Rada
Unii Europejskiej

Bruksela, 20 listopada 2025 r.
(OR. en)

15698/25

Międzyinstytucjonalny numer referencyjny:
2025/0360 (COD)

SIMPL 186
ANTICI 185
DATAPROTECT 307
CYBER 337
TELECOM 417
PROCIV 155
CODEC 1872

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	20 listopada 2025 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2025) 837 final
Dotyczy:	Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie zmiany rozporządzeń (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektyw 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram prawnych oraz uchylenia rozporządzeń (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 i dyrektywy (UE) 2019/1024 (akt zbiorczy prawa cyfrowego)

Delegacje otrzymują w załączeniu dokument COM(2025) 837 final.

Zał.: COM(2025) 837 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 19.11.2025 r.
COM(2025) 837 final

2025/0360 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zmiany rozporządzeń (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektyw 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram prawnych oraz uchylenia rozporządzeń (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 i dyrektywy (UE) 2019/1024 (akt zbiorczy prawa cyfrowego)

{SWD(2025) 836 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W swoim komunikacie dotyczącym wdrażania i upraszczania („Prostsza i szybsza Europa”)[1] Komisja przedstawiła swoje podejście do dostosowania unijnych ram regulacyjnych do bardziej niestabilnego świata: nowe działania, aby uprościć, wyjaśnić i usprawnić dorobek prawny UE, jako kluczowy środek wspierania konkurencyjności UE.

Wizja ta odzwierciedla szerzej zakrojony plan, jaki przewodnicząca Komisji Ursula von der Leyen przedstawiła w swoich wytycznych politycznych na kadencję 2024–2029[2]. Jak również podkreślono w raportach Draghiego[3] i Letty[4], kumulacja przepisów ma niekiedy negatywny wpływ na konkurencyjność. Obywatele i przedsiębiorstwa wymagają szybkich i widocznych usprawnień dzięki bardziej racjonalnemu pod względem kosztów i sprzyjającemu innowacjom wdrażaniu przepisów, przy jednoczesnym zachowaniu wysokich standardów i uzgodnionych celów.

W konkluzjach Rady Europejskiej z dnia 20 marca 2025 r. apelowano ponadto do Komisji, by „w dalszym ciągu prowadziła przegląd dorobku prawnego UE i poddawała ten dorobek testom warunków skrajnych w celu określenia sposobów dalszego uproszczenia i skonsolidowania obowiązujących przepisów”[5]. Podkreślono również potrzebę przedstawienia nowych zestawów inicjatyw uproszczeniowych. W konkluzjach z dnia 26 czerwca Rada Europejska podkreśliła znaczenie przepisów opartych na „prostocie z założenia”, „bez narażania na szwank przewidywalności, celów polityki i wysokich standardów”[6]. W konkluzjach Rady Europejskiej z dnia 23 października 2025 r. potwierdzono „pilną potrzebę przeprowadzenia ambitnego i horyzontalnego programu upraszczania przepisów i lepszego stanowienia prawa na wszystkich szczeblach – unijnym, krajowym i regionalnym – i we wszystkich obszarach, by zapewnić konkurencyjność Europy”. Zaapelowano również do Komisji o „pilne przedstawienie dalszych, ambitnych pakietów w sprawie uproszczenia dotyczących m.in. […] cyfryzacji”[7].

W rezolucji w sprawie wdrożenia i usprawnienia zasad rynku wewnętrznego UE w celu umocnienia jednolitego rynku, przegłosowanej 11 września na posiedzeniu plenarnym[8],

---

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Prostsza i szybsza Europa: komunikat dotyczący wdrażania i upraszczania”, COM(2025) 47 final, 11 lutego 2025 r.

[2] Ursula von der Leyen (2024), „Wybór Europy: wytyczne polityczne na następną kadencję Komisji Europejskiej (2024–2029)”. Dokument dostępny na stronie: e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

[3] M. Draghi, 2024, „Przyszłość europejskiej konkurencyjności. Dokument dostępny na stronie: Raport Draghiego na temat konkurencyjności UE.

[4] Letta, E. (2024), „Much more than a market” [Znacznie więcej niż rynek]. Dokument dostępny na stronie: Enrico Letta – Much more than a market (kwiecień 2024).

[5] Rada Europejska, konkluzje, EUCO 1/25, Bruksela, 20 marca 2025 r., pkt 13

[6] Rada Europejska, konkluzje, EUCO 12/25, Bruksela, 26 czerwca 2025 r., pkt 30.

[7] Rada Europejska, konkluzje, EUCO 18/25, Bruksela, 23 października 2025 r., pkt 33 i 35.

[8] Parlament Europejski, rezolucja w sprawie wdrożenia i usprawnienia zasad rynku wewnętrznego UE w celu umocnienia jednolitego rynku, 11 września 2025 r. (2025/2009/INI).

Parlament Europejski podkreślił potrzebę uproszczenia, aby ułatwić przestrzeganie przepisów przez przedsiębiorstwa bez uszczerbku dla głównych celów polityki UE.

W ramach prowadzonych przez Komisję działań w zakresie konsultacji i współpracy dotyczących programu uproszczenia zainteresowane strony reprezentujące różne interesy wezwały do ukierunkowanych zmian niektórych przepisów dotyczących sektora cyfrowego, aby zarówno zracjonalizować koszty przestrzegania przepisów, jak i wyjaśnić wzajemne zależności między przepisami w ich sektorze.

Sektor ICT, którego wartość dodana w całej Unii Europejskiej wynosiła w 2022 r. 791 mld EUR[9], odgrywa kluczową rolę w pobudzaniu konkurencyjności UE we wszystkich sektorach gospodarki, zarówno przez rozwój przedsiębiorstw cyfrowych, jak i oferowanie kluczowych rozwiązań cyfrowych w całej rozciągłości. Przepisy dotyczące sektora cyfrowego odegrały zasadniczą rolę w kształtowaniu sprawiedliwego otoczenia biznesowego w UE. Dzięki nim powstał prawdziwy jednolity rynek usług cyfrowych. UE stała się pionierem w dziedzinie regulacji usług cyfrowych i ustanowiła wzorzec najwyższych standardów ochrony praw podstawowych, bezpieczeństwa konsumentów i europejskich wartości.

Komisja zobowiązała się do przeprowadzania kompleksowego testu warunków skrajnych w odniesieniu do zbioru prawa cyfrowego w trakcie całej kadencji ustawodawczej. Cel jest bardzo jasny: zagwarantowanie, by przepisy były nadal odpowiednie do wspierania innowacji i wzrostu gospodarczego, służyły osiąganiu ich celów oraz były siłą napędową konkurencyjności. W trakcie tego procesu Komisja będzie dążyć do zapewnienia przekonujących rozwiązań w celu uproszczenia, wyjaśnienia i wzmocnienia skuteczności przepisów i ich egzekwowania za pomocą wszystkich dostępnych instrumentów, czy to dostosowań regulacyjnych, wzmocnionej współpracy między organami, promowania rozwiązań cyfrowych, które upraszczają zgodność regulacyjną w fazie projektowania, czy też innych środków towarzyszących.

Wniosek dotyczący aktu zbiorczego prawa cyfrowego jest pierwszym krokiem w kierunku optymalizacji stosowania zbioru prawa cyfrowego. Obejmuje on szereg zmian technicznych w dużym zbiorze przepisów cyfrowych, wybranych w celu zapewnienia natychmiastowej pomocy przedsiębiorstwom, podmiotom administracji publicznej i obywatelom, aby pobudzić konkurencyjność. Bezpośrednim celem jest zapewnienie, aby przestrzeganie przepisów wiązało się z niższymi kosztami, realizowało te same cele i samo w sobie zapewniało przewagę konkurencyjną odpowiedzialnym przedsiębiorstwom. Zmiany uszeregowano pod względem ważności w oparciu o konsultacje z zainteresowanymi stronami i pierwsze dialogi na temat wdrażania przeprowadzone przez wiceprzewodniczącą wykonawczą Hennę Virkkunen i komisarza Michaela McGratha.

Z tych powodów zmiany koncentrują się na odblokowaniu możliwości wykorzystania danych jako podstawowego zasobu w gospodarce UE, zwłaszcza w celu wspierania rozwoju i stosowania godnych zaufania rozwiązań w zakresie sztucznej inteligencji na rynku UE.

---

[9] Eurostat (2025) *Statistics explained: Sektor ICT – wartość dodana, zatrudnienie oraz badania i rozwój*. Dokument dostępny na stronie: Sektor ICT – wartość dodana, zatrudnienie oraz badania i rozwój – Statistics Explained – Eurostat.

Ukierunkowane zmiany przepisów dotyczących ochrony danych i prywatności wspierają ten cel oraz zapewniają natychmiastowe środki upraszczające dla przedsiębiorstw i osób fizycznych, zwiększając ich zdolność do korzystania z przysługujących im praw.

Ponadto zmiany w rozporządzeniu (UE) 2024/1689 (akt w sprawie sztucznej inteligencji[10]), przedstawione w odrębnym wniosku ustawodawczym stanowiącym część pakietu aktów zbiorczych prawa cyfrowego, mają na celu ułatwienie sprawnego i skutecznego stosowania przepisów na rzecz bezpiecznego i godnego zaufania rozwoju i wykorzystania AI.

W akcie zbiorczym prawa cyfrowego proponuje się również bardzo jasne rozwiązanie służące usprawnieniu zgłaszania incydentów cyberbezpieczeństwa, łączące w ramach jednolitego mechanizmu zgłaszania wszystkie powiązane obowiązki sprawozdawcze.

Ponadto wniosek uchyla przestarzałe przepisy w dziedzinie regulacji platform, zastąpione nowszymi rozporządzeniami.

Zmiany mają na celu usprawnienie przepisów, zmniejszając ich liczbę i zapewniając ich harmonizację. Obniżają koszty administracyjne przez uproszczenie przepisów i procedur. Zwalniają małe spółki o średniej kapitalizacji z niektórych obowiązków wynikających z przepisów dotyczących danych i rozporządzenia (UE) 2024/1689 (akt w sprawie sztucznej inteligencji[11]), oprócz małych przedsiębiorstw i mikroprzedsiębiorstw już objętych specjalnym systemem. Stymulują również możliwości stworzenia dynamicznego otoczenia biznesowego, zapewniając większą pewność prawa i możliwości, w szczególności w zakresie dzielenia się danymi i ponownego wykorzystywania danych, przetwarzania danych osobowych lub trenowania systemów i modeli sztucznej inteligencji.

Jednocześnie proponowane zmiany zachowują charakter techniczny i mają na celu dostosowanie ram regulacyjnych, a nie zmianę ich podstawowych celów. Środki skalibrowano w taki sposób, aby zachować taki sam standard ochrony praw podstawowych.

Wraz z aktem zbiorczym prawa cyfrowego Komisja przedstawia również wniosek dotyczący **rozporządzenia w sprawie europejskich portfeli biznesowych** jako podstawową inicjatywę mającą na celu uproszczenie zgodności regulacyjnej i zmniejszenie obciążeń administracyjnych dla przedsiębiorstw. Portfele biznesowe zostaną zaprojektowane jako bezpieczne narzędzia cyfrowe dla przedsiębiorstw, działające jako jednolita platforma w celu uproszczenia ich interakcji w całej UE. Dzięki wdrożeniu unikalnego i trwałego identyfikatora przedsiębiorstwa będą uprawnione do cyfrowej weryfikacji tożsamości, podpisywania dokumentów, stosowania znacznika czasu i sprawnej transgranicznej wymiany zweryfikowanych informacji cyfrowych za pomocą jednego rozwiązania. Dzięki przyjęciu europejskich portfeli biznesowych przedsiębiorstwa, zwłaszcza MŚP, będą mogły łatwo radzić sobie z przestrzeganiem przepisów, uwalniając istotne zasoby, które można przekierować na wzrost gospodarczy i innowacje.

[10] Zgodnie z odrębnym wnioskiem ustawodawczym.
[11] Zgodnie z odrębnym wnioskiem.

W ramach drugiego etapu zobowiązania do przeprowadzenia testu warunków skrajnych w odniesieniu do zbioru prawa cyfrowego **Komisja przeprowadza również ocenę adekwatności przepisów cyfrowych**. Podczas gdy wnioski w ramach pakietu aktów zbiorczych prawa cyfrowego mają bezpośredni i ukierunkowany charakter, analiza, którą Komisja przeprowadzi w ramach oceny adekwatności przepisów cyfrowych, skoncentruje się na skumulowanym oddziaływaniu przepisów dotyczących sektora cyfrowego, aby sprawdzić, w jaki sposób wspierają one konkurencyjność UE i w jakich obszarach konieczne będzie zaproponowanie dalszych dostosowań w drugiej połowie kadencji ustawodawczej.

Rozpoczęcie oceny adekwatności przepisów cyfrowych zbiega się w czasie z przedstawieniem wniosku dotyczącego aktu zbiorczego, wraz z szeroko zakrojonymi konsultacjami publicznymi. Komisja dąży do nawiązania współpracy ze wszystkimi zainteresowanymi stronami i przeprowadzenia szeroko zakrojonych konsultacji. Celem jest realizacja działań następczych w postaci przeglądu i szeroko zakrojonego zestawienia sposobów, w jakie zbiór prawa cyfrowego obejmuje strategiczne sektory przemysłu UE, oraz zajęcie się wpływem łącznych skutków przepisów na ich konkurencyjność. Na tej podstawie analiza zostanie pogłębiona na drugim etapie dotyczącym synergii i obszarów, które można jeszcze bardziej ujednolicić, począwszy od definicji i pojęć prawnych, a skończywszy na skuteczności i wzajemnym oddziaływaniu systemów zarządzania i innych środków wspierających.

Kontynuacja testu warunków skrajnych w odniesieniu do cyfrowego dorobku prawnego UE będzie również odbywać się w drodze dialogów na temat wdrażania, a także **ocen wszystkich głównych instrumentów prawnych**. W ramach obecnego planowania Komisja oczekuje m.in. opublikowania w 2026 r. przeglądu aktu o rynkach cyfrowych, programu polityki „Droga ku cyfrowej dekadzie”, aktu w sprawie czipów i dyrektywy o audiowizualnych usługach medialnych oraz oceny dyrektywy w sprawie prawa autorskiego. Akty, których oceny oczekuje się w 2027 r., obejmują m.in. akt w sprawie cybersolidarności, rozporządzenie w sprawie otwartego internetu, dyrektywę NIS 2 i akt o usługach cyfrowych. W 2028 r. Komisja powinna przeprowadzić ocenę na przykład europejskiego aktu o wolności mediów i aktu w sprawie danych, a następnie w 2029 r. ocenę aktu w sprawie AI oraz ocenę klauzuli wygaśnięcia rozporządzenia ustanawiającego Europejskie Centrum i Sieć Kompetencji w dziedzinie Cyberbezpieczeństwa.

