatkowo zwiększyć spójność między niniejszym rozporządzeniem a przepisami mającymi zastosowanie do instytucji kredytowych uregulowanych w dyrektywie 2013/36/UE, niektóre obowiązki proceduralne dostawców związane z zarządzaniem ryzykiem, monitorowaniem po wprowadzeniu do obrotu oraz prowadzeniem dokumentacji należy również włączyć do istniejących obowiązków i procedur przewidzianych w dyrektywie 2013/36/UE. Aby uniknąć nakładania się przepisów, należy również przewidzieć ograniczone odstępstwa dotyczące systemu zarządzania jakością prowadzonego przez dostawców oraz obowiązku monitorowania nałożonego na podmioty stosujące systemy AI wysokiego ryzyka w zakresie, w jakim mają one zastosowanie do instytucji kredytowych uregulowanych w dyrektywie 2013/36/UE. Ten sam system powinien mieć zastosowanie do zakładów ubezpieczeń i zakładów reasekuracji oraz ubezpieczeniowych spółek holdingowych na podstawie dyrektywy 2009/138/WE oraz pośredników ubezpieczeniowych na mocy dyrektywy (UE) 2016/97, a także do innych rodzajów instytucji finansowych objętych wymogami dotyczącymi systemu zarządzania wewnętrznego, uzgodnień lub procedur ustanowionych zgodnie z odpowiednimi przepisami prawa Unii dotyczącymi usług finansowych, w celu zapewnienia spójności i równego traktowania w sektorze finansowym.

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

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

(161) Konieczne jest wyjaśnienie odpowiedzialności i kompetencji na poziomie Unii i poziomie krajowym w odniesieniu do systemów AI, które opierają się na modelach AI ogólnego przeznaczenia. Aby uniknąć nakładania się kompetencji, w przypadku gdy system AI opiera się na modelu AI ogólnego przeznaczenia, a model i system są dostarczone przez tego samego dostawcę, nadzór powinien odbywać się na poziomie Unii za pośrednictwem Urzędu ds. AI, który w tym celu powinien posiadać uprawnienia organu nadzoru rynku w rozumieniu rozporządzenia (UE) 2019/1020. We wszystkich innych przypadkach krajowe organy nadzoru rynku pozostają odpowiedzialne za nadzór nad systemami AI. Natomiast w przypadku systemów AI ogólnego przeznaczenia, które mogą być wykorzystywane bezpośrednio przez podmioty stosujące do co najmniej jednego celu zaklasyfikowanego jako cel wysokiego ryzyka, organy nadzoru rynku powinny współpracować z Urzędem ds. AI przy prowadzeniu ocen zgodności

i by odpowiednio informować Radę ds. AI i inne organy nadzoru rynku. Ponadto organy nadzoru rynku powinny mieć możliwość zwrócenia się o pomoc do Urzędu ds. AI, jeżeli organ nadzoru rynku nie jest w stanie zakończyć postępowania w sprawie systemu AI wysokiego ryzyka ze względu na niemożność dostępu do niektórych informacji związanych z modelem AI ogólnego przeznaczenia, na którym opiera się ten system AI wysokiego ryzyka. W takich przypadkach powinna mieć zastosowanie odpowiednio procedura dotycząca wzajemnej pomocy transgranicznej określona w rozdziale VI rozporządzenia (UE) 2019/1020.

(162) Aby jak najlepiej wykorzystać scentralizowaną unijną wiedzę fachową i synergie na poziomie Unii, uprawnienia w zakresie nadzoru i egzekwowania obowiązków spoczywających na dostawcach modeli AI ogólnego przeznaczenia powinny należeć do kompetencji Komisji. Urząd ds. AI powinien mieć możliwość prowadzenia wszelkich niezbędnych działań w celu monitorowania skutecznego wykonywania niniejszego rozporządzenia w odniesieniu do modeli AI ogólnego przeznaczenia. Powinien mieć możliwość prowadzenia postępowań w sprawie ewentualnych naruszeń przepisów dotyczących dostawców modeli AI ogólnego przeznaczenia zarówno z własnej inicjatywy, na podstawie wyników swoich działań monitorujących, jak i na wniosek organów nadzoru rynku zgodnie z warunkami określonymi w niniejszym rozporządzeniu. W celu wsparcia skutecznego monitorowania Urząd ds. AI powinien ustanowić możliwość składania przez dostawców niższego szczebla skarg na dostawców modeli i systemów AI ogólnego przeznaczenia dotyczących ewentualnych naruszeń przepisów.

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

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

(165) Rozwój systemów AI innych niż systemy AI wysokiego ryzyka zgodnie z wymogami niniejszego rozporządzenia może doprowadzić do szerszego upowszechnienia etycznej i godnej zaufania AI w Unii. Dostawców systemów AI niebędących systemami wysokiego ryzyka należy zachęcać do opracowywania kodeksów postępowania, w tym powiązanych mechanizmów zarządzania, wspierających dobrowolne stosowanie niektórych lub wszystkich obowiązkowych wymogów mających zastosowanie do systemów AI wysokiego ryzyka, dostosowanych do przeznaczenia tych systemów i związanego z nimi niższego ryzyka oraz z uwzględnieniem dostępnych rozwiązań technicznych i najlepszych praktyk branżowych, takich jak karty modeli i karty charakterystyki. Dostawców wszystkich systemów AI, zarówno wysokiego ryzyka, jak i nie stanowiących wysokiego ryzyka, oraz modeli AI, a w stosownych przypadkach, podmioty stosujące te systemy i modele należy również zachęcać do dobrowolnego stosowania dodatkowych wymogów dotyczących na przykład elementów unijnych Wytycznych w zakresie etyki dotyczących godnej zaufania sztucznej inteligencji, zrównoważenia środowiskowego, środków wspierających kompetencje w zakresie AI, projektowania i rozwoju systemów AI z uwzględnieniem różnorodności i inkluzywności, w tym szczególnej uwagi poświęconej osobom szczególnie wrażliwym i dostępności dla osób z niepełnosprawnościami, udziału zainteresowanych stron w tym, w stosownych przypadkach, organizacji przedsiębiorców i społeczeństwa obywatelskiego, środowisk akademickich, organizacji badawczych,

związków zawodowych i organizacji ochrony konsumentów w projektowaniu i rozwoju systemów AI oraz dotyczących różnorodności zespołów programistycznych, w tym pod względem równowagi płci. W celu zapewnienia skuteczności dobrowolnych kodeksów postępowania, powinny się one opierać się na jasnych celach i kluczowych wskaźnikach skuteczności działania służących do pomiaru stopnia osiągnięcia tych celów. Należy je również rozwijać w sposób inkluzywny, w stosownych przypadkach, z udziałem odpowiednich zainteresowanych stron, takich jak organizacje przedsiębiorców i społeczeństwa obywatelskiego, środowiska akademickie, organizacje badawcze, związki zawodowe i organizacje ochrony konsumentów. Komisja może opracowywać inicjatywy, również o charakterze sektorowym, aby ułatwiać zmniejszanie barier technicznych utrudniających transgraniczną wymianę danych na potrzeby rozwoju AI, w tym w zakresie infrastruktury dostępu do danych oraz interoperacyjności semantycznej i technicznej różnych rodzajów danych.

(166) Istotne jest, aby systemy AI powiązane z produktami, które nie są systemami wysokiego ryzyka w rozumieniu niniejszego rozporządzenia, a zatem nie muszą być zgodne z wymogami ustanowionymi w przypadku systemów AI wysokiego ryzyka, były mimo to bezpieczne w chwili wprowadzenia ich do obrotu lub oddawania ich do użytku. Aby przyczynić się do osiągnięcia tego celu, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988[53] miałoby zastosowanie jako rozwiązanie zapasowe.

(167) W celu zapewnienia opartej na zaufaniu i konstruktywnej współpracy właściwych organów na poziomie Unii i poziomie krajowym wszystkie strony uczestniczące w stosowaniu niniejszego rozporządzenia powinny przestrzegać zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań, zgodnie z prawem Unii lub prawem krajowym. Powinny one wykonywać swoje zadania i prowadzić działania w taki sposób, aby chronić w szczególności prawa własności intelektualnej, poufne informacje handlowe i tajemnice przedsiębiorstwa, skuteczne wykonywanie niniejszego rozporządzenia, interesy bezpieczeństwa publicznego i narodowego, integralność postępowań karnych i administracyjnych oraz integralność informacji niejawnych.

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

(169) Spełnienie obowiązków spoczywających na dostawcach modeli AI ogólnego przeznaczenia nałożonych na mocy niniejszego rozporządzenia powinna być możliwa do wyegzekwowania między innymi za pomocą kar pieniężnych. W tym celu należy również ustanowić odpowiednią wysokość kar pieniężnych za naruszenie tych obowiązków, w tym za niezastosowanie środków wymaganych przez Komisję zgodnie z niniejszym rozporządzeniem, z zastrzeżeniem odpowiednich terminów przedawnienia zgodnie z zasadą proporcjonalności. Wszystkie decyzje przyjmowane przez Komisję na podstawie niniejszego rozporządzenia podlegają kontroli Trybunału Sprawiedliwości Unii Europejskiej zgodnie z TFUE, w tym nieograniczonemu prawu orzekania zgodnie z art. 261 TFUE.

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

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

(172) Osoby działające w charakterze sygnalistów w związku z naruszeniami niniejszego rozporządzenia powinny być chronione na mocy prawa Unii. Do zgłaszania naruszeń przepisów niniejszego rozporządzenia

oraz ochrony osób zgłaszających przypadki takich naruszeń powinno zatem stosować się dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937[54].

(173) Aby zapewnić możliwość dostosowania w razie potrzeby ram regulacyjnych, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu zmiany warunków, na podstawie których systemu AI nie uznaje się za system AI wysokiego ryzyka, zmiany wykazu systemów AI wysokiego ryzyka, przepisów dotyczących dokumentacji technicznej, treści deklaracji zgodności UE, przepisów dotyczących procedur oceny zgodności, przepisów określających systemy AI wysokiego ryzyka, do których powinna mieć zastosowanie procedura oceny zgodności oparta na ocenie systemu zarządzania jakością oraz ocenie dokumentacji technicznej, progu, poziomów odniesienia i wskaźników, które zostały określone w przepisach dotyczących klasyfikacji modeli AI ogólnego przeznaczenia z ryzykiem systemowym, w tym poprzez uzupełnienie tych poziomów odniesienia i wskaźników, kryteriów uznawania modeli za modele AI ogólnego przeznaczenia z ryzykiem systemowym, dokumentacji technicznej dostawców modeli AI ogólnego przeznaczenia oraz informacji dotyczących przejrzystości od dostawców modeli AI ogólnego przeznaczenia. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[55]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(174) Z uwagi na szybki rozwój technologiczny i wiedzę techniczną wymaganą do skutecznego stosowania niniejszego rozporządzenia, Komisja powinna dokonać oceny i przeglądu niniejszego rozporządzenia do dnia 2 sierpnia 2029 r., a następnie co cztery lata oraz składać sprawozdania Parlamentowi Europejskiemu i Radzie. Ponadto ze względu na skutki dla zakresu stosowania niniejszego rozporządzenia Komisja powinna raz w roku ocenić, czy konieczne jest wprowadzenie zmian w wykazie systemów AI wysokiego ryzyka i w wykazie zakazanych praktyk. Dodatkowo do dnia 2 sierpnia 2028 r., a następnie co cztery lata, Komisja powinna ocenić, czy należy wprowadzić zmiany w wykazie nagłówków dotyczących obszarów wysokiego ryzyka zawartym w załączniku do niniejszego rozporządzenia, zmiany w zakresie systemów AI objętych obowiązkami w zakresie przejrzystości, zmiany służące skuteczności systemu nadzoru i zarządzania oraz ocenić postępy w opracowywaniu dokumentów normalizacyjnych dotyczących efektywnego energetycznie rozwoju modeli AI ogólnego przeznaczenia, w tym potrzebę wprowadzenia dalszych środków lub działań, a następnie przekazać sprawozdania z tych ocen Parlamentowi Europejskiemu i Radzie. Ponadto do dnia 2 sierpnia 2028 r., a następnie co trzy lata, Komisja powinna oceniać wpływ i skuteczność dobrowolnych kodeksów postępowania pod względem wspierania stosowania wymogów przewidzianych w przypadku systemów AI wysokiego ryzyka do systemów AI innych niż systemy AI wysokiego ryzyka oraz ewentualnie innych dodatkowych wymogów dotyczących takich systemów AI.

(175) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[56].

(176) Ponieważ cel niniejszego rozporządzenia, a mianowicie poprawa funkcjonowania rynku wewnętrznego i promowanie upowszechniania zorientowanej na człowieka i godnej zaufania AI, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa i praw podstawowych zapisanych w Karcie, w tym demokracji, praworządności i ochrony środowiska przed szkodliwymi skutkami systemów AI w Unii, oraz wspieranie innowacji, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary lub skutki działania możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

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

podjąć niezbędne kroki w celu spełnienia wymogów niniejszego rozporządzenia do końca 2030 r. i do dnia 2 sierpnia 2030 r.

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

(179) Niniejsze rozporządzenie należy stosować od dnia 2 sierpnia 2026 r. Biorąc jednak pod uwagę niedopuszczalne ryzyko związane z niektórymi sposobami wykorzystania AI, zakazy oraz przepisy ogólne niniejszego rozporządzenia należy stosować już od dnia 2 lutego 2025 r. Chociaż pełne skutki tych zakazów zrealizowane zostaną w momencie ustanowienia zarządzania i egzekwowania niniejszego rozporządzenia, wcześniejsze ich stosowanie jest ważne, by uwzględnić niedopuszczalne ryzyko i wywrzeć wpływ na inne procedury, np. w prawie cywilnym. Ponadto infrastruktura związana z zarządzaniem i systemem oceny zgodności powinna być gotowa przed dniem 2 sierpnia 2026 r., w związku z czym przepisy dotyczące jednostek notyfikowanych oraz struktury zarządzania należy stosować od dnia 2 sierpnia 2025 r. Biorąc pod uwagę szybkie tempo postępu technologicznego i przyjęcie modeli AI ogólnego przeznaczenia, obowiązki dostawców modeli AI ogólnego przeznaczenia należy stosować od dnia 2 sierpnia 2025 r. Kodeksy praktyk powinny być gotowe do dnia 2 maja 2025 r., tak aby umożliwić dostawcom terminowe wykazanie zgodności. Urząd ds. AI powinien zapewniać aktualność zasad i procedur klasyfikacji w świetle rozwoju technologicznego. Ponadto państwa członkowskie powinny ustanowić przepisy dotyczące kar, w tym administracyjnych kar pieniężnych i powiadomić o nich Komisję oraz zapewnić ich właściwe i skuteczne wdrożenie przed dniem rozpoczęcia stosowania niniejszego rozporządzenia. Przepisy dotyczące kar należy zatem stosować od dnia 2 sierpnia 2025 r.

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

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

[1] Dz.Urz. C 517 z 22.12.2021 r., s. 56.

[2] Dz.Urz. C 115 z 11.03.2022 r., s. 5.

[3] Dz.Urz. C 97 z 28.02.2022 r., s. 60.