Zainteresowane strony wielokrotnie podkreślały, że w wielu przypadkach działania na rzecz uproszczenia polegają w mniejszym stopniu na zmianie przepisów, a w większym na zapewnieniu jasności co do ich stosowania. **Komisja priorytetowo traktuje szereg wytycznych** mających na celu wspieranie jednolitego stosowania przepisów, bez uszczerbku dla wykładni Trybunału Sprawiedliwości.

Jeżeli chodzi o ramy regulacyjne dotyczące danych, Komisja ogłosiła ich priorytetowe traktowanie w strategii na rzecz europejskiej unii danych, koncentrując się w szczególności na wytycznych dotyczących rozsądnej rekompensaty w celu wyjaśnienia, jakie opłaty można pobierać za dzielenie się danymi, przy zapewnieniu pewności prawa zarówno posiadaczom danych, jak i odbiorcom danych, a także na wytycznych dotyczących wyjaśnienia definicji.

Aby wesprzeć stosowanie aktu w sprawie sztucznej inteligencji, Komisja nadal priorytetowo traktuje wydawanie wytycznych dotyczących kilku aspektów, jak szczegółowo opisano w uzasadnieniu wniosku dotyczącego pakietu aktów zbiorczych prawa cyfrowego zmieniającego akt w sprawie sztucznej inteligencji.

Wnioski zawarte w akcie zbiorczym prawa cyfrowego

„Dorobek prawny UE w zakresie danych” rozszerzono w ostatnich latach o szereg rozporządzeń, co skutkowało złożonością prawną, w tym pewnym nakładaniem się przepisów, niedoskonałym dostosowaniem definicji i pytaniami dotyczącymi wzajemnych zależności między instrumentami. W szczególności przyjęto rozporządzenie (UE) 2018/1807 (rozporządzenie w sprawie swobodnego przepływu danych nieosobowych), które miało na celu stworzenie jednolitego rynku usług w chmurze. Częściowo zastąpiono je rozdziałem VI rozporządzenia (UE) 2023/2854 (akt w sprawie danych), w którym określono obowiązki w zakresie zmiany dostawcy usług przetwarzania danych.

Innym przykładem jest rozdział II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi), który uzupełnia przepisy dotyczące ponownego wykorzystywania informacji sektora publicznego zawarte w dyrektywie (UE) 2019/1024 (dyrektywa w sprawie otwartych danych) w odniesieniu do danych, których nie można ponownie wykorzystywać bez ograniczeń. Ponadto w innych rozdziałach rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) ustanowiono przepisy dotyczące usług pośrednictwa danych, altruizmu danych i wymogów dotyczących wniosków rządów zagranicznych o dostęp do danych nieosobowych oraz utworzono Europejską Radę ds. Innowacji w zakresie Danych. Z drugiej strony w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) nałożono na producentów urządzeń podłączonych do internetu i dostawców usług powiązanych istotne zobowiązanie do dzielenia się danymi z użytkownikami, natomiast na przedsiębiorstwa nałożono obowiązek dzielenia się danymi z agencjami rządowymi, a także ustanowiono przepisy dotyczące sprawiedliwych umów w sprawie dzielenia się danymi.

Aby zająć się tą kwestią, w akcie zbiorczym proponuje się uchylenie przestarzałych przepisów, w szczególności obecnych przepisów rozporządzenia (UE) 2018/1807 (rozporządzenie w sprawie swobodnego przepływu danych nieosobowych), z wyjątkiem zakazu stosowania wymogów dotyczących lokalizacji danych w Unii, oraz konsolidację i usprawnienie przepisów rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi), takich jak przepisy dotyczące altruizmu danych i usług pośrednictwa danych, w celu zwiększenia atrakcyjności tych mechanizmów dzielenia się danymi. Jednocześnie przepisy aktu w sprawie zarządzania danymi dotyczące ponownego wykorzystywania danych chronionych połączono z przepisami dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych), aby stworzyć jednolite ramy ponownego wykorzystywania danych będących w posiadaniu organów sektora publicznego, odzwierciedlone w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych). Rozwiązanie to przynosi liczne korzyści administracjom publicznym posiadającym dane sektora publicznego, a także ponownym użytkownikom, ponieważ może usprawnić procesy i zmniejszyć obciążenie administracyjne związane z wykładnią i wdrażaniem różnych przepisów krajowych.

We wniosku wprowadzono ponadto możliwość określania przez organy sektora publicznego różnych warunków i pobierania wyższych opłat za ponowne wykorzystywanie przez bardzo duże przedsiębiorstwa, a w szczególności przedsiębiorstwa wskazane jako strażnicy dostępu, zgodnie z definicją zawartą w art. 3 rozporządzenia (UE) 2022/1925 (akt o rynkach cyfrowych), o znaczącej pozycji i wpływie na rynek wewnętrzny. Aby uniemożliwić takim podmiotom wykorzystanie swojej znaczącej pozycji rynkowej ze szkodą dla uczciwej konkurencji i innowacji, organy sektora publicznego muszą mieć możliwość określenia szczególnych warunków ponownego wykorzystywania danych i dokumentów przez takie podmioty.

Wniosek włącza skonsolidowane i usprawnione przepisy rozporządzenia (UE) 2024/1689 (rozporządzenie w sprawie swobodnego przepływu danych), rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) i dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych) do rozporządzenia (UE) 2023/2854 (akt w sprawie danych), tworząc jeden skonsolidowany instrument dla europejskiej gospodarki opartej na danych. Rozporządzenie (UE) 2024/1689 (rozporządzenie w sprawie swobodnego przepływu danych), dyrektywa (UE) 2019/1024 (dyrektywa w sprawie otwartych danych) i rozporządzenie (UE) 2022/868 (akt w sprawie zarządzania danymi) zostają uchylone. Przepisy w ramach wszystkich czterech instrumentów są lepiej dostosowane i usprawnione, aby zwiększyć jasność i spójność, wzmacniając tym samym ich skuteczność i wspierając przedsiębiorstwa w stymulowaniu innowacji. Niniejsza inicjatywa jest zgodna ze strategią na rzecz europejskiej unii danych, której zasadniczym celem jest uproszczenie ram prawnych.

Ponadto, aby dalej wspierać mniejsze przedsiębiorstwa, przepisy ułatwiające małym i średnim przedsiębiorstwom (MŚP) przestrzeganie unijnego prawodawstwa w dziedzinie danych rozszerzono na małe spółki o średniej kapitalizacji. Rozporządzenie (UE) 2023/2854 (akt w sprawie danych), które weszło w życie 12 września 2025 r., stanowi istotny krok w kierunku sprawiedliwej i konkurencyjnej gospodarki opartej na danych w UE. Zamierzeniem zmian przedstawionych w niniejszym wniosku nie jest wprowadzenie zmian w osiągnięciach rozporządzenia (UE) 2023/2854 (akt w sprawie danych).

Aby jednak w pełni osiągnąć cel polegający na zrównoważeniu innowacji i dostępności danych z ochroną praw i interesów posiadaczy danych, należy skalibrować cztery kluczowe elementy. W szczególności należy zapewnić, aby rozporządzenie (UE) 2023/2854 (akt w sprawie danych) nie tylko zmniejszało obciążenia, ale również zwiększało jasność prawa i stymulowało konkurencyjność. Po pierwsze, istnieje pilna potrzeba wzmocnienia zabezpieczeń przed ryzykiem wycieku tajemnic przedsiębiorstwa do państw trzecich w kontekście przepisów dotyczących obowiązkowego dzielenia się danymi w ramach internetu rzeczy. Po drugie, szeroki zakres ram współpracy między przedsiębiorstwami a administracją publiczną może potencjalnie prowadzić do niejasności prawnych. Po trzecie, brak pewności prawa może wynikać z przepisów dotyczących zasadniczych wymogów w odniesieniu do inteligentnych umów realizujących umowy w sprawie dzielenia się danymi. Wreszcie przepisy rozporządzenia (UE) 2023/2854 (akt w sprawie danych) dotyczące zmiany dostawcy usług przetwarzania danych zachowują swoje znaczenie, zapewniając główny wkład w bardziej otwarty i konkurencyjny rynek usług w chmurze. Przepisy te nie uwzględniały jednak w wystarczającym stopniu szczególnej sytuacji usług, które są w znacznym stopniu dostosowane do potrzeb klienta w celu zapewnienia ich użyteczności lub świadczone przez MŚP i małe spółki o średniej kapitalizacji. Zmiany zawarte w niniejszym wniosku utrzymają ambitny cel, jakim jest zniesienie uzależnienia od jednego dostawcy, w szczególności w odniesieniu do zmiany dostawcy i opłat z tytułu wychodzącego ruchu danych, przy jednoczesnym zmniejszeniu obciążeń administracyjnych dla dostawców wyżej wymienionych usług. We wniosku przedstawiono zatem zmiany, które zwiększają jasność prawa i są silnie dostosowane do ogólnych celów rozporządzenia (UE) 2023/2854 (akt w sprawie danych).

Ponadto, aby dalej wspierać mniejsze przedsiębiorstwa, przepisy ułatwiające małym i średnim przedsiębiorstwom (MŚP) przestrzeganie dorobku prawnego UE w zakresie danych rozszerzono na małe spółki o średniej kapitalizacji.

Jeżeli chodzi o dane osobowe, rozporządzenie (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych, RODO) zaczęło

obowiązywać 25 maja 2018 r., ustanawiając ogólnounijne normy, przepisy i zabezpieczenia dotyczące przetwarzania danych osobowych osób fizycznych, prawa osób, których dane dotyczą, a także ogólne ramy prawne dla podmiotów przetwarzających dane osobowe. Chociaż zainteresowane strony zasadniczo uznały rozporządzenie (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) za wyważone i solidne oraz nadal adekwatne do zakładanych celów, niektóre podmioty, zwłaszcza mniejsze przedsiębiorstwa i stowarzyszenia charakteryzujące się niewielką liczbą nieintensywnych operacji przetwarzania danych, często o niskim ryzyku, wyraziły obawy dotyczące stosowania niektórych obowiązków wynikających z ogólnego rozporządzenia o ochronie danych. Niektóre z tych obaw można rozwiać dzięki spójniejszej i bardziej zharmonizowanej interpretacji i egzekwowaniu przepisów we wszystkich państwach członkowskich, podczas gdy inne wymagają ukierunkowanych zmian w przepisach. W tym kontekście zmiany zawarte w niniejszym wniosku mają na celu uwzględnienie tych obaw, w szczególności przez wyjaśnienie niektórych kluczowych definicji, na przykład pojęć związanych z danymi osobowymi; przez ułatwienie przestrzegania przepisów, na przykład w drodze wspierania administratorów pod względem kryteriów i środków służących ustaleniu, czy dane wynikające z pseudonimizacji nie stanowią danych osobowych, w odniesieniu do wymogów informacyjnych i powiadamiania organów nadzorczych o naruszeniu ochrony danych; a także przez wyjaśnienie niektórych aspektów przetwarzania danych na potrzeby trenowania i rozwoju AI. Proponowane zmiany uwzględniają również brak jasności co do warunków dla badań naukowych, ponieważ zawierają definicję badań naukowych, doprecyzowując, że dalsze przetwarzanie do celów naukowych jest zgodne z pierwotnym celem przetwarzania, oraz wyjaśniając, że badania naukowe stanowią uzasadniony interes. Proponuje się również rozszerzenie zakresu wyjątków od obowiązku informowania w odniesieniu do przetwarzania. W stosownych przypadkach niniejszy wniosek odzwierciedla zmiany w ogólnym rozporządzeniu o ochronie danych wprowadzone rozporządzeniem (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii.

Ponadto już od dawna potrzebne jest rozwiązanie regulacyjne dotyczące zmęczenia wyrażaniem zgody i zbyt dużej liczby banerów informujących o plikach cookie. Dyrektywa (UE) 2002/58/WE o prywatności i łączności elektronicznej („dyrektywa o e-prywatności”), ostatnio zmieniona w 2009 r., zapewnia ramy ochrony poufności komunikacji i precyzuje rozporządzenie (UE) 2016/679 („ogólne rozporządzenie o ochronie danych”, „RODO”), w przypadku gdy przetwarzanie danych osobowych odbywa się w kontekście łączności elektronicznej. Chroni ona również końcowe urządzenia użytkowników, które można wykorzystywać do naruszania ich prywatności i gromadzenia informacji dotyczących tych użytkowników. Zasadniczym elementem użytkowania końcowych urządzeń – takich jak telefony i komputery osobiste – jest korzystanie z treści i usług online. Wiele z tych usług online opiera się na dochodach z reklam, w tym z reklam spersonalizowanych. Dotyczy to również usług medialnych. Dostawcy usług online polegają na tzw. plikach cookie lub podobnych technologiach, które wykorzystują możliwości końcowego urządzenia w zakresie przetwarzania i przechowywania, wskutek czego uzyskują dostęp na przykład do informacji przechowywanych w końcowym urządzeniu lub z niego przesyłanych. Wykorzystuje się to do różnych celów, takich jak optymalizacja świadczenia usługi dla danego końcowego urządzenia, zapewnienie bezpieczeństwa końcowego urządzenia i całej usługi, a także śledzenie zachowania danej osoby i interakcji z różnymi usługami online w celu dostarczania spersonalizowanych reklam.

Gdy wykorzystywanie takich technologii nie jest konieczne do technicznego przechowywania danych lub dostępu do danych jedynie w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to szczególnie

niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika, dyrektywa 2002/58/WE („dyrektywa o e-prywatności”) wymaga udzielenia zgody. Zgody takiej zazwyczaj żąda się za pośrednictwem wyskakujących banerów wyświetlanych na stronie internetowej lub w aplikacji mobilnej. Takie banery zawierają informacje na temat celów przetwarzania, często powiązane z rodzajami plików cookie i odbiorcami danych, oraz nie zawsze są łatwe do zrozumienia dla osób fizycznych. Z tych powodów mogą one nie osiągać swojego celu, jakim jest poinformowanie osoby fizycznej i zapewnienie jej kontroli nad ochroną własnej prywatności i przetwarzaniem jej danych osobowych, natomiast są postrzegane jako uciążliwość dla użytkowników internetu. Jednocześnie dostawcy usług online ponoszą znaczne koszty związane z projektowaniem banerów spełniających wymogi.

Złożoność jest jeszcze większa, gdyż art. 5 ust. 3 dyrektywy 2002/58/WE (dyrektywa o e-prywatności) ma zastosowanie do umieszczania plików cookie lub podobnych technologii w celu uzyskania informacji z końcowego urządzenia użytkownika, natomiast dalsze przetwarzanie danych osobowych podlega rozporządzeniu (UE) 2016/679 (ogólne rozporządzenie o ochronie danych). Chociaż w celu zapewnienia kontroli osobom, których dane dotyczą, wymagana jest zgoda, nie zawsze jest ona najwłaściwszą podstawą prawną dalszego przetwarzania, na przykład gdy przetwarzanie jest niezbędne do świadczenia usługi innej niż usługa społeczeństwa informacyjnego. Doprowadziło to do braku pewności prawa i wyższych kosztów przestrzegania przepisów dla administratorów, którzy przetwarzają dane osobowe uzyskane z końcowych urządzeń. Ponadto podwójny system dyrektywy o e-prywatności i ogólnego rozporządzenia o ochronie danych doprowadził do sytuacji, w której różne organy krajowe są właściwe do nadzorowania przepisów tych dwóch ram prawnych.

Z tych powodów proponuje się natychmiastowe uproszczenie wzajemnych powiązań między obowiązującymi przepisami. Przetwarzanie danych osobowych na końcowym urządzeniu i z tego urządzenia powinno być regulowane wyłącznie rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych), z uwzględnieniem również wyraźnego wymogu uzyskania zgody na dostęp do końcowego urządzenia osoby fizycznej w przypadku gromadzenia danych osobowych. Proponowane zmiany przewidują również pewne cele, w przypadku których uzyskanie zgody nie powinno być konieczne i w przypadku których dalsze przetwarzanie należy uznać za zgodne z prawem, w szczególności gdy stwarzają niewielkie ryzyko naruszenia praw i wolności osób, których dane dotyczą, lub gdy umieszczenie takich technologii jest niezbędne do świadczenia usługi żądanej przez osobę, której dane dotyczą.

Ponadto wniosek toruje drogę do zautomatyzowanych i nadających się do odczytu maszynowego wskazań indywidualnych wyborów i stosowania się do tych wskazań przez dostawców stron internetowych i aplikacji mobilnych oraz dostawców aplikacji na telefony komórkowe po udostępnieniu norm. Cel ten opiera się na zmianie dyrektywy (UE) 2002/58/WE (dyrektywa o e-prywatności) z 2009 r. (por. motyw 66 dyrektywy 2009/136/WE), w której zachęcano już do umożliwienia wyrażenia zgody przez użytkownika poprzez zastosowanie odpowiednich ustawień w przeglądarce lub innej aplikacji, jeżeli jest to technicznie możliwe i skuteczne, oraz na art. 21 ust. 5 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych), a także na wniosku Komisji z 2017 r. dotyczącym rozporządzenia w sprawie prywatności i łączności elektronicznej (COM(2017) 10), w którym zaproponowano zarządzanie wyborem użytkownika za pomocą ustawień przeglądarki internetowej. Upoważnia to Komisję do zwrócenia się do jednostek normalizacyjnych o opracowanie zestawu norm na potrzeby kodowania zautomatyzowanego i nadającego się do odczytu maszynowego wskazania wyborów osób, których dane dotyczą, oraz przekazywania informacji o tych wyborach z przeglądarek do stron internetowych i z aplikacji na telefony

komórkowe do usług sieciowych. Po ich udostępnieniu i po upływie sześciomiesięcznego dodatkowego okresu administratorzy korzystający ze stron internetowych i aplikacji mobilnych w celu świadczenia usług są zobowiązani do przestrzegania tych zakodowanych zautomatyzowanych i nadających się do odczytu maszynowego wskazań. W przypadku gdy administratorzy zapewniają zgodność swoich stron internetowych lub aplikacji na telefony komórkowe z takimi normami, powinni korzystać z domniemania zgodności. Na tej podstawie oczekuje się, że opracowane zostaną również odpowiednie ustawienia w przeglądarkach. Przepisy sformułowano w sposób neutralny pod względem technologicznym, tak aby również inne narzędzia, np. agentowa AI, mogły wspierać użytkowników w dokonywaniu wyborów dotyczących zgody, jeżeli będą one w stanie zapewnić zgodność z wymogami RODO. Biorąc pod uwagę znaczenie źródeł dochodów online dla niezależnego dziennikarstwa jako niezbędnego filaru społeczeństwa demokratycznego, dostawcy usług medialnych zdefiniowani w rozporządzeniu (UE) 2024/1083 (europejski akt o wolności mediów) nie powinni być zobowiązani do poszanowania takich sygnałów i powinni mieć możliwość bezpośredniej interakcji z użytkownikami, aby przekazywać im informacje i umożliwiać im dokonywanie wyborów dotyczących zgody.

Zmiany przedstawione w niniejszym rozporządzeniu wprowadzą **pojedynczy punkt kontaktowy, za pośrednictwem którego podmioty będą mogły jednocześnie wypełniać swoje obowiązki w zakresie zgłaszania incydentów wynikające z wielu aktów prawnych**. Dzięki propagowaniu zasady „zgłoś raz, udostępnij wielu” pojedynczy punkt kontaktowy zmniejszy obciążenie administracyjne podmiotów, a jednocześnie zapewni skuteczny i bezpieczny przepływ informacji na temat incydentów bezpieczeństwa do odbiorców określonych w odpowiednich przepisach.

We wniosku nałożono na ENISA obowiązek opracowania pojedynczego punktu kontaktowego, z uwzględnieniem pojedynczej platformy sprawozdawczej do powiadamiania o aktywnie wykorzystywanych podatnościach i poważnych incydentach na podstawie rozporządzenia (UE) 2024/2847 (akt dotyczący cyberodporności). Określono w nim szczegółowe wymogi dotyczące tego narzędzia jako bezpiecznego kanału przekazywania informacji zgłaszanych przez podmioty i wysyłanych właściwym organom. Nie zmienia to podstawowych wymogów prawnych dotyczących zgłaszania incydentów, ale znacznie optymalizuje przepływ pracy i zasoby wymagane od podmiotów.

We wniosku przewidziano również obowiązek korzystania z pojedynczego punktu kontaktowego w odniesieniu do szeregu ściśle powiązanych ze sobą obowiązków w zakresie zgłaszania incydentów określonych w dyrektywie (UE) 2022/2555 (dyrektywa NIS 2), rozporządzeniu (UE) 2016/679 (RODO), rozporządzeniu (UE) 2022/2554 (DORA), rozporządzeniu (UE) nr 910/2014 (rozporządzenie eIDAS) i dyrektywie (UE) 2022/2557 (dyrektywa CER). Inne sektorowe obowiązki sprawozdawcze, takie jak obowiązki określone w ramach kodeksu sieci dotyczącego aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (NCCS) oraz odpowiednich instrumentów dla sektora lotnictwa, zostaną również objęte pojedynczym punktem kontaktowym dzięki zmianom odpowiednich aktów delegowanych i wykonawczych ustanawiających obowiązki sprawozdawcze na podstawie tych ram.

Wniosek ma również na celu usprawnienie treści zgłaszanych informacji przez wprowadzenie uprawnień w odniesieniu do kilku aktów prawnych, w przypadku gdy takie uprawnienia nie istnieją. We wniosku wyjaśniono, że przy opracowywaniu wspólnych wzorów sprawozdawczych na potrzeby dyrektywy (UE) 2022/2555, dyrektywy (UE) 2022/2557 lub rozporządzenia (UE) 2016/679, aby zapewnić spójność, promować synergie i zmniejszyć obciążenie administracyjne podmiotów dzięki ograniczeniu do minimum liczby pól danych,

które podmioty są zobowiązane wypełnić, Komisja powinna należycie uwzględnić zdobyte doświadczenia i wspólne wzory opracowane na podstawie rozporządzenia (UE) 2022/2554 (DORA).

Oprócz tych podstawowych zmian wniosek uchyla rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (rozporządzenie w sprawie stosunków między platformami a przedsiębiorcami lub „rozporządzenie P2B"). Rozporządzenie jest stosowane od 12 lipca 2020 r. i stanowiło pierwszy krok w kierunku zapewnienia kompleksowych ram prawnych dla gospodarki platform. Od czasu rozpoczęcia jego stosowania wprowadzono inne akty prawa Unii regulujące usługi pośrednictwa internetowego i platformy internetowe. Obejmują one rozporządzenie (UE) 2022/1925 (akt o rynkach cyfrowych, DMA) i rozporządzenie (UE) 2022/2065 (akt o usługach cyfrowych, DSA), które w dużej mierze uchylają przepisy rozporządzenia P2B. Wybrane przepisy rozporządzenia P2B pozostaną w mocy w celu zapewnienia pewności prawa w odniesieniu do aktów zawierających odesłania do tych przepisów, na przykład dyrektywy (UE) 2023/2831 w sprawie poprawy warunków pracy za pośrednictwem platform. Ogólnie rzecz biorąc, uproszczenie ram regulacyjnych dla platform internetowych zmniejszy koszty przestrzegania przepisów wynikające z wielowarstwowych i nakładających się na siebie przepisów, o co apelowały zainteresowane strony. Dostawcy usług pośrednictwa internetowego odniosą korzyści z większej jasności przepisów prawnych. Egzekwowanie przepisów będzie bardziej ukierunkowane.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Wnioskowi towarzyszy drugi wniosek zmieniający rozporządzenie (UE) 2024/1689 (akt w sprawie AI), tworzą one wspólnie „pakiet aktów zbiorczych prawa cyfrowego" i stanowią pierwszy, bezpośredni krok w kierunku uproszczenia zbioru prawa cyfrowego. Oprócz aktu zbiorczego prawa cyfrowego wniosek dotyczący zmiany rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie) będzie obejmował m.in. zaktualizowany mandat Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), a także środki mające na celu uproszczenie przestrzegania wymogów cyberbezpieczeństwa.

Akt zbiorczy prawa cyfrowego jest częścią szerszej strategii uproszczenia przepisów zapowiedzianej w pakiecie cyfrowym, przedstawionej bardziej szczegółowo w części wprowadzającej niniejszego uzasadnienia.

- **Spójność z innymi politykami Unii**

Wniosek jest częścią programu Komisji na rzecz uproszczenia ram regulacyjnych UE. Szeroki zakres zmienianych aktów wskazuje na wyraźny potencjał uproszczenia dzięki uwzględnieniu wzajemnych zależności między różnymi przepisami, w tym w przypadku gdy odnoszą się one do różnych obszarów polityki. Dotyczy to na przykład rozwiązania w zakresie uproszczenia cyfrowego opracowanego w ramach pojedynczego punktu kontaktowego do celów zgłaszania incydentów, które nie narusza podstawowych obowiązków regulacyjnych, ale łączy w tym samym interfejsie przepisy dotyczące cyberbezpieczeństwa mające zastosowanie do podmiotów kluczowych, przepisy mające zastosowanie do sektora finansowego, przepisy o ochronie danych itp.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawą wniosku są art. 114 i 16 Traktatu o funkcjonowaniu Unii Europejskiej, odzwierciedlające podstawę prawną zmienianych aktów. Właściwą podstawą prawną przepisów zmieniających rozporządzenie (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) i rozporządzenie (UE) 2018/1725 jest art. 16 Traktatu. Ponieważ wszystkie pozostałe zmieniane akty opierają się na art. 114 Traktatu, ta sama podstawa prawna jest również właściwa dla odpowiednich przepisów zmieniających niniejszego rozporządzenia.

• Pomocniczość (w przypadku kompetencji niewyłącznych)

Biorąc pod uwagę, że zmieniane przepisy są przepisami unijnymi, można je zmienić wyłącznie na poziomie Unii. Dostosowania techniczne przedstawione w niniejszym rozporządzeniu zachowują logikę pomocniczości, która leży u podstaw zmienianych aktów.

Jeżeli chodzi o rozporządzenie (UE) 2023/2854 (akt w sprawie danych), zmiany wzmacniają cel rozporządzenia, jakim jest usunięcie barier na jednolitym rynku dla gospodarki opartej na danych. Cel ten jest realizowany przez dołączenie do rozporządzenia obowiązujących przepisów. Ukierunkowane zmiany wprowadzone do tych przepisów mają na celu uproszczenie, zapewnienie jasności i zmniejszenie obciążeń administracyjnych zarówno dla sektora prywatnego, jak i dla organów krajowych. Nie ingerują one w kompetencje państw członkowskich ani instytucji Unii.

Dotyczy to również uchylenia dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych), mając na uwadze, że zawarte w niej przepisy prawa materialnego są włączane do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) bez istotnej zmiany kompetencji przyznanych państwom członkowskim. Znaczna część danych sektora publicznego podlega już obecnie bezpośrednio stosowanemu rozporządzeniu wykonawczemu (UE) 2023/138 w sprawie zbiorów danych o wysokiej wartości[12]. Przekształcenie do postaci rozporządzenia ułatwi jednolite stosowanie proponowanych zmian we wszystkich państwach członkowskich. Będzie to w szczególności wspierać administracje publiczne posiadające dane sektora publicznego, ale także ponownych użytkowników takich danych, przez usprawnienie procesów i zmniejszenie obciążeń administracyjnych związanych z interpretacją i wdrażaniem różnych przepisów krajowych. Egzekwowanie bezpośrednio stosowanych przepisów prawdopodobnie stanie się bardziej spójne. Wniosek nie zmienia krajowych systemów dostępu i ma na celu zapewnienie wystarczającej elastyczności rozwiązań krajowych – którą to prerogatywę podkreśliły państwa członkowskie.

W odniesieniu do rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) i rozporządzenia (UE) 2018/1725 proponowane zmiany mają na celu zapewnienie jasności i przewidywalności w stosowaniu obowiązujących przepisów oraz zmniejszenie obciążeń administracyjnych, w miarę możliwości, bez podważania wysokiego poziomu ochrony danych na podstawie rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie

[12] Rozporządzenie wykonawcze Komisji (UE) 2013/138.

danych) i rozporządzenia (UE) 2018/1725. Podobnie nie zmieniają one kompetencji państw członkowskich ani organów i instytucji UE.

Wraz z wprowadzeniem pojedynczego punktu kontaktowego do zgłaszania incydentów proponuje się rozwiązanie ogólnoeuropejskie, aby zapewnić jeden kanał dla wielu obowiązków prawnych, jakim podlegają przedsiębiorstwa w związku ze zgłaszaniem zasadniczo tego samego incydentu. Rozwiązanie to nie zmienia w żaden sposób praw i kompetencji organów krajowych do przyjmowania takich zgłoszeń. Zamiast tego zachęca do zgłaszania, zapewniając pojedynczy punkt kontaktowy z łatwym w użyciu interfejsem, w którym składa się na pozór jedno sprawozdanie, aby wywiązać się jednocześnie z licznych obowiązków prawnych. Biorąc pod uwagę, że świadczenie wielu z tych usług odbywa się transgranicznie, a usługodawcy są obecni w wielu państwach członkowskich, wymagane jest rozwiązanie na szczeblu europejskim.

- **Proporcjonalność**

Wniosek obejmuje zmiany techniczne, które są niezbędne do osiągnięcia celów polegających na zmniejszeniu obciążeń administracyjnych i zapewnieniu jasności przepisów, przy jednoczesnym zachowaniu i optymalizacji podstawowych celów zmienionych przepisów. Są one proporcjonalne, ponieważ nakładają na przedsiębiorstwa i organy znikome, o ile jakiekolwiek, koszty związane z okresem przejściowym i koszty dostosowania, ale ułatwiają uzyskanie wysokich oszczędności kosztów w nadchodzących latach.