[4] Stanowisko Parlamentu Europejskiego z 13.03.2024 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z 21.05.2024 r.

[5] Rada Europejska, Nadzwyczajne posiedzenie Rady Europejskiej (1 i 2.10.2020 r.) – Konkluzje, EUCO 13/20, 2020, s. 6.

[6] Rezolucja Parlamentu Europejskiego z 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).

[7] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z 9.07.2008 r. ustanawiające wymagania w zakresie akredytacji i uchylające rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L 218, s. 30).

[8] Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z 9.07.2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz.Urz. UE L 218, s. 82).

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z 20.06.2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L 169, s. 1).

[10] Dyrektywa Rady 85/374/EWG z 25.07.1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.Urz. UE L 210, s. 29).

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1).

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 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.Urz. UE L 295, s. 39).

[13] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89).

[14] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201, s. 37).

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.Urz. UE L 277, s. 1).

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z 17.04.2019 r. w sprawie wymogów dostępności produktów i usług (Dz.Urz. UE L 151, s. 70).

[17] Dyrektywa Parlamentu Europejskiego i Rady 2005/29/WE z 11.05.2005 r. dotycząca nieuczciwych praktyk handlowych.

[18] Decyzja ramowa Rady 2002/584/WSiSW z 13.06.2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.Urz. UE L 190, s. 1).

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14.12.2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.Urz. UE L 333, s. 164).

[20] Dz.Urz. C 247 z 29.06.2022 r., s. 1.

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5.04.2017 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.Urz. UE L 117, s. 1).

[22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z 5.04.2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.Urz. UE L 117, s. 176).

[23] Dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady z 17.05.2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE (Dz.Urz. UE L 157, s. 24).

[24] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z 11.03.2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz.Urz. UE L 97, s. 72).

[25] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 167/2013 z 5.02.2013 r. w sprawie homologacji i nadzoru rynku pojazdów rolniczych i leśnych (Dz.Urz. UE L 60, s. 1).

[26] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 168/2013 z 15.01.2013 r. w sprawie homologacji i nadzoru rynku pojazdów dwu- lub trzykołowych oraz czterokołowców (Dz.Urz. UE L 60, s. 52).

[27] Dyrektywa Parlamentu Europejskiego i Rady 2014/90/UE z 23.07.2014 r. w sprawie wyposażenia morskiego i uchylająca dyrektywę Rady 96/98/WE (Dz.Urz. UE L 257, s. 146).

[28] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/797 z 11.05.2016 r. w sprawie interoperacyjności systemu kolei w Unii Europejskiej (Dz.Urz. UE L 138, s. 44).

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 z 30.05.2018 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.Urz. UE L 151, s. 1).

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z 4.07.2018 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.Urz. UE L 212, s. 1).

[31] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2144 z 27.11.2019 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.Urz. UE L 325, s. 1).

[32] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z 13.07.2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz.Urz. UE L 243, s. 1).

[33] Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z 26.06.2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (Dz.Urz. UE L 180, s. 60).

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/900 w sprawie przejrzystości i targetowania reklamy politycznej (Dz.Urz. UE L 2024/900, z 20.03.2024 r., ELI: http://data.europa.eu/eli/reg/2024/900/oj).

[35] Dyrektywa Parlamentu Europejskiego i Rady 2014/31/UE z 26.02.2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku wag nieautomatycznych (Dz.Urz. UE L 96, s. 107).

[36] Dyrektywa Parlamentu Europejskiego i Rady 2014/32/UE z 26.02.2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych (Dz.Urz. UE L 96, s. 149).

[37] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 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.Urz. UE L 151, s. 15).

[38] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z 26.10.2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.Urz. UE L 327, s. 1).

[39] Dyrektywa 2002/14/WE Parlamentu Europejskiego i Rady z 11.03.2002 r. ustanawiająca ogólne ramowe warunki informowania i przeprowadzania konsultacji z pracownikami we Wspólnocie Europejskiej (Dz.Urz. UE L 80, s. 29).

[40] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92).

[41] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z 25.10.2012 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.Urz. UE L 316, s. 12).

[42] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30.05.2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.Urz. UE L 152, s. 1).

[43] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z 13.12.2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.Urz. UE L 2023/2854, ELI: http://data.europa. eu/eli/reg/2023/2854/oj).

[44] Zalecenie Komisji z 6.05.2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.Urz. UE L 124, s. 36).

[45] Decyzja Komisji z 24.01.2024 r. ustanawiająca Europejski Urząd ds. Sztucznej Inteligencji C(2024) 390.

[46] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z 26.06.2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.Urz. UE L 176, s. 1).

[47] Dyrektywa Parlamentu Europejskiego i Rady nr 2008/48/WE z 23.04.2008 r. w sprawie umów o kredyt konsumencki oraz uchylająca dyrektywę Rady 87/102/EWG (Dz.Urz. UE L 133, s. 66).

[48] Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z 25.11.2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.Urz. UE L 335, s. 1).

[49] Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z 26.06.2013 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.Urz. UE L 176, s. 338).

[50] Dyrektywa Parlamentu Europejskiego i Rady 2014/17/UE z 4.02.2014 r. w sprawie konsumenckich umów o kredyt związanych z nieruchomościami mieszkalnymi i zmieniająca dyrektywy 2008/48/WE i 2013/36/UE oraz rozporządzenie (UE) nr 1093/2010 (Dz.Urz. UE L 60, s. 34).

[51] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z 20.01.2016 r. w sprawie dystrybucji ubezpieczeń (Dz.Urz. UE L 26, s. 19).

[52] Rozporządzenie Rady (UE) nr 1024/2013 z 15.10.2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz.Urz. UE L 287, s. 63).

[53] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z 10.05.2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz.Urz. UE L 135, s. 1).

[54] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23.10.2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.Urz. UE L 305, s. 17).

[55] Dz.Urz. UE L 123 z 12.05.2016 r., s. 1.

[56] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16.02.2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.Urz. UE L 55, s. 13).

Rozdział I. Przepisy ogólne

Maria Jędrzejczak

Artykuł 1
Przedmiot

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

2. W niniejszym rozporządzeniu ustanawia się:

a) zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów AI w Unii;
b) zakazy dotyczące niektórych praktyk w zakresie AI;
c) szczególne wymogi dotyczące systemów AI wysokiego ryzyka oraz obowiązki spoczywające na operatorach takich systemów;
d) zharmonizowane przepisy dotyczące przejrzystości w przypadku niektórych systemów AI;
e) zharmonizowane przepisy dotyczące wprowadzania do obrotu modeli AI ogólnego przeznaczenia;
f) przepisy dotyczące monitorowania wprowadzania do obrotu, nadzoru rynku, zarządzania i egzekwowania;
g) środki wspierające innowacje, ze szczególnym uwzględnieniem MŚP, w tym przedsiębiorstw typu startup.

1. Komentowany artykuł wyznacza ramy prawne dla AI w UE, które – w założeniu – priorytetowo traktują zarówno innowacyjność, jak i rozwój, wdrażanie i użytkowanie systemów AI w zgodzie z prawami człowieka. Innymi słowy, unijna polityka w tym zakresie powinna koncentrować się na maksymalizacji potencjalnych korzyści społecznych i ekonomicznych przy jednoczesnym ograniczaniu ryzyka związanego z wykorzystaniem systemów AI. Jednym z celów prawodawcy unijnego było stworzenie środowiska przyjaznego rozwojowi systemów AI na rynku wewnętrznym UE, zapewniającego swobodny transgraniczny przepływ towarów i usług opartych na AI oraz uniemożliwiającego państwom członkowskim nakładanie ograniczeń na rozwój, wprowadzanie do obrotu i wykorzystywanie systemów AI, chyba że jest to wyraźnie dozwolone w niniejszym rozporządzeniu[1].

2. W motywie 1 preambuły AI Act podkreślono, że podstawowym celem rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego przez ustanowienie jednolitych ram prawnych zgodnie z wartościami unijnymi w celu promowania upowszechniania zorientowanej na człowieka i godnej zaufania AI przy jednoczesnym zapewnieniu wysokiego poziomu

[1] Zob. motyw 1 preambuły AI Act.

ochrony interesów publicznych w dziedzinie zdrowia, bezpieczeństwa i praw podstawowych, zwłaszcza w obszarze funkcjonowania systemów AI wysokiego ryzyka[2].

3. Ważnym aspektem wskazanym wśród celów rozporządzenia jest „zorientowanie na człowieka". Sztuczna inteligencja powinna służyć jako narzędzie dla ludzi, którego ostatecznym celem jest zwiększenie dobrostanu człowieka[3]. Również w uzasadnieniu AI Act wskazano, że „przepisy dotyczące sztucznej inteligencji, która jest dostępna na rynku Unii lub w inny sposób wpływa na obywateli Unii, powinny zatem być ukierunkowane na człowieka, aby ludzie mogli mieć pewność, że technologię tę wykorzystuje się w sposób bezpieczny i zgodny z prawem"[4].

4. Odnosząc się bezpośrednio do treści komentowanego artykułu, należy zauważyć, że definiuje przedmiot niniejszego rozporządzenia. W ust. 1 prawodawca unijny wyjaśnił cel rozporządzenia, a w ust. 2 zawarł określenie zakresu spraw nim regulowanych. Artykuł 1 ust. 1 będzie miał przede wszystkim znaczenie w przypadku wątpliwości interpretacyjnych, gdyż wykładnia celowościowa stanowi integralną część metod interpretacyjnych TSUE, przynajmniej w formie *effet utile*[5]. Co oczywiste, wykorzystanie ogólnych celów określonych w art. 1 ust. 1 podczas wykładni jest możliwe tylko w takim zakresie, w jakim z pozostałych przepisów rozporządzenia nie można wyodrębnić bardziej szczegółowych celów.

5. W ust. 1 zostały określone najważniejsze cele AI Act, którymi są:

1) poprawa funkcjonowania rynku wewnętrznego;
2) promowanie upowszechniania zorientowanej na człowieka i godnej zaufania AI przy jednoczesnym zapewnieniu wysokiego poziomu ochrony:
   a) zdrowia i bezpieczeństwa,
   b) praw podstawowych, w tym demokracji, praworządności i ochrony środowiska przed szkodliwymi skutkami systemów AI w UE;
3) wspieranie innowacji.

Należy podkreślić, że prawodawca unijny nie ustalił hierarchii między tymi celami, co oznacza, że – przynajmniej w założeniu – są one równorzędne.

***Ad* 1.** Jednym z głównych celów AI Act jest ujednolicenie ram prawnych dotyczących funkcjonowania systemów AI w UE, „zapewniając (…) sprawne funkcjonowanie rynku wewnętrznego i obejmując systemy zasadą swobodnego przepływu towarów i usług"[6].

Ma to na celu rozwiązanie dwóch głównych problemów:

– rozdrobnienia rynku wewnętrznego, w szczególności w zakresie wymogów dla systemów AI i ich odbiorców, ich wprowadzania do obrotu, stosowania, odpowiedzialności i nadzoru organów publicznych; oraz
– zmniejszenia pewności prawnej dla podmiotów rynkowych co do tego, w jaki sposób istniejące i nowe przepisy będą miały zastosowanie do tych systemów w UE[7].

---

[2] Zob. motyw 7 preambuły AI Act.
[3] Zob. motyw 6 preambuły AI Act.
[4] Uzasadnienie AI Act, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206 (dostęp: 23.02.2025 r.).
[5] J. Blockx, *Effet utile reasoning by the Court of Justice of the European Union is mostly indirect: evidence and consequences*, „European Journal of Legal Studies" 2022/1 i przywołane tam orzecznictwo.
[6] Motyw 8 preambuły AI Act.
[7] P. Van Eecke, B. Regenhardt [w:] *The EU Artificial Intelligence (AI) Act: A Commentary*, red. C.N. Pehlivan, N. Forgó, P. Valcke, Alphen aan den Rijn 2024, art. 1, s. 10.

Fragmentaryczna regulacja, przyjęta przez różne państwa członkowskie w odmiennym zakresie, utrudniałaby działalność podmiotom chcącym wdrażać systemy AI na rynku unijnym. Państwa członkowskie, takie jak Hiszpania[8], Niemcy[9] i Włochy[10], przed przyjęciem komentowanego rozporządzenia opracowały krajowe dokumenty programowe i inicjatywy legislacyjne dotyczące AI. Niniejsze rozporządzenie poprzez harmonizację i utworzenie jednej spójnej regulacji, która ma zastosowanie we wszystkich państwach członkowskich, zapobiegło fragmentacji rynku unijnego.

Ponadto ustanawiając kompleksowe ramy regulacyjne, UE oczekuje, że inne kraje przyjmą podobne standardy i będą promować odpowiedzialne praktyki dotyczące AI w skali globalnej, „czyniąc Unię liderem w upowszechnianiu godnej zaufania AI"[11].

Mając na uwadze cel, jakim jest poprawa funkcjonowania rynku wewnętrznego, AI Act został przyjęty jako rozporządzenie, które zgodnie z art. 288 TFUE jest bezpośrednio stosowane w państwach członkowskich, bez konieczności implementowania do prawa krajowego. Wybór rozporządzenia jako formy regulacji został uzasadniony potrzebą jednolitego stosowania nowych przepisów dotyczących AI, w tym definicji systemu AI, zakazanych praktyk w zakresie AI czy klasyfikacji niektórych systemów AI.

***Ad* 2.** Kolejnym celem rozporządzenia jest promowanie upowszechniania zorientowanej na człowieka i godnej zaufania sztucznej inteligencji. Oznacza to wykorzystanie potencjału AI przy jednoczesnym zapewnieniu jej zgodności z prawami podstawowymi i wartościami UE[12]. Systemy AI powinny być wykorzystywane dla dobra ludzi i społeczeństwa, chronić ich prawa i wolności oraz przyczyniać się do poprawy jakości życia, m.in. poprzez rozwiązywanie problemów społecznych z zakresu opieki zdrowotnej, edukacji czy ochrony środowiska.

Podejście oparte na „zorientowanej na człowieka i godnej zaufania" sztucznej inteligencji pojawiło się w różnych aktach prawnych. Należą do nich m.in.: wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji[13], rezolucja Parlamentu Europejskiego zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, ro-

[8] Spanish Ministry of Science, Innovation and Universities, *Spanish RDI Strategy in Artificial Intelligence,* https://www.ciencia.gob.es/dam/jcr:d78856a6-10c2-4772-a96c-b52fc0fd3a84/SPANISHRDISTRATEGYINARTIFICIALINTELLIGENCESGT2019.pdf (dostęp: 21.02.2025 r.).

[9] Deutsches Institut für Normung e. V. (DIN), *German Standardization Roadmap on Artificial Intelligence*, www.din.de/go/roadmap-ai (dostęp: 21.02.2025 r.).

[10] Garante Per La Protezione Dei Dati Personati, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale*, 2023, https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0 (dostęp: 21.02.2025 r.).

[11] Motyw 2 preambuły AI Act. Zob. także Konwencję ramową Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności, https://rm.coe.int/1680afae3c (dostęp: 15.03.2025 r.). W trakcie negocjacji przedstawiciele niektórych państw UE podkreślali potrzebę zapewnienia zbieżności terminologicznej Konwencji z AI Act. Biorąc pod uwagę fakt, że sygnatariuszami Konwencji zostało także wiele państw spoza UE, w tym USA, Kanada czy Japonia, wypracowane ramy prawne mogą oddziaływać na poziomie globalnym, czyniąc UE liderem w upowszechnianiu godnej zaufania AI.