Celem szeregu zmian przedstawionych w niniejszym rozporządzeniu jest uproszczenie, przede wszystkim dzięki zapewnieniu pewności prawa i wyjaśnieniu stosowania przepisów – na przykład w odniesieniu do wyjaśnień dla posiadaczy danych dotyczących ochrony tajemnic przedsiębiorstwa w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) lub wyjaśnień dotyczących trenowania modeli i systemów AI, które obejmują dane osobowe regulowane rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych), lub pojęcia danych osobowych w rozporządzeniu (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) i rozporządzeniu (UE) 2018/1725. Niektóre przepisy mają na celu skodyfikowanie wykładni Trybunału Sprawiedliwości Unii Europejskiej, np. w odniesieniu do pseudonimizacji danych osobowych doprecyzowanej w rozporządzeniu (UE) 2016/679 (ogólne rozporządzenie o ochronie danych). W związku z tym obejmują one bardzo ukierunkowane zmiany przepisów, które zgodnie z oczekiwaniami będą miały duży wpływ na gwarantowanie pewności prawa przedsiębiorstwom i inwestorom.

Zmiany proponowane w niniejszym rozporządzeniu mają również na celu zmniejszenie kosztów bezpośrednich ponoszonych przez przedsiębiorstwa i organy, przy uwzględnieniu, że te same cele regulacyjne można osiągnąć przy mniejszych obciążeniach i z zapewnieniem proporcjonalności przepisów. Na przykład obowiązkowy system usług pośrednictwa danych przewidziany w rozporządzeniu (UE) 2022/868 (akt w sprawie zarządzania danymi) przekształcono w dobrowolny system zwiększający zaufanie w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych).

Dzięki rozszerzeniu na małe spółki o średniej kapitalizacji niektórych przepisów mających zastosowanie do małych i średnich przedsiębiorstw środki upraszczające mają ukierunkowany charakter i wprowadzają minimalne zmiany w zakresie tych obowiązków, zapewniając jednocześnie pewność prawa szerszemu gronu przedsiębiorstw o wysokim potencjale wspierania konkurencyjności UE. Wnioski ograniczają się do tych zmian, które są niezbędne do zapewnienia, aby małe spółki o średniej kapitalizacji korzystały z tych samych ram prawnych co MŚP.

Pojedynczy punkt kontaktowy do zgłaszania incydentów i powiadamiania o naruszeniach ochrony danych przynosi przedsiębiorstwom wysokie oszczędności kosztów, a jednocześnie rozwiązuje ogólny problem niskiego poziomu zgłaszania. Jest to nie tylko rozwiązanie proporcjonalne, ale także kluczowe rozwiązanie upraszczające za pomocą narzędzia cyfrowego i wspierające skuteczność obowiązków sprawozdawczych objętych punktem kontaktowym.

Uchylenie rozporządzenia (UE) 2019/1150 (rozporządzenie P2B) jest konieczne, aby wyeliminować powielanie przepisów; rozporządzenie ma jedynie wartość rezydualną, a w świetle proporcjonalnego podejścia regulacyjnego do przepisów w sprawie platform internetowych konieczne jest wyeliminowanie podwójnych obowiązków.

- **Wybór instrumentu**

Zmiany proponuje się w formie rozporządzenia, biorąc pod uwagę charakter zmienianych przepisów. W przypadku zmiany dyrektyw przepisy są skierowane do organów europejskich lub wprowadzają ukierunkowane zmiany w szczególności w celu wyodrębnienia przepisów dopracowanych w rozporządzeniach.

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

- **Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa**

Większość przepisów rozważanych w niniejszym wniosku jest stosunkowo nowa i podlega trwającej ocenie wyników. Najważniejsze uwagi podsumowano w towarzyszącym dokumencie roboczym służb Komisji.

Wyjątek stanowi tu wstępny przegląd rozporządzenia (UE) 2019/1150 (rozporządzenie w sprawie stosunków między platformami a przedsiębiorcami (P2B)) z 2023 r.[13)] W sprawozdaniu odnotowano początkowe pozytywne skutki pod względem na przykład przejrzystości umów dla użytkowników biznesowych i sprawiedliwości proceduralnej w rozpatrywaniu skarg. W sprawozdaniu wykazano jednak również, że użytkownicy biznesowi oraz dostawcy usług pośrednictwa internetowego i wyszukiwarek internetowych nie są świadomi swoich praw i obowiązków wynikających z rozporządzenia (UE) 2019/1150 (rozporządzenie P2B). Wiązało się to także z niewystarczającą zgodnością z rozporządzeniem (UE) 2019/1150 (rozporządzenie P2B) i doprowadziło do braku wdrożenia. Do 2023 r. otrzymano bardzo niewiele skarg na mocy rozporządzenia (UE) 2019/1150 (rozporządzenie P2B). W sprawozdaniu stwierdzono, że „obecnie nie urzeczywistniono pełnego potencjału rozporządzenia (UE) 2019/1150 (rozporządzenie P2B)”. Tymczasem rozporządzenie (UE) 2022/2065 (akt o usługach cyfrowych) i rozporządzenie (UE) 2022/1925 (akt o rynkach

[13] Dokument roboczy służb Komisji, Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów dotyczące pierwszego wstępnego przeglądu wdrażania rozporządzenia (UE) 2019/1150 w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego {SWD(2023) 300 final}.

cyfrowych) zaczęły w pełni obowiązywać i w dużej mierze zastąpiły przepisy rozporządzenia (UE) 2019/1150 (rozporządzenie P2B).

- **Konsultacje z zainteresowanymi stronami**

Podczas przygotowywania wniosku przeprowadzono szereg konsultacji. Każde z nich miały się wzajemnie uzupełniać, obejmując różne aspekty tematyczne albo różne grupy zainteresowanych stron.

Wiosną 2025 r. opublikowano trzy konsultacje publiczne i zaproszenia do zgłaszania uwag na temat kluczowych filarów wniosku. W dniach od 9 kwietnia do 4 czerwca przeprowadzono konsultacje dotyczące strategii w sprawie zastosowania AI[14], w dniach od 11 kwietnia do 20 czerwca konsultacje w sprawie zmiany rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie)[15], a w dniach od 23 maja do 20 lipca konsultacje w sprawie strategii na rzecz europejskiej unii danych[16]. Każdy kwestionariusz zawierał specjalną sekcję (lub niekiedy wiele sekcji) poświęconą obawom dotyczącym wdrażania i uproszczenia, bezpośrednio związanym z refleksjami na temat aktu zbiorczego prawa cyfrowego. Łącznie w ramach pierwszej ścieżki konsultacji otrzymano 718 odrębnych odpowiedzi.

Ponadto w okresie od 16 września do 14 października 2025 r. opublikowano zaproszenie do zgłaszania uwag na temat aktu zbiorczego prawa cyfrowego[17]. Jego celem było umożliwienie zainteresowanym stronom przedstawienia uwag na temat skonsolidowanego wniosku dotyczącego zakresu aktu zbiorczego prawa cyfrowego. Otrzymano 513 odpowiedzi od różnych grup zainteresowanych stron, w tym przedsiębiorstw i stowarzyszeń przedsiębiorców, społeczeństwa obywatelskiego, środowisk akademickich i organów, a także indywidualne uwagi od obywateli.

Wiceprzewodnicząca wykonawcza Henna Virkkunen prowadziła dwa dialogi na temat wdrażania dotyczące kluczowych tematów poruszonych w akcie zbiorczym prawa cyfrowego: pierwszy dotyczył polityki w zakresie danych[18] (1 lipca 2025 r.), a drugi polityki w zakresie cyberbezpieczeństwa[19] (15 września).

Komisarz McGrath prowadził dialog na temat wdrażania dotyczący stosowania RODO (16 lipca 2025 r.).

---

[14] Komisja Europejska (2025), *Zaproszenie do zgłaszania uwag dotyczących strategii w sprawie zastosowania AI*. Dokument dostępny na stronie: Strategia w sprawie zastosowania AI – wzmocnienie kontynentu sztucznej inteligencji

[15] Komisja Europejska (2025), *Zaproszenie do zgłaszania uwag dotyczących zmiany aktu o cyberbezpieczeństwie*. Dokument dostępny na stronie: Unijny akt o cyberbezpieczeństwie

[16] Komisja Europejska (2025), *Zaproszenie do zgłaszania uwag na temat strategii na rzecz europejskiej unii danych*. Dokument dostępny na stronie: Strategia na rzecz europejskiej unii danych

[17] Komisja Europejska (2025), *Zaproszenie do zgłaszania uwag na temat pakietu cyfrowego i zbiorczego*. Dokument dostępny na stronie: Uproszczenie – pakiet cyfrowy i zbiorczy.

[18] Komisja Europejska (2025), *Dialog na temat wdrażania – polityka w zakresie danych*. Dokument dostępny pod adresem: Dialog na temat wdrażania – polityka w zakresie danych – Komisja Europejska.

[19] Komisja Europejska (2025), *Dialog na temat wdrażania polityki cyberbezpieczeństwa z wiceprzewodniczącą wykonawczą Henną Virkkunen*. Dokument dostępny na stronie: Dialog na temat wdrażania polityki cyberbezpieczeństwa z wiceprzewodniczącą wykonawczą Henną Virkkunen – Komisja Europejska.

Służby Komisji przeprowadziły również szereg „konsultacji na temat stosowania przepisów w praktyce” w ramach pogłębionych grup dyskusyjnych z udziałem przedsiębiorstw i przedstawicieli społeczeństwa obywatelskiego, zorganizowanych w okresie od 15 września do 6 października 2025 r. w celu omówienia praktycznych wyzwań związanych z wdrażaniem obserwowanych na co dzień oraz oszacowania kosztów przestrzegania przepisów.

W okresie od 4 września do 16 października 2025 r. za pośrednictwem Europejskiej Sieci Przedsiębiorczości (EEN)[20] zorganizowano specjalne badanie panelowe z udziałem MŚP w celu skonsultowania się w szczególności z małymi i średnimi przedsiębiorstwami (MŚP) oraz zebrania od nich informacji zwrotnych.

Ponadto służby Komisji otrzymały liczne stanowiska i zorganizowały dwustronne posiedzenia z różnymi zainteresowanymi stronami. Służby Komisji współpracowały również z państwami członkowskimi przy okrągłym stole lub w ramach różnych grup roboczych Rady.

Ogólnie rzecz biorąc, informacje zwrotne od zainteresowanych stron były zbieżne co do potrzeby uproszczonego stosowania niektórych przepisów cyfrowych. Zainteresowane strony z zadowoleniem przyjęły skupienie się na spójności i konsolidacji przepisów oraz na optymalizacji kosztów przestrzegania przepisów.

Wyraźnie zaapelowano o usprawnienie dorobku prawnego UE w zakresie danych i konsolidację przepisów. Kwestię tę uwzględniono we wniosku wraz z ukierunkowanymi zmianami, które uzyskały poparcie zainteresowanych stron, w tym w odniesieniu do ogólnego rozporządzenia o ochronie danych i zmęczenia spowodowanego banerami informującymi o plikach cookie. Ponadto przedsiębiorstwa wskazały na dalsze oceny wzajemnych zależności między przepisami dotyczącymi danych, które wymagają głębszej analizy z wykorzystaniem narzędzi lepszego stanowienia prawa, w szczególności zbliżającą się ocenę adekwatności przepisów cyfrowych.

Przedsiębiorstwa z różnych sektorów wskazały również na nieuzasadnione obciążenia wynikające z podwójnego zgłaszania incydentów w wielu ramach prawnych. To wezwanie do działania realizuje się za pomocą wniosku dotyczącego pojedynczego punktu kontaktowego do zgłaszania incydentów.

Jeżeli chodzi o akt w sprawie sztucznej inteligencji, zainteresowane strony wskazały na potrzebę zagwarantowania pewności prawa w zakresie stosowania przepisów, a w szczególności podkreśliły potrzebę dostępności norm i wytycznych przed rozpoczęciem stosowania przepisów. Odpowiedź na ich obawy stanowi odrębny wniosek regulacyjny w ramach pakietu aktów zbiorczych prawa cyfrowego.

Wreszcie zainteresowane strony nie wypowiedziały się na temat wpływu rozporządzenia w sprawie stosunków między platformami a przedsiębiorcami, co potwierdza wyniki sprawozdania z oceny śródokresowej, zgodnie z którymi przepisy te nie są ani dobrze znane, ani skuteczne w osiąganiu swojego celu. W niniejszym rozporządzeniu proponuje się uchylenie przepisów w sprawie stosunków między platformami a przedsiębiorcami, w szczególności w świetle ich pokrywania się z nowszymi przepisami.

---

[20] EEN jest największą na świecie siecią wsparcia dla małych i średnich przedsiębiorstw i jest wdrażana przez Agencję Wykonawczą Europejskiej Rady ds. Innowacji i ds. MŚP (EISMEA) Komisji Europejskiej.

Szczegółowy przegląd tych konsultacji z zainteresowanymi stronami oraz informacje na temat sposobu, w jaki uwzględniono je we wniosku, można znaleźć w dokumencie roboczym służb Komisji uzupełniającym akt zbiorczy prawa cyfrowego.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Poza opisanymi powyżej ścieżkami konsultacji do celów niniejszego wniosku Komisja opierała się głównie na analizie wewnętrznej. Zlecono również dwa badania na poparcie analizy rozdziałów wniosku dotyczących danych. Pierwsze z nich dotyczyło wdrożenia rozporządzenia (UE) 2018/1807 (rozporządzenie w sprawie swobodnego przepływu danych nieosobowych), dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych) i rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi). W drugim badaniu, ściślej powiązanym z komunikatem w sprawie strategii na rzecz europejskiej unii danych (przyjętym jako część tego samego pakietu w sprawie uproszczenia wraz z pakietem aktów zbiorczych prawa cyfrowego), skoncentrowano się na zmianach polityki w zakresie danych związanych z generatywną AI, zgodnością regulacyjną i wymiarem międzynarodowym. Oba badania są obecnie finalizowane i zostaną opublikowane na późniejszym etapie.

Służby Komisji przeprowadziły również badanie dotyczące wzajemnych zależności między rozporządzeniem (UE) 2022/2065 (akt o usługach cyfrowych) a innymi aktami ustawodawczymi, w tym rozporządzeniem (UE) 2019/1150 (rozporządzenie P2B). W ramach pakietu cyfrowego Komisja publikuje sprawozdanie opisujące wzajemne zależności między rozporządzeniem (UE) 2022/2065 (akt o usługach cyfrowych) a innymi powiązanymi przepisami, zgodnie z wymogiem określonym w art. 91 rozporządzenia (UE) 2022/2065 (akt o usługach cyfrowych).

- **Ocena skutków**

Zmiany zaproponowane w niniejszym rozporządzeniu są ukierunkowane i mają charakter techniczny. Mają one na celu zapewnienie skuteczniejszego wdrażania przepisów. Nie są one podatne na wiele wariantów strategicznych, które można by w znaczący sposób przetestować i porównać, oraz, zgodnie z wytycznymi dotyczącymi lepszego stanowienia prawa, nie są poparte pełnym sprawozdaniem z oceny skutków.