[12] C. Wendehorst [w:] *KI-VO: Verordnung über Künstliche Intelligenz*, red. M. Martini, C. Wendehorst, München 2024, art. 1, s. 83.

[13] Niezależna grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji powołana przez Komisję Europejską w czerwcu 2018 r., *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_PL.pdf (dostęp: 23.02.2025 r.).

botyki i powiązanych z nimi technologii[14] oraz komunikat Komisji w sprawie promowania europejskiego podejścia do sztucznej inteligencji[15].

Zorientowana na człowieka AI może być rozumiana jako skupiająca się na priorytetowym traktowaniu ludzkiego dobrostanu i poszanowaniu praw podstawowych. System AI może być uważany za godny zaufania, jeśli generuje dokładne wyniki, nie powoduje szkód dla ludzi ani społeczeństwa, zapewnia ochronę i prywatność danych, jest odporny na cyberataki, unika dyskryminacji lub niesprawiedliwego traktowania ze względu na czynniki takie jak rasa, płeć lub religia[16]. Jednocześnie godna zaufania sztuczna inteligencja jest związana z promowaniem przejrzystości poprzez umożliwienie ludziom zrozumienia, w jaki sposób systemy AI podejmują decyzje, aby kwestionować potencjalnie stronnicze wyniki.

Zgodnie z wytycznymi unijnymi „godny zaufania" system AI powinien posiadać trzy cechy:

– być zgodny z prawem, tj. przestrzegać wszystkich obowiązujących przepisów;
– być etyczny, zapewniając zgodność z zasadami i wartościami etycznymi oraz
– być solidny (ang. *robust*) zarówno z technicznego, jak i ze społecznego punktu widzenia, ponieważ systemy AI mogą wywoływać niezamierzone szkody nawet wówczas, gdy korzysta się z nich w dobrej wierze[17] oraz zgodnie z przeznaczeniem.

Prawodawca unijny w ramach AI Act przyjął regulacje pozwalające na wykorzystywanie systemów AI w bezpieczny i zgodny z prawem sposób, w tym z poszanowaniem praw podstawowych. W związku z tym koncepcja zorientowanej na człowieka i godnej zaufania sztucznej inteligencji znajduje swój wyraz w całym AI Act. Środki uwzględniające tę koncepcję obejmują:

– podejście oparte na ryzyku,
– wymogi przejrzystości dla konkretnych systemów AI, pozwalające użytkownikom zrozumieć, jak one działają i potencjalnie kwestionować stronnicze wyniki, a także
– nadzór ze strony człowieka, co ma zapewnić kontrolę nad istotnymi decyzjami.

***Ad* 2a.** Kolejnym celem rozporządzenia, który został wymieniony w art. 1 ust. 1, jest zapewnienie wysokiego poziomu ochrony zdrowia i bezpieczeństwa. Systemy AI nie powinny powodować szkód fizycznych ani psychicznych[18]. Skupienie uwagi na tych aspektach wynika z potencjalnych zagrożeń, jakie mogą stwarzać systemy AI, jeśli nie są rozwijane i wdrażane w sposób odpowiedzialny – w szczególności gdy takie systemy funkcjonują jako związane z bezpieczeństwem elementy produktów[19].

Wymóg ochrony zdrowia jest podkreślany w niemal wszystkich aktach prawnych dotyczących bezpieczeństwa produktów i nadzoru rynku, jak również w prawie pierwotnym[20].

---

[14] Rezolucja Parlamentu Europejskiego z 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii (2020/2012(INL)) (Dz.Urz. UE C 404 z 2021, s. 63).

[15] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Promowanie europejskiego podejścia do sztucznej inteligencji, COM(2021) 205 final.

[16] P. Van Eecke, B. Regenhardt [w:] *The EU Artificial…*, red. C.N. Pehlivan, N. Forgó, P. Valcke, art. 1, s. 12.

[17] Niezależna grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji powołana przez Komisję Europejską w czerwcu 2018 r., *Wytyczne…*, s. 2. Zob. także: D. Kaur, S. Uslu, K.J. Rittichier, A. Durresi, *Trustworthy Artificial Intelligence: A Review*, „ACM Computing Surveys (CSUR)" 2022/2, s. 1–38.

[18] Motyw 5 preambuły AI Act.

[19] Motyw 47 preambuły AI Act.

[20] Zob. m.in. art. 114 ust. 3 (środki dotyczące zbliżenia ustawodawstw), art. 168 (ochrona zdrowia) i art. 169 ust. 1 (ochrona interesów konsumentów) TFUE.

Ponadto jest również uwzględniany w innych aktach prawa pierwotnego UE, takich jak Karta Praw Podstawowych UE[21].

Natomiast o wysokim poziomie bezpieczeństwa mowa np. w art. 114 ust. 3 lub art. 169 ust. 1 TFUE. Wymóg ten stanowi także integralną część wszystkich przepisów dotyczących bezpieczeństwa produktów[22]. Odwoływanie się do unijnych ram prawnych dotyczących bezpieczeństwa produktów ma zagwarantować określony stopień pewności prawnej, ponieważ operatorzy mogą polegać na oczekiwaniach zbudowanych na podstawie już obowiązujących przepisów unijnych dotyczących bezpieczeństwa produktów, którym prawdopodobnie będą podlegać i które będą miały zastosowanie jako „rozwiązanie zapasowe"[23].

Należy dodać, że regulacje odnoszące się do zdrowia i bezpieczeństwa dotyczą zwłaszcza systemów AI wysokiego ryzyka. W AI Act zostały uregulowane różne wymagania z wyraźnym zamiarem złagodzenia wystąpienia zagrożenia bezpieczeństwa (zestawy danych treningowych, walidacyjnych i testowych[24]) oraz procedury zapewnienia jakości (obowiązki rejestrowania i śledzenia[25]).

***Ad* 2b.** W ust. 1 komentowanego przepisu wskazano także, że celem AI Act jest zapewnienie wysokiego poziomu ochrony praw podstawowych, w tym demokracji, praworządności i ochrony środowiska, przed szkodliwymi skutkami systemów AI w UE. Cel ten jest związany z wcześniej omówionym, czyli osiągnięciem zorientowanej na człowieka i godnej zaufania AI. Wykorzystanie systemów AI z ich specyficznymi cechami – np. nieprzejrzystością, złożonością, zależnością od danych i pewnym poziomem autonomii – może mieć wpływ na prawa podstawowe. Z tego powodu prawodawca unijny szczególnie podkreśla, że AI Act należy stosować zgodnie z wartościami UE zapisanymi m.in. w Karcie Praw Podstawowych UE[26].

Odniesienie do praw podstawowych zapisanych w Karcie należy rozumieć jako zbiorcze odniesienie do zbioru wszystkich praw w niej uregulowanych, których nie da się wymienić w sposób wyczerpujący[27]. Wśród podstawowych praw Karty, które są szczególnie uwzględniane w AI Act, znajduje się poszanowanie godności człowieka (art. 1 KPP), gdyż rozporządzenie ma na celu zapewnienie, że systemy AI nie naruszają godności człowieka, zwłaszcza w tak wrażliwych obszarach, jak identyfikacja biometryczna lub interakcja między ludźmi a maszynami. Ponadto AI Act respektuje prawo do prywatności (art. 7 KPP) i prawo do ochrony danych osobowych (art. 8 KPP), ponieważ określa szczegółowe wymagania dotyczące przetwarzania danych osobowych przez systemy AI, które uzupełniają lub precyzują rozporządzenie 2016/679. Prawodawca unijny uwzględnił w AI Act również prawo do niedyskryminacji (art. 21 KPP), gdyż istotnym aspektem rozporządzenia jest wymóg przejrzystości, uczciwości i solidności systemów AI, który odzwierciedlono m.in. w wymaganiach dotyczących danych treningowych w celu uniknięcia dyskryminacji.