W załączonym dokumencie roboczym służb Komisji szczegółowo omówiono logikę interwencji w odniesieniu do zmian, zaprezentowano opinie zainteresowanych stron na temat poszczególnych środków oraz przedstawiono analizę kosztów i korzyści w odniesieniu do wniosków, w tym uzyskane oszczędności kosztów i inne rodzaje skutków. W wielu przypadkach dokument ten opiera się na odpowiednich ocenach skutków, które pierwotnie przeprowadzono w odniesieniu do poszczególnych aktów.

- **Sprawność regulacyjna i uproszczenie**

Proponowane rozporządzenie wiąże się z bardzo dużym zmniejszeniem obciążeń dla przedsiębiorstw, a także dla administracji publicznej i obywateli. Wstępne szacunki przewidują możliwe oszczędności w wysokości co najmniej 1 mld EUR rocznie, począwszy od momentu wejścia w życie, z dodatkowymi oszczędnościami w wysokości 1 mld EUR w kosztach jednorazowych, co daje łącznie co najmniej 5 mld EUR w ciągu 3 lat do 2029 r. W dużej mierze oczekuje się również niewymiernych korzyści, w szczególności dzięki usprawnionemu zestawowi przepisów, ułatwiającemu ich wykonywanie i przestrzeganie. W obliczeniach nie uwzględniono również możliwości rynkowych, jakie stwarza proponowane podejście regulacyjne.

Chociaż MŚP są już objęte zwolnieniem na mocy szeregu przepisów aktów prawnych, które zmienia pakiet aktów zbiorczych prawa cyfrowego, proponuje się dalsze środki wsparcia w obszarze zmiany dostawcy usług w chmurze. W rozdziale dotyczącym zharmonizowanych zasad dzielenia się danymi niektóre zwolnienia już przewidziane dla MŚP rozszerzono na małe spółki o średniej kapitalizacji.

Wniosek jest również w pełni zgodny z przeprowadzoną przez Komisję „kontrolą cyfrową", której celem jest zapewnienie odpowiedniego dostosowania wniosków dotyczących polityki do środowisk cyfrowych. Więcej szczegółowych informacji na ten temat można znaleźć w załączonym rozdziale 4 oceny skutków finansowych regulacji.

- **Prawa podstawowe**

Proponowane zmiany wspierają możliwości innowacyjne dla przedsiębiorstw na jednolitym rynku, a tym samym wspierają prawo do prowadzenia działalności gospodarczej w Unii.

Niektóre przepisy są również związane z ochroną i propagowaniem innych praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych, i zostały tak dostosowane, aby zachowywać najwyższy standard ochrony oraz wspierać osoby fizyczne w skutecznym korzystaniu z przysługujących im praw, przy jednoczesnej optymalizacji kosztów i tworzeniu dalszych możliwości innowacyjnych. W ten sposób wniosek w sposób ścisły przestrzega zasady proporcjonalności zapisanej w art. 52 Karty.

W szczególnym przypadku ukierunkowanych zmian w rozporządzeniu (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) i rozporządzeniu (UE) 2018/1725 proponowane zmiany uprościłyby wymogi dotyczące przetwarzania niskiego ryzyka, zharmonizowałyby niektóre normy i doprecyzowałyby niektóre kluczowe pojęcia rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) i rozporządzenia (UE) 2018/1725, umożliwiając administratorom wdrażanie skuteczniejszych polityk ochrony danych. Umożliwiłoby im to skoncentrowanie zasobów na działaniach wymagających większych ilości danych i obarczonych wyższym ryzykiem, w przypadku których środki ochrony danych osobowych mają największe znaczenie.

Jeżeli chodzi o prywatność komunikacji, we wniosku zachowano najwyższy standard ochrony, w tym dostęp do końcowych urządzeń oparty na zgodzie. Zmiana dyrektywy (UE) 2002/58/WE (dyrektywa o e-prywatności) nie modyfikuje ochrony materialnej. Dostosowuje przepisy dotyczące przetwarzania danych osobowych na końcowych urządzeniach i z takich urządzeń do przepisów rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych). Utrzymuje się przepisy dyrektywy dotyczące integralności końcowych urządzeń w przypadku przetwarzania danych nieosobowych.

4. WPŁYW NA BUDŻET

Wpływ na budżet utworzenia i utrzymania pojedynczego punktu kontaktowego do zgłaszania incydentów przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) szczegółowo opisano w przeglądzie rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie) w ramach zasobów dla ENISA.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Nie dotyczy.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Zmiany w rozporządzeniu (UE) 2023/2854 – akt w sprawie danych

Zmiany ram prawnych dotyczących danych konsolidują w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) w solidnie uproszczony sposób przepisy rozporządzenia (UE) 2018/1807 (rozporządzenie w sprawie swobodnego przepływu danych), rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) i dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych). Rozdział I zawiera również ukierunkowane zmiany mające na celu dostosowanie obecnych przepisów rozporządzenia (UE) 2023/2854 (akt w sprawie danych).

Art. 1 dotyczy zmian w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) 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.

W art. 1:

W pkt 1 zaktualizowano zakres rozporządzenia (UE) 2023/2854 (akt w sprawie danych), do którego zostaną dodane nowe rozdziały, jak wyjaśniono poniżej.

W pkt 2 zmienia się definicje i dodaje nowe.

W pkt 3 ustanawia się nowy przepis na podstawie art. 4 ust. 8 rozporządzenia (UE) 2023/2854 (akt w sprawie danych), który umożliwia posiadaczom danych odmowę ujawnienia tajemnicy przedsiębiorstwa użytkownikowi, jeżeli istnieje wysokie ryzyko bezprawnego pozyskiwania, wykorzystywania lub ujawniania informacji państwom trzecim lub podmiotom pozostającym pod ich kontrolą, które podlegają jurysdykcjom o słabszych zabezpieczeniach niż dostępne w Unii.

W pkt 5 wprowadzono ten sam przepis w odniesieniu do art. 5 ust. 11 rozporządzenia (UE) 2023/2854 (akt w sprawie danych) odnośnie do posiadaczy danych ujawniających tajemnice przedsiębiorstwa osobom trzecim.

W pkt 5–19 zawężono zakres rozdziału V z „wyjątkowych potrzeb” wyłącznie do „niebezpieczeństwa publicznego”. Uchyla się w nich art. 14 i 15 oraz tworzy się nowy art. 15a, który staje się jedynym artykułem dotyczącym składania wniosków w przypadku wystąpienia niebezpieczeństwa publicznego w ramach systemu B2G ustanowionego w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych). Wnioski można składać, gdy jest to konieczne w celu zareagowania na niebezpieczeństwo publiczne (art. 15a ust. 2), lub w celu złagodzenia sytuacji lub wsparcia procesu przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego (art. 15a ust. 3). Odpowiednio dostosowuje się wzajemne odniesienia, a język jest prostszy i jaśniejszy. W art. 1 pkt 21 tworzy się nowy art. 22a, który określa ramy systemu rozpatrywania skarg na podstawie rozdziału V i łączy ze sobą wcześniej powtarzające się przepisy.

Pkt 20–22 obejmują pewne wyłączenia z rozdziału VI rozporządzenia (UE) 2023/2854 (akt w sprawie danych) (zmiana dostawcy usług przetwarzania danych): w art. 31 wprowadzono łagodniejsze szczegółowe uregulowania w odniesieniu do usług przetwarzania danych, które są wykonywane na zamówienie, tj. usług przetwarzania danych, które nie są gotowym rozwiązaniem i nie funkcjonowałyby bez uprzedniego dostosowania do potrzeb i ekosystemu

użytkownika, jeżeli są świadczone na podstawie umów zawartych przed dniem 12 września 2025 r. Podobnie w art. 31 wprowadzono nowe, łagodniejsze szczegółowe uregulowania w odniesieniu do usług przetwarzania danych świadczonych przez MŚP i małe spółki o średniej kapitalizacji na podstawie umów zawartych przed dniem 12 września 2025 r., wraz z wyjaśnieniem, że dostawcy ci mogą włączać kary za przedterminowe rozwiązanie umowy do umów na czas określony.

Pkt 23–25 obejmują zmiany w art. 32 rozporządzenia (UE) 2023/2854 (akt w sprawie danych) wynikające z włączenia do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) organów obecnie regulowanych rozporządzeniem (UE) 2022/868 (akt w sprawie zarządzania danymi).

W pkt 26 zniesiono obowiązki spełniania zasadniczych wymagań przez dostawców inteligentnych umów, wraz z nadaniem Komisji uprawnienia do przyjmowania norm zharmonizowanych.

W pkt 27 połączono dwa systemy prawne zawarte obecnie w rozporządzeniu (UE) 2022/868 (akt w sprawie zarządzania danymi), które zostanie uchylone po wejściu w życie aktu zbiorczego prawa cyfrowego. W punkcie tym zreformowano obecne przepisy zawarte w rozdziałach III i IV aktu w sprawie zarządzania danymi, które przewidują obowiązkowy system zgłaszania dla dostawców usług pośrednictwa danych oraz dobrowolny system rejestracji organizacji altruizmu danych. Oba systemy wprowadza się jako nowy rozdział VIIa do rozporządzenia (UE) 2023/2854 (akt w sprawie danych). W świetle wschodzącego charakteru rynku usług pośrednictwa danych należy uelastycznić obowiązki określone w rozporządzeniu (UE) 2022/868 (akt w sprawie zarządzania danymi), aby umożliwić rozwój tego rynku: po pierwsze, system dostawców usług pośrednictwa danych zostaje przekształcony w system dobrowolny. Po drugie, najistotniejszy obowiązek, tj. obowiązek prawnego oddzielenia usług pośrednictwa danych od wszelkich innych usług, które przedsiębiorstwo może zechcieć oferować, zastąpi się obowiązkiem funkcjonalnego oddzielenia usług w połączeniu z dodatkowym zestawem warunków. Wreszcie drastycznie skrócono wykaz obowiązków. Jeżeli chodzi o altruizm danych, uchyla się obowiązki organizacji altruizmu danych w zakresie sprawozdawczości i przejrzystości, a także pomysł uzupełnienia przepisów rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) w „zbiorze przepisów dotyczących altruizmu danych” o jeszcze bardziej szczegółowe przepisy.

Wprowadza się nowy rozdział VIIb, na mocy którego do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) dodano zakaz stosowania wymogów dotyczących lokalizacji w odniesieniu do danych nieosobowych na obszarze Unii, zawarty wcześniej w uchylanym rozporządzeniu (UE) 2018/1807 (rozporządzenie w sprawie swobodnego przepływu danych nieosobowych). Utrzymano obowiązek powiadamiania Komisji, ale zniesiono krajowy centralny internetowy punkt informacyjny, w którym państwa członkowskie powinny publikować mające zastosowanie wymogi dotyczące lokalizacji danych.

W pkt 4 i 33–58 wprowadzono połączone przepisy dotyczące ponownego wykorzystywania danych i dokumentów będących w posiadaniu organów sektora publicznego na podstawie rozdziału II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) i dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych):

- w pkt 4 wprowadzono definicje z przepisów wprowadzonych do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) harmonizujące definicję danych i dokumentów przez zapewnienie ścisłego rozgraniczenia między treściami cyfrowymi (dane) i niecyfrowymi (dokumenty);

- wprowadza się nowy rozdział VIIc dotyczący ponownego wykorzystywania danych i dokumentów będących w posiadaniu organów sektora publicznego;
- wprowadza się nową sekcję 1 zawierającą ogólne zasady mające zastosowanie do nowo dodanego rozdziału;
- wprowadza się przedmiot i zakres połączonego rozdziału, łączącego wspólne przepisy rozdziału II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) i dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych);
- określa się wspólną zasadę niedyskryminacji mającą zastosowanie do udostępniania otwartych danych publicznych i niektórych kategorii danych chronionych;
- ustanawia się zakaz uzgodnień dotyczących wyłączności, wspólny dla systemu otwartych danych publicznych i niektórych kategorii danych chronionych;
- określa się ogólne zasady dotyczące pobierania opłat za ponowne wykorzystywanie otwartych danych publicznych lub niektórych kategorii danych chronionych. Zgodnie z nowym przepisem organy sektora publicznego będą musiały zapewnić możliwość uiszczania wszelkich opłat również przez internet za pośrednictwem powszechnie dostępnych transgranicznych usług płatniczych, bez dyskryminacji, za ponowne wykorzystywanie otwartych danych publicznych. Stanowi to rozszerzenie tego przepisu, znanego wcześniej jedynie w odniesieniu do ponownego wykorzystywania niektórych kategorii danych chronionych na podstawie rozdziału II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi);
- przewiduje się prawo ponownych użytkowników otwartych danych publicznych i niektórych kategorii danych chronionych do uzyskania informacji o dostępnych środkach odwoławczych w odniesieniu do decyzji lub praktyk, które na nich wpływają;
- dodaje się sekcję dotyczącą przepisów w sprawie ponownego wykorzystywania otwartych danych publicznych, dawniej przepisów dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych);
- określa się zakres sekcji, w tym brak stosowania do niektórych kategorii danych chronionych objętych zakresem ogólnego rozdziału dotyczącego ponownego wykorzystywania danych i dokumentów będących w posiadaniu organów sektora publicznego;
- określa się ogólną zasadę ponownego wykorzystywania otwartych danych publicznych;
- określa się zasady przetwarzania wniosków o ponowne wykorzystywanie otwartych danych publicznych, dodając dawny przepis dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych);
- wprowadza się przepisy w sprawie dostępnych formatów ponownego wykorzystywania otwartych danych publicznych, wcześniej zawarte w dyrektywie (UE) 2019/1024 (dyrektywa w sprawie otwartych danych);
- wprowadza się przepisy regulujące pobieranie opłat za otwarte dane publiczne, wcześniej regulowane dyrektywą (UE) 2019/1024 (dyrektywa w sprawie otwartych danych). Zgodnie z nową zasadą organy sektora publicznego mogą pobierać wyższe opłaty za ponowne wykorzystywanie przez bardzo duże przedsiębiorstwa. Takie opłaty muszą być proporcjonalne, a ich wysokość musi opierać się na obiektywnych kryteriach;

- wprowadza się przepisy w sprawie licencji standardowych na ponowne wykorzystywanie otwartych danych publicznych, wcześniej zawarte w dyrektywie (UE) 2019/1024 (dyrektywa w sprawie otwartych danych). Zgodnie z nową zasadą organy sektora publicznego mogą przewidzieć specjalne warunki dla bardzo dużych przedsiębiorstw. Warunki te muszą być proporcjonalne i oparte na obiektywnych kryteriach;
- w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie ustaleń praktycznych zawarte wcześniej w dyrektywie (UE) 2019/1024 (dyrektywa w sprawie otwartych danych), aby ułatwić wyszukiwanie danych lub dokumentów dostępnych do ponownego wykorzystywania;
- w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie danych badawczych zawarte wcześniej w dyrektywie (UE) 2019/1024 (dyrektywa w sprawie otwartych danych);
- w rozporządzeniu (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie zbiorów danych o wysokiej wartości, wcześniej zawarte w dyrektywie (UE) 2019/1024 (dyrektywa w sprawie otwartych danych);
- tworzy się nową sekcję dotyczącą ponownego wykorzystywania niektórych kategorii danych chronionych w celu włączenia do tego rozdziału dawnych przepisów rozdziału II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi). W punkcie tym określono zakres stosowania tej sekcji trzeciej, która wyłącza z zakresu stosowania dane i dokumenty objęte zakresem sekcji drugiej, regulującej system ponownego wykorzystywania otwartych danych publicznych. Zgodnie z nową zasadą dokumenty wchodzą w zakres tej sekcji;
- ustanawia się ogólną zasadę dotyczącą ponownego wykorzystywania niektórych kategorii danych chronionych. Jest to zasada określona w rozdziale II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi), zgodnie z którą w sekcji tej nie nakłada się na organy sektora publicznego obowiązku zezwalania na ponowne wykorzystywanie danych chronionych, lecz określa się minimalne warunki, na jakich organy sektora publicznego podejmują decyzję o udostępnieniu takich danych do ponownego wykorzystywania;
- wprowadza się przepisy w sprawie warunków ponownego wykorzystywania niektórych kategorii danych chronionych, wcześniej zawarte w rozdziale II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi), w uproszczonej i usprawnionej formie. Zawierają one wyjaśnienie, które przepisy mają zastosowanie w przypadkach, gdy dane osobowe zanonimizowano. Utrzymano wymogi dotyczące przekazywania danych nieosobowych do państw trzecich, ale podzielono je na nowy artykuł w pkt 54;
- do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie pobierania opłat, dawniej stanowiące część rozdziału II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi). Zgodnie z nową zasadą organy sektora publicznego mogą przewidzieć wyższe opłaty za ponowne wykorzystywanie przez bardzo duże przedsiębiorstwa. Takie opłaty muszą być proporcjonalne i oparte na obiektywnych kryteriach. Szczególne zachęty dla MŚP do ponownego wykorzystywania rozszerzono na małe spółki o średniej kapitalizacji;
- do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie właściwych organów, dawniej stanowiące część rozdziału II

rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi). Właściwe organy mają pomagać organom sektora publicznego w odpowiadaniu na wnioski o ponowne wykorzystywanie danych i dokumentów, o których mowa w sekcji 3;

- do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie pojedynczego punktu informacyjnego, dawniej stanowiące część rozdziału II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi). Pojedyncze punkty informacyjne mają pomóc ponownym użytkownikom w łatwym znalezieniu informacji na temat ponownego wykorzystywania niektórych kategorii danych chronionych;
- do rozporządzenia (UE) 2023/2854 (akt w sprawie danych) wprowadza się przepisy w sprawie procedury składania wniosków o ponowne wykorzystywanie niektórych kategorii danych chronionych, uregulowane wcześniej w rozdziale II rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi).

W pkt 57 uwzględniono podstawowe przepisy dotyczące Europejskiej Rady ds. Innowacji w zakresie Danych (EDIB), grupy doradzającej Komisji w obszarze spójnego egzekwowania aktu w sprawie danych i służącej jako forum koordynacji kształtowania polityki w dziedzinie gospodarki opartej na danych. Komisja włączy podstawowe przepisy do aktu w sprawie danych. Zmiany te umożliwią Komisji modyfikację odpowiednich dokumentów założycielskich Europejskiej Rady ds. Innowacji w zakresie Danych (decyzja Komisji z dnia 20 lutego 2023 r. – C(2023)1074 final) i rozszerzenie członkostwa na przedstawicieli krajowych podmiotów kształtujących politykę, oprócz właściwych organów.

Pkt 61–65 obejmują zmiany przepisów rozporządzenia (UE) 2023/2854 (akt w sprawie danych) dotyczących procedury komitetowej i uprawnień do przyjmowania aktów delegowanych, a pkt 66 zmiany w rozporządzeniu (UE) 2022/868 (akt w sprawie zarządzania danymi) niezbędne do wprowadzenia przepisów rozporządzenia (UE) 2022/868 (akt w sprawie zarządzania danymi) i dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych) do rozporządzenia (UE) 2023/2854 (akt w sprawie danych).

W pkt 68 szczególną uwagę poświęconą MŚP w kontekście oceny rozszerzono na małe spółki o średniej kapitalizacji, a w pkt 69 wprowadzono ocenę nowo wprowadzonych przepisów do rozporządzenia (UE) 2023/2854 (akt w sprawie danych).

W **art. 2** wprowadzono do rozporządzenia (UE) 2018/174 odpowiednie odniesienia do usług pośrednictwa danych i altruizmu danych w załączniku dotyczącym „rozpoczęcia, odnowienia i zamknięcia działalności gospodarczej”.

Zmiany w rozporządzeniu (UE) 2016/679, rozporządzeniu (UE) 2018/1725 i dyrektywie 2002/58/WE

W art. 3 wniosku wprowadza się ukierunkowane zmiany w rozporządzeniu (UE) 2016/679 („ogólne rozporządzenie o ochronie danych”).

W art. 3:

W pkt 1 doprecyzowuje się definicję danych osobowych zawartą w art. 4 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) przez stwierdzenie, że informacji nie uznaje się za dane osobowe w odniesieniu do danego podmiotu, jeżeli nie dysponuje on środkami, co do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane do zidentyfikowania osoby fizycznej, której dotyczą informacje. W związku z tym taki podmiot nie byłby co do zasady objęty zakresem stosowania tego rozporządzenia.

W pkt 2 przewiduje się dwa dodatkowe zwolnienia dotyczące przetwarzania szczególnych kategorii danych: przewidziano zwolnienie z ogólnego zakazu przetwarzania danych biometrycznych, gdy jest to konieczne do potwierdzenia tożsamości osoby, której dane dotyczą, oraz gdy dane i środki do takiej weryfikacji znajdują się pod wyłączną kontrolą tej osoby, której dane dotyczą. Przewidziano również zwolnienie dotyczące rezydualnego przetwarzania szczególnych kategorii danych osobowych na potrzeby opracowania i eksploatacji systemu AI lub modelu AI, z zastrzeżeniem pewnych warunków, w tym odpowiednich środków organizacyjnych i technicznych, aby uniknąć gromadzenia szczególnych kategorii danych osobowych i usuwania takich danych.

W pkt 3 zawarto objaśnienie sytuacji określonej w art. 12 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych), w przypadku gdy osoby, których dane dotyczą, nadużywają prawa dostępu do celów innych niż ochrona ich danych osobowych. W związku z tym administrator mógłby odmówić zastosowania się do żądania lub pobrać rozsądną opłatę. Ponadto doprecyzowuje się warunki wykazania, że żądanie udzielenia dostępu było nadmierne.

W pkt 4 skoncentrowano się na spoczywającym na administratorze obowiązku informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych na podstawie art. 13 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) przez zniesienie tego obowiązku w sytuacjach, w których istnieją uzasadnione podstawy, by przypuszczać, że osoba, której dane dotyczą, posiada już te informacje, chyba że administrator przekazuje dane innym odbiorcom lub kategoriom odbiorców, przekazuje dane do państwa trzeciego, dokonuje zautomatyzowanego podejmowania decyzji lub przetwarzanie może powodować wysokie ryzyko naruszenia praw osoby, której dane dotyczą.

W pkt 5 doprecyzowuje się wymogi dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach na podstawie art. 22 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) w kontekście zawierania lub wykonywania umowy między osobą, której dane dotyczą, a administratorem danych, w szczególności że wymóg „konieczności” jest niezależny od tego, czy decyzję można by podjąć w inny sposób niż w sposób całkowicie zautomatyzowany.

W pkt 6 dostosowuje się spoczywający na administratorze obowiązek powiadamiania właściwego organu nadzorczego o naruszeniach ochrony danych na podstawie art. 33 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) do spoczywającego na nim obowiązku powiadamiania osób, których dane dotyczą, o takich naruszeniach, stanowiąc, że powiadomienie jest wymagane tylko wtedy, gdy naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw osoby, której dane dotyczą. Wydłuża się również termin powiadomienia do 96 godzin. Proponuje się również, aby administratorzy korzystali z pojedynczego punktu kontaktowego, gdy zgłaszają organowi nadzorczemu naruszenia ochrony danych. Ponadto Europejska Rada Ochrony Danych zostanie zobowiązana do przygotowania i przedłożenia Komisji wniosku w sprawie wspólnego wzoru powiadomienia o naruszeniu ochrony danych, który Komisja będzie uprawniona przyjąć w drodze aktu wykonawczego, w razie potrzeby po dokonaniu jego przeglądu.

W pkt 7 harmonizuje się wykazy czynności przetwarzania wymagających i niewymagających oceny skutków dla ochrony danych, stanowiąc, że na szczeblu UE należy przedstawić pojedyncze wykazy operacji przetwarzania, które wymagają i nie wymagają oceny skutków dla ochrony danych, aby przyczynić się do harmonizacji pojęcia wysokiego ryzyka. Europejska Rada Ochrony Danych zostanie zobowiązana do przygotowania wniosków dotyczących takich wykazów. Będzie ona również zobowiązana do przygotowania wniosku w

sprawie wspólnego wzoru i wspólnej metodyki przeprowadzania ocen skutków dla ochrony danych, do przyjęcia których Komisja zostanie uprawniona w drodze aktu wykonawczego, w razie potrzeby po dokonaniu ich przeglądu.

Pkt 8 stanowi, że Komisja wraz z Europejską Radą Ochrony Danych może wspierać administratorów w ocenie, czy dane wynikające z pseudonimizacji nie stanowią danych osobowych, przez określenie środków i kryteriów istotnych dla takiej oceny, w tym najnowocześniejszych dostępnych technik i kryteriów w celu oceny ryzyka deanonimizacji.

W pkt 12 zreformowano system prawny dotyczący przetwarzania danych osobowych na końcowych urządzeniach lub z takich urządzeń („urządzenia podłączone do internetu"), który jest obecnie częścią dyrektywy 2002/58/WE (dyrektywa o e-prywatności). Do rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) dodano nowy art. 88a, który ustanawia wymóg uzyskania zgody na przechowywanie danych osobowych na końcowym urządzeniu osób fizycznych lub na dostęp do takich danych i który włącza przetwarzanie danych osobowych na końcowym urządzeniu i z takiego urządzenia do przepisów rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych). Nowy art. 88b rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) dotyczy zautomatyzowanych i nadających się do odczytu maszynowego wskazań indywidualnych wyborów i stosowania się do tych wskazań przez dostawców stron internetowych po udostępnieniu norm.

W art. 4:

W art. 4 wniosku wprowadza się ukierunkowane zmiany w rozporządzeniu (UE) 2018/1725 w celu dostosowania jego tekstu do zmian w rozporządzeniu (UE) 2016/679 wprowadzonych w art. 3.

W art. 5:

W art. 5 przewidziano zmiany dyrektywy 2002/58/WE, tj. dyrektywy o prywatności i łączności elektronicznej („dyrektywa o e-prywatności"). Uchyla się art. 4 tej dyrektywy. Dodanie do art. 5 ust. 3 tej dyrektywy pozwala na przeniesienie do rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) przepisów dotyczących przechowywania danych osobowych i dostępu do danych osobowych z końcowego urządzenia osoby fizycznej przez dodanie nowego art. 88a rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych), jak opisano powyżej.

Pojedynczy punkt kontaktowy do zgłaszania incydentów

W art. 6:

W pkt 1 i 2 ustanawia się pojedynczy punkt kontaktowy do zgłaszania incydentów, uwzględniając szczegółowe wymogi wobec ENISA. Ponadto ustala się, że zgłaszanie incydentów wymagane na mocy dyrektywy NIS 2 powinno odbywać się za pośrednictwem nowego pojedynczego punktu kontaktowego.

W art. 7: pojedynczy punkt kontaktowy jest również wymagany do zgłaszania incydentów na podstawie rozporządzenia (UE) nr 910/2014 (rozporządzenie eIDAS).

W art. 8: pojedynczy punkt kontaktowy jest również wymagany w odniesieniu do rozporządzenia (UE) 2022/2554 (DORA).

W art. 9: pojedynczy punkt kontaktowy jest również wymagany w odniesieniu do dyrektywy (UE) 2022/2557 (CER).

Ponadto zgodnie z art. 3 ust. 6 za pośrednictwem pojedynczego punktu kontaktowego wymagane jest również zgłaszanie incydentów naruszenia ochrony danych na potrzeby rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych). W art. 5 ust. 1 uchyla się wymogi sprawozdawcze określone w dyrektywie 2002/58/WE (dyrektywa o e-prywatności), ponieważ są one nieaktualne w świetle przepisów rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych).

Uchylenie aktów prawnych i przepisy końcowe

W art. 10:

W pkt 1 uchyla się rozporządzenie (UE) 2019/1150 (rozporządzenie P2B), co do którego uznano, że ma ono rezydualne znaczenie w świetle niedawnych przepisów, które w dużej mierze obejmują te same kwestie. Na zasadzie odstępstwa pkt 2 dotyczy wszelkich odniesień do rozporządzenia (UE) 2019/1150 (rozporządzenie P2B) w innych instrumentach prawnych: aby uniknąć wszelkiej niepewności prawa, będą one nadal mieć zastosowanie do czasu ich zmiany w pierwotnych aktach, najpóźniej do dnia 31 grudnia 2032 r.

W pkt 3 uchyla się teksty prawne wchłonięte do rozporządzenia (UE) 2023/2854 (akt w sprawie danych).

W **art. 11** ustanowiono przepisy końcowe rozporządzenia zmieniającego.

2025/0360 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zmiany rozporządzeń (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektyw 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram prawnych oraz uchylenia rozporządzeń (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 i dyrektywy (UE) 2019/1024 (akt zbiorczy prawa cyfrowego)

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[21],

uwzględniając opinię Europejskiego Banku Centralnego[22],

uwzględniając opinię Komitetu Regionów[23],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W swoim komunikacie w sprawie prostszej i szybszej Europy[24] Komisja ogłosiła swoje zobowiązanie do realizacji ambitnego programu na rzecz promowania przyszłościowych, innowacyjnych polityk, które wzmacniają konkurencyjność Unii i radykalnie zmniejszają obciążenie regulacyjne obywateli, przedsiębiorstw i administracji, przy jednoczesnym utrzymaniu najwyższych standardów promowania wartości Unii. W związku z tym Komisja priorytetowo potraktowała wniosek dotyczący natychmiastowego dostosowania przepisów, w tym przepisów cyfrowych, w celu sprostania wyzwaniu, jakim jest konkurencyjność Unii.

---

[21] Dz.U. C […], […], s. […].

[22] Dz.U. C […], […], s. […].

[23] Dz.U. C […], […], s. […].

[24] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Prostsza i szybsza Europa: komunikat dotyczący wdrażania i upraszczania”, COM(2025) 47 final, 11 lutego 2025 r.