Prawodawca unijny podkreślił również, że celem AI Act jest zapewnienie wysokiego poziomu ochrony środowiska. Wyznaczenie tego celu odzwierciedla rosnącą świadomość wpły-

[21] Zob. m.in. art. 2 (prawo do życia), art. 3 (prawo do integralności fizycznej), art. 35 (ochrona zdrowia) KPP.

[22] Rozporządzenie 2023/988 w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG.

[23] Motyw 166 preambuły AI Act.

[24] Zob. komentarz do art. 10.

[25] Zob. komentarz do art. 12.

[26] Motyw 6 preambuły AI Act.

[27] Nie można wykluczyć sytuacji, w której pojawią się także nowe prawa wyinterpretowane przez TSUE, tak jak kiedyś prawo do bycia zapomnianym. Potrzeba dostosowywania interpretacji i katalogu praw jest szczególnie widoczna w przypadku nowych technologii.

wu zastosowań systemów AI na środowisko, pod względem zarówno ich rozwoju (np. zużycie energii), jak i ich użytkowania (np. ślad węglowy[28])[29]. W rozporządzeniu znajduje się odwołanie do ochrony środowiska jako celu dalszego przetwarzania danych osobowych na potrzeby opracowywania określonych systemów AI w interesie publicznym w tzw. piaskownicy regulacyjnej AI[30] oraz jako do czynnika, który należy wziąć pod uwagę w kontekście opracowywania kodeksów postępowania[31]. Istotne szkody dla środowiska są również uznawane za „poważny incydent"[32].

Włączenie ochrony środowiska jako jednego z celów AI Act poddaje się krytyce[33]. Z jednej strony fakt, że rozporządzenie uwzględnia ochronę środowiska, jest postrzegany jako zbędne obciążenie regulacji elementami, które nie są bezpośrednio związane ze zorientowaną na człowieka AI. Z drugiej strony prawodawca unijny w AI Act nie zapewnił w wystarczającym stopniu, że działalność w zakresie AI będzie rozwijała się w sposób zrównoważony dla środowiska, np. nie wprowadził bardziej rygorystycznego podejścia do bieżącego zarządzania śladem środowiskowym AI – w tym obowiązkowych ocen wpływu na zrównoważony rozwój centrów danych i innych energochłonnych procesów przetwarzania danych.

***Ad* 3.** Ostatnim z celów AI Act, wymienionym w ust. 1 komentowanego artykułu, jest wspieranie innowacji. Niniejsze rozporządzenie należy stosować, „pobudzając innowacje"[34], co wskazuje, że prawodawca unijny wyraźnie uznaje ich znaczenie i promuje je na kilku poziomach. Po pierwsze, wspieranie innowacji widocznie jest w ustanowieniu zharmonizowanych ram prawnych w UE. Pozwoliło to uniknąć różnych ram prawnych na poziomie państw członkowskich i stworzyło większą pewność regulacyjną dla dostawców i operatorów systemów AI – sektora, który ze względu na jego cyfrową naturę jest oparty na transgranicznym przepływie danych i usług. Kolejnym sposobem wspierania innowacji jest promowanie opracowywania i przyjmowania standardów oraz certyfikatów dla systemów AI, a także kodeksów postępowania. Ma to na celu zachęcenie do inwestowania w nowe technologie i opracowywania innowacyjnych rozwiązań poprzez ustanowienie jasnych i przewidywalnych reguł funkcjonowania w obrocie prawnym systemów AI. W założeniu ma to nie tylko przyczynić się do rozwoju gospodarczego, lecz także – jak wynika z preambuły AI Act – uczynić UE światowym liderem w zakresie etycznego i odpowiedzialnego wykorzystania AI[35].

Ten cel mają realizować także przepisy rozdziału VI, które dotyczą środków wspierających innowacyjność, w tym tworzenia piaskownic regulacyjnych, zapewniających kon-

[28] Użytkowanie systemów AI wiąże się z ogromną produkcją ciepła, które generują serwery. Na terenie Poznania planowana jest budowa zaawansowanej instalacji do odzysku ciepła odpadowego, które jest ubocznym produktem przetwarzania danych. Zob. *Czy ciepło z serwerowni może ogrzać miasto? Rusza projekt w Poznaniu*, https://www.gramwzielone.pl/trendy/20283732/czy-cieplo-z-serwerowni-moze-ogrzac-miasto-rusza-projekt-w-poznaniu (dostęp: 5.03.2025 r.).

[29] P. Van Eecke, B. Regenhardt [w:] *The EU Artificial…*, red. C.N. Pehlivan, N. Forgó, P. Valcke, art. 1, s. 17.

[30] Zgodnie z art. 59 ust. 1 lit. a AI Act jednym z obszarów jest „wysoki poziom ochrony środowiska i poprawa jego jakości, ochrona różnorodności biologicznej, ochrona przed zanieczyszczeniem, środki w zakresie transformacji ekologicznej, środki w zakresie łagodzenia zmiany klimatu i przystosowania się do niej".

[31] Zgodnie z art. 95 ust. 2 lit. b AI Act podczas opracowywania kodeksów postępowania należy wziąć pod uwagę m.in. element, jakim jest „ocena i minimalizacja oddziaływania systemów AI na zrównoważenie środowiskowe, w tym w odniesieniu do energooszczędnego programowania i technik wydajnego projektowania, trenowania i wykorzystywania AI".

[32] Zob. komentarz do art. 3 pkt 49.

[33] P. Van Eecke, B. Regenhardt [w:] *The EU Artificial…*, red. C.N. Pehlivan, N. Forgó, P. Valcke, art. 1, s. 17–18.

[34] Motyw 2 preambuły AI Act.

[35] Motyw 2 preambuły AI Act.

trolowane środowisko ułatwiające opracowywanie, testowanie i walidację innowacyjnych systemów AI przez ograniczony czas przed wprowadzeniem ich do obrotu lub oddaniem do użytku. Odbywa się to pod nadzorem właściwych organów, aby zapewnić zgodność z wymogami AI Act i innych przepisów. Ponadto w art. 60 przyjęto regulację umożliwiającą prowadzenie testów systemów AI wysokiego ryzyka w warunkach rzeczywistych poza piaskownicami regulacyjnymi. To z kolei ma pomóc przedsiębiorstwom rozwijającym systemy AI w zbieraniu opinii i dostosowywaniu produktów przed ich wprowadzeniem na rynek, a także dostarczyć organom regulacyjnym ważnych informacji, w jaki sposób w przyszłości można dostosować ramy prawne w sposób sprzyjający innowacjom[36].

Można w tym zakresie wyrazić pewną wątpliwość dotyczącą tego, czy przyjęte regulacje rzeczywiście promują innowacyjność. Rozwój, wdrażanie i użytkowanie systemów AI (zwłaszcza tych wysokiego ryzyka) są restrykcyjnie uregulowane w AI Act. Podobnie bariery wejścia na europejski rynek start-upów zajmujących się AI są na tyle wysokie, że można się spodziewać, iż przedsiębiorstwa będą wybierać państwa z bardziej przyjaznymi regulacjami prawnymi, np. z Azji Wschodniej. Prawodawca unijny w praktyce wyraźnie przyznał pierwszeństwo ochronie praw podstawowych przed swobodnym rozwojem działalności w zakresie systemów AI. Takie założenie może ograniczać rozwój wybranych zastosowań AI, co sprawi, że Europa, która już jest określana przez niektórych jako „technologiczny skansen", nadal będzie tak postrzegana. Regulacja przyjęta w AI Act może być zatem krytykowana za to, że nie stworzyła całościowych możliwości rozwoju i użytkowania systemów AI oraz niedostatecznie wspiera innowacyjność[37].