(2) Unijne przepisy cyfrowe wyznaczają wysokie standardy w Unii i mogą być potężnym źródłem przewagi konkurencyjnej dla przedsiębiorstw, które przestrzegają przepisów, stanowiąc wiodący na skalę międzynarodową znak jakości, bezpieczeństwa i wiarygodności. W przepisach cyfrowych określono jasne zasady działania w Unii skierowane do odpowiedzialnych przedsiębiorstw, zapewniając uczciwość i przejrzystość w relacjach między przedsiębiorstwami, stymulując innowacyjne modele biznesowe oraz ustanawiając wysokie standardy ochrony i bezpieczeństwa konsumentów, a także ochrony praw podstawowych, zwłaszcza prywatności i ochrony danych.

(3) Unijne przepisy cyfrowe zmieniały się stopniowo w ostatnich latach w odpowiedzi na szybko zwiększający się ślad technologii cyfrowych w gospodarce i dynamikę społeczną Unii oraz w celu sprostania pojawiającym się wyzwaniom i promowania możliwości rynkowych w UE. Niezależnie od zobowiązania Komisji do przeprowadzania systematycznego „testu warunków skrajnych" przepisów cyfrowych wraz z innymi przepisami unijnymi, który mógłby prowadzić do dalszych dostosowań regulacyjnych, w szczególności w następstwie zbliżającej się oceny adekwatności przepisów cyfrowych, a także innych ukierunkowanych ocen przepisów cyfrowych, konieczne są natychmiastowe zmiany regulacyjne. W związku z tym w niniejszym rozporządzeniu proponuje się pierwszy zestaw zmian w cyfrowych ramach prawnych, mających na celu zapewnienie natychmiastowych wyjaśnień regulacyjnych, które stymulują innowacje na rynku unijnym i obniżają administracyjne koszty przestrzegania przepisów, w szczególności dla przedsiębiorstw, przy jednoczesnym ograniczeniu kosztów nadzorczych i administracyjnych ponoszonych przez organy nadzorcze i organy doradcze. Zmiany mają również zapewnić jasność osobom fizycznym.

(4) Biorąc pod uwagę zasadniczą rolę danych w tworzeniu wartości w gospodarce cyfrowej oraz zgodnie z celami komunikatu w sprawie strategii na rzecz europejskiej unii danych, przedstawione w niniejszym rozporządzeniu zmiany ram prawnych dotyczących danych mają na celu stworzenie spójnych h ram regulacyjnych dotyczących dostępności i wykorzystywania danych, usprawniając i konsolidując ramy regulacyjne dotyczące danych w tylko dwóch aktach prawnych, a mianowicie w rozporządzeniach Parlamentu Europejskiego i Rady (UE) 2016/679[25] i (UE) 2023/2854[26], zamiast pięciu obecnie obowiązujących aktów prawnych. Zmiany mają na celu zmniejszenie zbędnych kosztów administracyjnych i stymulowanie dostępności danych jako warunku wstępnego wspierania konkurencyjnych przedsiębiorstw cyfrowych w Unii przy jednoczesnym utrzymaniu najwyższych standardów ochrony prywatności, ochrony danych osobowych i uczciwych praktyk

---

[25] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[26] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO i RADY (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych).

biznesowych oraz zapewnieniu podstawowych celów regulacyjnych, w tym zgodności z unijnym i krajowym prawem konkurencji.

(5) Uwzględniając wielokrotne zmiany przepisów horyzontalnych i sektorowych, należy również zająć się kwestią nakładania się przepisów szczegółowych, które prowadzi do niepotrzebnego powielania obciążeń administracyjnych. Odnosi się to do wymogów zawartych w kilku przepisach dotyczących zgłaszania incydentów związanych z cyberbezpieczeństwem i incydentów powiązanych, w przypadku których rozwiązania cyfrowe zaproponowane w niniejszym rozporządzeniu mogą przynieść natychmiastową pomoc przedsiębiorstwom we wszystkich zainteresowanych sektorach.

(6) Podobnie w ostatnich latach podejmowano wielokrotne próby regulowania platform internetowych, przy czym nowsze przepisy ustanowiły jaśniejsze i ambitniejsze ramy niż niektóre wcześniejsze przepisy, które stały się przestarzałe. Konieczne jest zatem przekształcenie ram prawnych, aby wyeliminować wszelkie zbędne powielanie zwiększające złożoność prawa.

(7) W rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/868[27] ustanowiono przepisy dotyczące funkcji pośrednika w trzech różnych kontekstach: a) funkcje wspierające ponowne wykorzystywanie chronionych danych będących w posiadaniu organów sektora publicznego w kontrolowanych warunkach; b) usługi pośrednictwa danych ułatwiające dzielenie się danymi między osobami, których dane dotyczą, posiadaczami danych i użytkownikami danych; oraz c) organizacje altruizmu danych, które wspierają wykorzystywanie danych udostępnianych przez osoby, których dane dotyczą, i posiadaczy danych z pobudek altruistycznych lub charytatywnych. Funkcje wspierające ponowne wykorzystywanie danych chronionych będących w posiadaniu sektora publicznego są ściśle powiązane z przepisami dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024[28]. Wzajemne zależności między nimi spowodowały dezorientację, zwłaszcza wśród organów sektora publicznego. Konieczne jest zatem połączenie tych dwóch zbiorów przepisów. Ocena przepisów dotyczących usług pośrednictwa danych pokazała, że w definicji dostawców usług pośrednictwa danych występują niedociągnięcia oraz że przepisy są zbyt rygorystyczne, aby dostawcy usług mogli znaleźć zrównoważony model finansowy. Konieczne jest zatem również usprawnienie systemu. W odniesieniu do altruizmu danych niektóre przepisy rozporządzenia (UE) 2022/868, w szczególności zobowiązanie państw członkowskich do wprowadzenia krajowych polityk w zakresie altruizmu danych, ustanowienie „zbioru prawa” i opracowanie europejskiego formularza zgody na potrzeby altruizmu danych, wydają się zbędne, również w świetle trwających prac Europejskiej Rady Ochrony Danych, o której mowa w art. 68

---

[27] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi), Dz.U. L 152 z 3.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

[28] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 172 z 26.6.2019, s. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[29], nad wytycznymi w sprawie przetwarzania danych osobowych w kontekście badań naukowych.

(8) Chociaż znaczenie usług pośrednictwa danych uznaje się w kontekście wielu inicjatyw, które wspierają dzielenie się danymi i współpracę, należy doprecyzować przepisy rozporządzenia (UE) 2022/868 dotyczące dostawców usług pośrednictwa danych. W szczególności należy doprecyzować definicję takich dostawców. Powinna ona wyeliminować elementy, które służyły jedynie jako przykłady, a nie stanowiły wyjątków. Ponadto powinna eliminować luki wynikające z niejednoznacznych sformułowań, w szczególności w odniesieniu do pojęcia „zamkniętej grupy". Usługi nie powinny kwalifikować się do rejestracji jako usługi pośrednictwa danych, jeżeli wykorzystuje je wyłącznie zamknięta grupa przedsiębiorstw i jeżeli decyzję o rozszerzeniu tej grupy przedsiębiorstw może podjąć wyłącznie ta grupa, a nie dostawca usług. Co ważniejsze, objęcie tego wschodzącego rynku obowiązkowym systemem spowodowało niepotrzebne koszty przestrzegania przepisów. Na tym etapie rozwoju rynku wystarczający wydaje się dobrowolny system umożliwiający neutralnym podmiotom odróżnienie się od innych podmiotów. Ponadto, aby zapewnić zrównoważone modele biznesowe, należy zmniejszyć rygorystyczność systemu przez zniesienie wymogu prawnego oddzielenia usług pośrednictwa danych od innych usług o wartości dodanej, które powinna móc oferować dana usługa, zastępując go funkcjonalnym oddzieleniem przy jednoczesnym zachowaniu pewnych zabezpieczeń. Należy uprościć administracyjny system monitorowania. Zamiast krajowego i unijnego rejestru publicznego dostawców usług pośrednictwa danych i organizacji altruizmu danych powinny istnieć wyłącznie unijne rejestry publiczne, a mianowicie jeden dla dostawców usług pośrednictwa danych i drugi dla organizacji altruizmu danych. Właściwe organy nadzorujące przyznawanie znaku i spełnianie przez podmioty wymogów w celu jego uzyskania powinny być niezależne w wykonywaniu tego zadania. Należy to rozumieć w taki sposób, że muszą być one prawnie i funkcjonalnie niezależne od usługi pośrednictwa danych lub organizacji altruizmu danych, w tym na poziomie ich ścisłego kierownictwa. Organizacje rządowe powinny mieć możliwość finansowego wspierania usług pośrednictwa danych lub organizacji altruizmu danych, w szczególności ze względu na rozwojowy charakter tych podmiotów, pod warunkiem że są one odrębnymi osobami prawnymi. Aby zapewnić łatwą identyfikację uznanych podmiotów w całej Unii, Komisja ustanowiła rozporządzenie wykonawcze (UE) 2023/1622 w sprawie wzoru wspólnych logo służących identyfikacji uznanych w Unii dostawców usług pośrednictwa danych i organizacji altruizmu danych.

(9) Rozporządzenie (UE) 2023/2854 usuwa bariery w dostępie do danych i ich wykorzystywaniu, odblokowuje innowacje i konkurencyjność oparte na danych oraz chroni zachęty dla podmiotów inwestujących w technologie danych.

---

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

(10) W rozdziale II rozporządzenia (UE) 2023/2854 zobowiązano posiadaczy danych do udostępniania danych, w tym danych chronionych jako tajemnice przedsiębiorstwa, użytkownikom i wybranym przez nich osobom trzecim pod warunkiem utrzymania środków poufności ustanowionych przez posiadacza danych. Ten wymóg zachowania poufności stanowi uzupełnienie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943[30], w której określono standard ochrony tajemnic przedsiębiorstwa w Unii. Ujawnienie tajemnic przedsiębiorstwa podmiotom z państw trzecich może jednak zwiększyć ryzyko naruszenia ich integralności i poufności, jeżeli podlegają jurysdykcjom o nieodpowiednich zabezpieczeniach lub trudnościach w ich faktycznym egzekwowaniu, co mogłoby prowadzić do nieuprawnionego wykorzystania, szkód gospodarczych i braku pewności prawa.

(11) Należy wzmocnić rozporządzenie (UE) 2023/2854 przez wprowadzenie dodatkowej podstawy odmowy ujawnienia tajemnic przedsiębiorstwa przez posiadaczy danych, aby uzupełnić istniejące przepisy, które umożliwiają odmowę na podstawie wykazania przez posiadacza danych wysokiego prawdopodobieństwa wystąpienia poważnych szkód gospodarczych. Zgodnie z nowym przepisem posiadacze danych mogą odmówić ujawnienia tajemnic przedsiębiorstwa, jeżeli wykażą wysokie ryzyko bezprawnego pozyskiwania, wykorzystywania lub ujawniania podmiotom, które podlegają systemom charakteryzującym się nieodpowiednią ochroną oraz nierównoważnymi lub słabszymi ramami prawnymi niż mające zastosowanie przepisy Unii. Nowy przepis obejmuje również przypadki, w których ramy prawne państwa trzeciego teoretycznie są solidne lub bardziej rygorystyczne niż takie przepisy unijne, ale nie są odpowiednio egzekwowane w praktyce. Takie ryzyko uwypukla możliwość pozyskiwania, wykorzystywania lub ujawniania tajemnic przedsiębiorstwa z naruszeniem prawa Unii, co zagraża integralności i poufności tajemnic przedsiębiorstwa.

(12) Uruchomienie mechanizmu odmowy powinno pozostać dobrowolne, a wykazane informacje należy przedstawić dopiero po jego uruchomieniu. Posiadacze danych nie powinni być zobowiązani do przeprowadzenia pełnej analizy lub wykazania poziomu ochrony tajemnicy przedsiębiorstwa w państwach trzecich lub przez podmiot z państwa trzeciego jako warunku wstępnego, aby móc uzasadnić odmowę dzielenia się danymi lub ujawnienia tajemnic przedsiębiorstwa. Podczas wykazywania informacji posiadacze danych mogą wziąć pod uwagę różne czynniki, takie jak niewystarczające lub nieodpowiednie normy prawne, słabe lub arbitralne egzekwowanie, historyczne naruszenia przepisów, obowiązki ujawniania informacji za granicą sprzeczne z prawem Unii, ograniczone środki odwoławcze lub środki zaradcze dla podmiotów Unii, strategiczne nadużywanie taktyk proceduralnych w celu osłabienia konkurentów lub nadmierne wpływy polityczne. Biorąc pod uwagę różnorodność zaangażowanych podmiotów, państw trzecich i scenariuszy dzielenia się danymi, posiadacze danych powinni skoncentrować swoją ocenę i wykazane informacje na istotnych ryzykach i podjąć odpowiednie działania, w tym przez ustanowienie odpowiednich zabezpieczeń

[30] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.U. L 157 z 15.6.2016, s. 1).

lub uruchomienie mechanizmu odmowy. Odmowy powinny być jasne, proporcjonalne i dostosowane do szczególnych okoliczności każdej sprawy, a nie stosowane systematycznie lub w sposób ogólny w całym państwie trzecim.

(13) Niewystarczająca ochrona tajemnic przedsiębiorstwa i wyzwania związane z jej egzekwowaniem w państwach trzecich mogą powodować nieodwracalne szkody dla europejskich przedsiębiorstw. Celem jest zatem wzmocnienie zabezpieczeń tajemnic przedsiębiorstwa przez zapobieganie ich wyciekowi do osób fizycznych lub prawnych mających siedzibę w jurysdykcjach stwarzających takie ryzyko lub podlegających takim jurysdykcjom. Obejmuje to podmioty z siedzibą w Unii kontrolowane przez podmioty z państw trzecich, które mogą działać w złej wierze lub jako przykrywki dla podmiotów z państw trzecich. Ponadto celem jest zapobieganie bezpośredniemu narażeniu na działania podmiotów z państw trzecich prowadzących działalność w Unii, które podlegają takim jurysdykcjom. Podleganie jurysdykcji państwa trzeciego oznacza, że osoba fizyczna lub prawna jest prawnie regulowana, kontrolowana lub w inny sposób związana przepisami ustawowymi lub z organem regulacyjnym państwa trzeciego. Jednostki zależne lub powiązane jednostek dominujących z państw trzecich mogą wykorzystywać te jurysdykcje do unikania lub obchodzenia prawa Unii. Bezpośrednia lub pośrednia kontrola odnosi się do zdolności do wywierania decydującego lub dominującego wpływu na zarządzanie lub decyzje strategiczne innego podmiotu za pośrednictwem własności kapitału lub praw głosu, wkładu finansowego, ustaleń umownych lub podmiotów pośredniczących. Kontrolę można sprawować bezpośrednio lub w inny sposób, nawet bez udziału większościowego. Posiadacze danych powinni dołożyć wszelkich starań, aby uzyskać odpowiednie informacje, co może obejmować wyszukiwanie w rejestrach publicznych lub zwrócenie się o nie bezpośrednio do użytkownika lub osoby trzeciej, przy jednoczesnym zapewnieniu, aby działania te pozostały odpowiednio nieinwazyjne.