6. Z kolei w ust. 2 komentowanego artykułu znalazło się określenie zakresu spraw regulowanych rozporządzeniem. Wskazano, że w rozporządzeniu ustanawia się:

1) zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów AI w Unii;
2) zakazy dotyczące niektórych praktyk w zakresie AI;
3) szczególne wymogi dotyczące systemów AI wysokiego ryzyka oraz obowiązki spoczywające na operatorach takich systemów;
4) zharmonizowane przepisy dotyczące przejrzystości w przypadku niektórych systemów AI;
5) zharmonizowane przepisy dotyczące wprowadzania do obrotu modeli AI ogólnego przeznaczenia;
6) przepisy dotyczące monitorowania wprowadzania do obrotu, nadzoru rynku, zarządzania i egzekwowania;
7) środki wspierające innowacje, ze szczególnym uwzględnieniem MŚP, w tym przedsiębiorstw typu startup.

Powyższe zagadnienia są przedmiotem regulacji AI Act i pozostają częściowo zgodne z nagłówkami kolejnych rozdziałów rozporządzenia.

***Ad* 1.** W ust. 2 lit. a wskazano, że w rozporządzeniu ustanawia się zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów AI w UE. Przepis ten określa zakres materialny, osobowy i terytorialny AI Act, mając na względzie cel, jakim jest poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych dotyczących AI.

[36] C. Wendehorst [w:] *KI-VO: Verordnung…*, red. M. Martini, C. Wendehorst, art. 1, s. 86.
[37] Podobnie: P. Van Eecke, B. Regenhardt [w:] *The EU Artificial…*, red. C.N. Pehlivan, N. Forgó, P. Valcke, art. 1, s. 18 oraz przywołana tam literatura.

***Ad* 2.** Z kolei w ust. 2 lit. b wskazano na zakazy dotyczące niektórych praktyk w zakresie AI, co odpowiada treści normatywnej zamieszczonej w rozdziale II „Zakazane praktyki"[38]. W przywołanym rozdziale ustanowiono listę zakazanych praktyk w zakresie AI, obejmującą wszystkie systemy AI, których stosowanie jest uważane za niedopuszczalne z uwagi na fakt, że naruszają wartości unijne i prawa podstawowe. Należą do nich np. systemy AI, które wykorzystują techniki manipulacyjne w celu nakłonienia ludzi do angażowania się w szkodliwe zachowania.

***Ad* 3.** Natomiast w ust. 2 lit. c wskazano, że w rozporządzeniu ustanawia się szczególne wymogi dotyczące systemów AI wysokiego ryzyka oraz obowiązki spoczywające na operatorach takich systemów, co jest skorelowane z treścią rozdziału III „Systemy AI wysokiego ryzyka" (art. 6–49). Rozdział III zawiera szczegółowe przepisy dotyczące systemów Al wysokiego ryzyka, które są dozwolone na rynku UE pod warunkiem spełnienia pewnych obowiązkowych wymagań i oceny zgodności przed ich wdrożeniem. Oprócz przepisów dotyczących klasyfikacji systemu AI jako systemu wysokiego ryzyka rozdział ten określa wymogi prawne, które operatorzy tych systemów muszą następnie spełnić, w tym obowiązki przejrzystości lub wymóg przeprowadzenia oceny wpływu na prawa podstawowe. Dotyczy on również ram procedur oceny zgodności.

***Ad* 4.** W ust. 2 lit. d wskazano na zharmonizowane przepisy dotyczące przejrzystości w przypadku niektórych systemów AI, co odpowiada rozdziałowi IV „Obowiązki w zakresie przejrzystości dla dostawców i podmiotów stosujących niektóre systemy AI" (art. 50). Rozdział ten nakłada obowiązki przejrzystości na dostawców niektórych systemów AI, aby uwzględnić ryzyko manipulacji, jakie one stwarzają. Obowiązki objęte tym rozdziałem dotyczą dostawców systemów AI, w tym systemów AI ogólnego przeznaczenia, generujących syntetyczną treść audio, obrazu, wideo lub tekstu lub wdrażających systemy, które generują tekst publikowany w celu informowania opinii publicznej o sprawach będących w interesie publicznym lub manipulują takim tekstem.

***Ad* 5.** W ust. 2 lit. e wskazano, że w rozporządzeniu ustanawia się zharmonizowane przepisy dotyczące wprowadzania do obrotu modeli AI ogólnego przeznaczenia, co odpowiada rozdziałowi V „Modele Al ogólnego przeznaczenia" (art. 51–56). W przywołanym rozdziale zostały określone obowiązki dotyczące modeli AI ogólnego przeznaczenia, które są uporządkowane w ramach czterech sekcji:

– zasady klasyfikacji,
– obowiązki dostawców modeli AI ogólnego przeznaczenia,
– obowiązki dostawców modeli AI ogólnego przeznaczenia z ryzykiem systemowym oraz
– kodeksy praktyk.

W rozdziale V rozróżniono obowiązki, które mają zastosowanie do wszystkich modeli AI ogólnego przeznaczenia oraz obowiązki dotyczące modeli z ryzykiem systemowym. Dostawcy modeli AI ogólnego przeznaczenia muszą m.in. tworzyć i utrzymywać dokumentację techniczną, opracować zasady dotyczące przestrzegania prawa autorskiego oraz utworzyć szczegółowe podsumowanie treści używanych do trenowania modelu. Dodatkowe obowiązki dotyczą dostawców modeli z ryzykiem systemowym, w tym przeprowadzania ocen modeli oraz oceny i łagodzenia ryzyka systemowego.

***Ad* 6.** Z kolei ust. 2 lit. f wskazuje na przepisy dotyczące monitorowania wprowadzania do obrotu, nadzoru rynku, zarządzania i egzekwowania, co odpowiada treściowo rozdziało-

[38] Zob. komentarz do art. 5.

wi IX „Monitorowanie po wprowadzeniu do obrotu, wymiana informacji oraz nadzór rynku" (art. 72–94). Rozdział ten obejmuje w pięciu sekcjach obowiązki takie, jak:
- monitorowanie po wprowadzeniu do obrotu,
- wymiana informacji na temat poważnych incydentów,
- egzekwowanie,
- środki ochrony prawnej oraz
- nadzór, postępowania, egzekwowanie i monitorowanie w odniesieniu do dostawców modeli AI ogólnego przeznaczenia.

Ad 7. Ostatnim zagadnieniem znajdującym się w zakresie spraw regulowanych rozporządzeniem, zgodnie z ust. 2 lit. g, są środki wspierające innowacje, ze szczególnym uwzględnieniem MŚP, w tym przedsiębiorstw typu startup. Te treści zostały dookreślone w rozdziale VI „Środki wspierające innowacyjność" (art. 57–63). Rozdział VI w założeniu ma stwarzać ramy prawne przyjazne innowacjom poprzez ustanowienie piaskownic regulacyjnych w zakresie AI, możliwość testowania systemów AI wysokiego ryzyka w warunkach rzeczywistych poza piaskownicami regulacyjnymi w zakresie AI oraz podstawowych ram w zakresie środków na rzecz dostawców i podmiotów stosujących, w szczególności MŚP, w tym przedsiębiorstw typu startup.

W zakresie spraw regulowanych rozporządzeniem, określonym w komentowanym art. 1 ust. 2, nie wymieniono wprost rozdziału VII „Zarządzanie" (art. 64–70), rozdziału VIII „Baza danych UE dla systemów AI wysokiego ryzyka" (art. 71), rozdziału X „Kodeksy postępowania i wytyczne" (art. 95–96), rozdziału XI „Delegowanie uprawnień i procedura komitetowa" (art. 97–98), rozdziału XII „Kary" (art. 99–101) i rozdziału XIII „Postanowienia końcowe" (art. 102–113). Rozdziały te nie zawierają postanowień istotnych bezpośrednio dla operatorów, ale bez tych regulacji AI Act nie spełniałby skutecznie swojego celu (np. norm sankcjonujących przewidzianych w rozdziale XII).

Maria Jędrzejczak

Artykuł 2
Zakres stosowania

1. Niniejsze rozporządzenie stosuje się do:

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

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

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

d) importerów i dystrybutorów systemów AI;

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

f) upoważnionych przedstawicieli dostawców niemających siedziby w Unii;

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

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

3. Niniejszego rozporządzenia nie stosuje się do obszarów wykraczających poza zakres stosowania prawa Unii i w żadnym wypadku nie wpływa ono na kompetencje państw członkowskich w zakresie bezpieczeństwa

narodowego, niezależnie od rodzaju podmiotu, któremu państwa członkowskie powierzyły wykonywanie zadań związanych z tymi kompetencjami.

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

Niniejszego rozporządzenia nie stosuje się do systemów AI, które nie zostały wprowadzone do obrotu ani oddane do użytku w Unii, a których wyniki są wykorzystywane w Unii wyłącznie do celów wojskowych, obronnych lub de celów bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu prowadzącego te działania.

4. Niniejszego rozporządzenia nie stosuje się do organów publicznych w państwie trzecim ani do organizacji międzynarodowych objętych zakresem stosowania niniejszego rozporządzenia na podstawie ust. 1, jeżeli te organy lub organizacje wykorzystują systemy AI w ramach współpracy międzynarodowej lub umów międzynarodowych w sprawie ścigania przestępstw i współpracy sądowej zawartych z Unią lub z jednym państwem członkowskim bądź ich większą liczbą, pod warunkiem zapewnienia przez to państwo trzecie lub organizację międzynarodową odpowiednich zabezpieczeń w odniesieniu do ochrony podstawowych praw i wolności osób fizycznych.

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

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

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

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

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

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

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

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

1. Komentowany artykuł określa przedmiotowy, podmiotowy i terytorialny zakres stosowania AI Act. W ogólności można stwierdzić, że art. 2 wprowadza w życie podstawowy cel rozporządzenia, jakim jest zapewnienie swobodnego, transgranicznego przepływu towarów i usług opartych na AI, zapobiegając w ten sposób nakładaniu przez państwa członkowskie ograniczeń na rozwój i użytkowanie systemów AI, chyba że rozporządzenie wyraźnie na to pozwala. W art. 2 wymieniono również adresatów regulacji, którzy powinni wypełniać obowiązki wynikające z AI Act. Ponadto komentowany artykuł definiuje zakres obowiązywania rozporządzenia ze znacznym skutkiem eksterytorialnym. Każde z postanowień art. 2 ust. 1 lit. a–g odnosi się do terytorium UE lub do tego, czy sytuacja ma miejsce w UE. Wreszcie art. 2 wskazuje sytuacje, w których AI Act nie ma zastosowania, jak też przewiduje jego związek z innymi przepisami unijnymi i państw członkowskich.

2. Artykuł 2 nie jest jedyną regulacją w AI Act, która ma znaczenie dla zakresu stosowania rozporządzenia. Komentowany przepis posługuje się pojęciami, które zostały zdefiniowane

w art. 3. Z tego powodu również słowniczek zawarty w art. 3 i zamieszczone w nim definicje odgrywają ważną rolę przy określaniu przedmiotowego i podmiotowego zakresu stosowania rozporządzenia[39].

3. Brak uporządkowania przepisów zamieszczonych w art. 2 wskazuje, że podczas opracowywania tak tego, jak też niektórych dalszych przepisów rozporządzenia nie poświęcono wystarczająco dużo uwagi właściwemu pogrupowaniu różnych treści regulacyjnych. W art. 2 ust. 1 zdefiniowano zakres zastosowania zarówno podmiotowego, jak i terytorialnego. Natomiast ust. 2, 3, 6, 8 i 12 służą doprecyzowaniu przedmiotowego zakresu stosowania rozporządzenia, a w szczególności wyłączeniu niektórych systemów AI z tego zakresu. Z kolei ust. 10 przewiduje wyjątek od zakresu zastosowania dotyczącego osoby fizycznej. Przepis zawarty w ust. 4 przewiduje dalszy wyjątek, który może dotyczyć zakresu zarówno przedmiotowego, jak i podmiotowego zastosowania. Natomiast ust. 5, 7 i 9 dotyczą związku AI Act z innymi aktami prawnymi na szczeblu unijnym. Ustęp 11 również należy do tej kategorii, ale odnosi się bezpośrednio do zakresu harmonizacji, jaki ma zostać osiągnięty dzięki rozporządzeniu.

4. W art. 2 ust. 1 uregulowano zakres podmiotowy stosowania rozporządzenia poprzez wymienienie podmiotów, dla których rozporządzenie ustanawia określone prawa i obowiązki. Wskazana w ust. 1 lista nie jest wyczerpująca, gdyż adresatami regulacji są również organy oraz inne podmioty unijne i krajowe (np. organy notyfikujące lub jednostki notyfikowane). Także podmioty gospodarcze objęte zakresem normowania AI Act nie zostały wymienione w wyczerpujący sposób, np. brakuje osób trzecich dostarczających system AI, o których mowa w art. 25 ust. 4. Zakres stosowania podmiotowego jest zatem uzupełniany przez pojedyncze przepisy AI Act, z których wynika, kto jest adresatem danej regulacji. Z tego względu art. 2 ust. 1 może być uznawany za bardziej odpowiedni dla określenia terytorialnego zakresu stosowania[40]. W AI Act, podobnie jak w wielu innych rozporządzeniach unijnych, określony został własny terytorialny zakres stosowania, rozszerzony na podmioty mające siedzibę lub działające poza terytorium UE, co określa się mianem skutku eksterytorialnego. Przykładowo taki rozszerzony zakres stosowania jest uzasadniony w sytuacji, gdy przedsiębiorca mający siedzibę w państwie trzecim wchodzi na rynek unijny ze swoimi produktami lub usługami.

5. Zgodnie z art. 2 ust. 1 lit. a niniejsze rozporządzenie stosuje się do dostawców[41] wprowadzających do obrotu lub oddających do użytku systemy AI lub wprowadzających do obrotu[42] modele AI ogólnego przeznaczenia w UE, niezależnie od tego, czy dostawcy ci mają siedzibę lub znajdują się w UE, czy w państwie trzecim. Wynika to z przyjęcia założenia, że przepisy AI Act powinny mieć zastosowanie do dostawców systemów AI w sposób niedyskryminacyjny, niezależnie od tego, czy mają oni siedzibę w UE, czy w państwie trzecim. Uwzględniając w zakresie stosowania dostawców krajowych i zagranicznych, AI Act ma na celu również zapobieganie budowaniu przewagi konkurencyjnej u dostawców spoza UE, którzy mogliby nie podlegać podobnym przepisom.

[39] Dotyczy to w szczególności definicji „systemu AI" – zob. komentarz do art. 3 pkt 1.
[40] C. Wendehorst [w:] *KI-VO: Verordnung…*, red. M. Martini, C. Wendehorst, art. 2, s. 107.
[41] Zob. art. 3 pkt 3.
[42] Zob. art. 3 ust. 9.