(14) Ochrona tajemnic przedsiębiorstwa przed tymi podatnościami ma zasadnicze znaczenie dla utrzymania pozycji rynkowej i przewagi konkurencyjnej przemysłu europejskiego. Chociaż posiadacze danych mogą korzystać ze swobody uznania w zakresie ochrony swoich tajemnic przedsiębiorstwa, odmowy dzielenia się danymi powinny być ograniczone do uzasadnionych, wyjątkowych okoliczności, aby zachować cele rozporządzenia (UE) 2023/2854 polegające na wspieraniu innowacji opartych na danych i dobrze prosperującej gospodarki cyfrowej w Unii. Należy utrzymać zabezpieczenia przed nadużywaniem mechanizmu odmowy, w tym spoczywający na posiadaczu danych obowiązek wykazania w należycie uzasadniony sposób, że ujawnienie stwarza wysokie ryzyko, oraz obowiązek powiadomienia właściwych organów. Takie wykazane informacje należy przekazać użytkownikowi lub osobie trzeciej na piśmie bez zbędnej zwłoki i powinny być one proporcjonalne do danej sprawy. Wszystkie zaangażowane strony powinny traktować decyzję i towarzyszące jej wykazane informacje jako poufne, aby zachować poufny charakter przedmiotowych tajemnic przedsiębiorstwa. Użytkownicy i osoby trzecie, w zależności od przypadku, mogą zaskarżyć decyzję posiadacza danych do właściwego organu, do sądu lub za pośrednictwem organów rozstrzygających spory.

(15) Aby uprościć ramy dzielenia się danymi między przedsiębiorstwami a organami administracji na podstawie rozporządzenia (UE) 2023/2854 oraz wyjaśnić niejasności, które wcześniej skutkowały nakładaniem na przedsiębiorstwa szerszych obowiązków, konieczne jest zawężenie zakresu rozdziału V tego rozporządzenia z „wyjątkowej potrzeby” do „niebezpieczeństwa publicznego”. Pojęcie „niebezpieczeństwa publicznego”, zdefiniowane w art. 2 pkt 29 rozporządzenia (UE) 2023/2854, zapewnia

zatem, aby na obowiązki określone w tym rozdziale powoływano się wyłącznie w ściśle określonych, pilnych sytuacjach, ograniczając wyzwania techniczne, administracyjne i prawne, których doświadczyły przedsiębiorstwa w ramach poprzedniego systemu. Zapewni to, aby wnioski o dane były odpowiednie i proporcjonalne do reagowania na niebezpieczeństwo publiczne, łagodzenia jego skutków lub wspierania przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego. Ponieważ zaktualizowane unijne ramy dotyczące statystyki europejskiej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 223/2009[31] nie odnoszą się do niebezpieczeństwa publicznego, konieczne jest zachowanie roli statystyki publicznej na podstawie rozdziału V rozporządzenia (UE) 2023/2854 w celu zapewnienia jasności i skuteczności w takich sytuacjach. Konieczne jest również doprecyzowanie systemu rekompensat w sytuacjach, w których mikroprzedsiębiorstwa i małe przedsiębiorstwa są zobowiązane do przekazywania danych w celu zareagowania na niebezpieczeństwo publiczne, w którym to przypadku takie przedsiębiorstwa mogą domagać się rekompensaty.

(16) Aby ograniczyć niepewność prawa, która mogłaby zniechęcać do stosowania innowacyjnych modeli biznesowych, konieczne jest wyeliminowanie istotnych niejasności i obciążeń związanych z przestrzeganiem przepisów dotyczących inteligentnych umów na potrzeby wykonywania umów w sprawie dzielenia się danymi na podstawie art. 36 rozporządzenia (UE) 2023/2854. Brak norm zharmonizowanych i jasnych definicji kluczowych pojęć, takich jak „odporność", „kontrola dostępu" i „spójność z warunkami umownymi", w połączeniu z wymogiem dotyczącym „mechanizmu bezpiecznego zakończenia lub przerwania", potencjalnie niezgodnym ze zdecentralizowanymi lub publicznymi architekturami łańcucha bloków opartymi na niezmiennych rejestrach, stanowił wyzwanie dla innowatorów z perspektywy kosztów i możliwości. Ponadto niejednoznaczność związana z przeprowadzaniem oceny zgodności na podstawie art. 36 ust. 2 tego rozporządzenia grozi nałożeniem nieproporcjonalnych obciążeń. Usunięcie art. 36 rozporządzenia (UE) 2023/2854 promowałoby zatem rozwój i wprowadzanie na rynek nowych modeli biznesowych, wspierałoby innowacje oraz zmniejszałoby bariery dla powstających technologii.

(17) Niektóre usługi przetwarzania danych, które nie wchodzą w zakres modelu świadczenia infrastruktury jako usługi (IaaS), są wykonywane na zamówienie z dostosowaniem do potrzeb lub ekosystemu klienta. Świadczenie takich usług przetwarzania danych opiera się na czasochłonnych negocjacjach poprzedzających zawarcie umowy i negocjacjach umownych w celu określenia szczególnych wymogów klienta oraz wynikających z nich prac technicznych na rzecz dostosowania usługi przetwarzania danych i dostarczenia rozwiązania dostosowanego do potrzeb. Są to usługi, które nie są dostępne od ręki i które są spersonalizowane na podstawie potrzeb

---

[31] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich (Dz.U. L 87 z 31.3.2009, s. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

klienta w celu zapewnienia dostosowanego rozwiązania, w przypadku gdy większość cech i funkcji usługi przetwarzania danych jest dostosowana przez dostawcę do konkretnych potrzeb klienta i w przypadku gdy większość cech i funkcji nie byłaby możliwa do wykorzystania przez klienta bez uprzedniego dostosowania przez dostawcę. Usługi te różnią się od usług przetwarzania danych opracowanych na zamówienie, o których mowa w art. 31 ust. 1 rozporządzenia (UE) 2023/2854. Usługi przetwarzania danych opracowane na zamówienie to usługi, w przypadku których większość głównych cech została opracowana na zamówienie, tak aby dostosować je do konkretnych potrzeb indywidualnego klienta, lub w przypadku których te usługi przetwarzania danych nie są oferowane komercyjnie na szeroką skalę poprzez katalog usług dostawcy. Aby uniknąć dodatkowych kosztów i obciążeń administracyjnych związanych z koniecznością ponownego otwarcia i renegocjacji umów zawartych przed 12 września 2025 r. lub w tym dniu, należy wyjaśnić, że – z wyjątkiem obowiązku obniżenia i ostatecznego zniesienia opłat z tytułu zmiany dostawcy i opłat z tytułu wychodzącego ruchu danych – usługi opracowane na zamówienie świadczone zgodnie z umowami zawartymi przed 12 września 2025 r. lub w tym dniu nie powinny być objęte zakresem rozdziału VI rozporządzenia (UE) 2023/2854.

(18) Ze względów związanych z planowaniem finansowym i przyciąganiem inwestycji dostawcy usług przetwarzania danych, zwłaszcza MŚP i małe spółki o średniej kapitalizacji, mogą preferować i oferować umowy na czas określony. Należy wyjaśnić, że dostawcy usług przetwarzania danych mogą zawrzeć w tych umowach przepisy dotyczące proporcjonalnych kar za wcześniejsze rozwiązanie umowy, o ile nie stanowią one przeszkody dla zmiany dostawcy. Ponadto dostawcy usług przetwarzania danych będący MŚP lub małymi spółkami o średniej kapitalizacji są szczególnie obciążeni koniecznością dostosowania istniejących umów o świadczenie usług przetwarzania danych do rozporządzenia (UE) 2023/2854. Konieczne jest zatem ustanowienie szczegółowych uregulowań dla tych dostawców, jeżeli świadczą usługi przetwarzania danych inne niż IaaS na podstawie umów zawartych przed dniem 12 września 2025 r. lub w tym dniu. Biorąc pod uwagę cel rozporządzenia (UE) 2023/2854, jakim jest umożliwienie zmiany dostawcy usług przetwarzania danych, oraz biorąc pod uwagę, że opłaty z tytułu zmiany dostawcy, w tym opłaty z tytułu wychodzącego ruchu danych, stanowią poważną przeszkodę w zmianie dostawcy, nowe, łagodniejsze systemy w odniesieniu do usług przetwarzania danych, które są wykonywane na zamówienie lub są świadczone przez MŚP lub małe spółki o średniej kapitalizacji, nie powinny utrudniać stopniowego wycofywania tych opłat. Należy uznać, że postanowienia umowne sprzeczne z tym celem nigdy nie istniały, jeżeli są one zawarte w porozumieniach umownych dotyczących świadczenia usług objętych zakresem stosowania tych dwóch nowych szczegółowych uregulowań.

(19) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1807[32] wprowadzono kluczową zasadę wspierania w Unii gospodarki opartej na danych, stanowiącą konkretną podstawę swobody przedsiębiorczości i swobody świadczenia usług.

---

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.U. L 303 z 28.11.2018, s. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

„Swobodny przepływ danych” w Unii, doprecyzowany za pomocą zakazu narzucania lokalizacji danych, pozostaje podstawową zasadą zapewniającą przedsiębiorstwom pewność prawa i należy go utrzymać w rozporządzeniu (UE) 2023/2854. Przepis ten nie ma wpływu na przetwarzanie danych w zakresie, w jakim odbywa się ono w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności w odniesieniu do bezpieczeństwa narodowego, zgodnie z art. 4 Traktatu o Unii Europejskiej. Jednocześnie inne przepisy rozporządzenia (UE) 2018/1807 zastępuje się nowszymi przepisami. W szczególności w rozdziale VI rozporządzenia (UE) 2023/2854 wprowadzono nowoczesne horyzontalne ramy prawne dotyczące zmiany dostawcy usług przetwarzania danych i praktycznie zdezaktualizowano art. 6 rozporządzenia (UE) 2018/1807. Współistnienie tych przepisów zwiększyło złożoność prawną dla przedsiębiorstw. Należy zatem uchylić rozporządzenie (UE) 2018/1807.

(20) Pojęcie „bezpieczeństwa publicznego” w rozumieniu art. 52 TFUE i zgodnie z wykładnią Trybunału Sprawiedliwości obejmuje zarówno bezpieczeństwo wewnętrzne, jak i zewnętrzne danego państwa członkowskiego, a także kwestie ochrony publicznej, w szczególności w celu ułatwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw. Zakłada ono istnienie rzeczywistego i wystarczająco poważnego zagrożenia dla jednego z podstawowych interesów społecznych, takiego jak zagrożenie dla funkcjonowania instytucji i podstawowych usług publicznych oraz życia ludności, a także ryzyko poważnego zakłócenia stosunków zagranicznych lub pokojowego współistnienia narodów, lub zagrożenie dla interesów wojskowych. Zgodnie z zasadą proporcjonalności wymogi dotyczące lokalizacji danych, które uzasadnione są względami bezpieczeństwa publicznego, powinny być odpowiednie do zamierzonego celu oraz nie powinny wykraczać poza to, co jest niezbędne do realizacji tego celu.

(21) Zarówno dyrektywa (UE) 2019/1024, jak i rozdział II rozporządzenia (UE) 2022/868 regulują ponowne wykorzystywanie informacji sektora publicznego do celów innowacji. Wzajemne zależności między tymi dwoma zbiorami przepisów doprowadziły do braku pewności prawa, głównie dla organów sektora publicznego. Konieczne jest zatem dostosowanie przepisów w ramach jednego instrumentu prawnego, aby zapewnić większą spójność i pewność prawa.

(22) Z uwagi na fakt, że zarówno dyrektywa (UE) 2019/1024, jak i rozporządzenie (UE) 2022/868 mają wspólny cel, tj. usprawnienie ponownego wykorzystywania informacji sektora publicznego, a także w celu uproszczenia przepisów zarówno z punktu widzenia organów sektora publicznego, jak i ponownych użytkowników informacji sektora publicznego, uzasadnione jest uchylenie dyrektywy (UE) 2019/1024 i rozporządzenia (UE) 2022/868 oraz dostosowanie dwóch systemów i skonsolidowanie przepisów w jednym rozdziale w ramach niniejszego rozporządzenia. Rozwiązanie to zwiększy harmonizację tych przepisów w całej Unii, zmniejszy obciążenia administracyjne związane z interpretacją i wdrażaniem przepisów krajowych oraz ułatwi przedsiębiorstwom rozwój transgranicznych usług i produktów. Wyznaczając właściwe organy, państwa członkowskie powinny zapewnić, aby nawet w przypadku wyznaczenia właściwych organów sektorowych ostatecznie uwzględniono wszystkie odpowiednie sektory. Należy rozumieć, że zmiany w niniejszym rozporządzeniu nie zmieniają interpretacji poszczególnych definicji i terminów, chyba że wyraźnie to wskazano.

(23) Dane i dokumenty, które można publicznie udostępnić do ponownego wykorzystywania, oraz dane i dokumenty, które są chronione ze względu na poufność informacji handlowych, w tym tajemnicę handlową, tajemnicę zawodową i tajemnicę

przedsiębiorstwa, poufność informacji statystycznych, ochronę praw własności intelektualnej osób trzecich lub ochronę danych osobowych, często znajdują się w posiadaniu tych samych organów sektora publicznego. W związku z tym konieczne jest dostosowanie definicji i wspólnych zasad mających zastosowanie do wszystkich informacji sektora publicznego oraz zajęcie się kwestiami dotyczącymi wzajemnych zależności między dwoma zbiorami przepisów.

(24) Należy usprawnić obowiązujące przepisy, aby zwiększyć ich jasność i spójność. Oba systemy ponownego wykorzystywania powinny jednak pozostać odrębne, a ich odpowiedni zakres stosowania powinien nadal zależeć od cech danych lub dokumentów oraz kontekstu ich ponownego wykorzystywania. Organy sektora publicznego powinny w miarę możliwości stosować system otwartych danych. Jedynie w przypadku gdy stwierdzą, że dane lub dokument zawierają informacje odpowiadające niektórym kategoriom danych chronionych, powinny ograniczyć ich publiczną dostępność i rozważyć udostępnienie ich do ponownego wykorzystywania jako danych chronionych.

(25) Przedsiębiorstwom typu start-up, małym przedsiębiorstwom i przedsiębiorstwom, które kwalifikują się jako średnie przedsiębiorstwa zgodnie z art. 2 załącznika do zalecenia Komisji 2003/361/WE[33], oraz przedsiębiorstwom z sektorów o mniej rozwiniętych zdolnościach cyfrowych trudno jest wykorzystywać ponownie dane i dokumenty. Ponadto pojawiło się kilka bardzo dużych podmiotów posiadających znaczną siłę gospodarczą w gospodarce cyfrowej dzięki koncentracji i agregacji wielkich ilości danych oraz dzięki infrastrukturze technicznej pozwalającej na czerpanie z nich korzyści finansowych. Te bardzo duże przedsiębiorstwa obejmują przedsiębiorstwa, które świadczą podstawowe usługi platformowe i zostały wskazane jako strażnicy dostępu na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925[34] oraz podlegają szczególnym obowiązkom w zakresie eliminowania zakłóceń równowagi. Aby zaradzić tym zakłóceniom równowagi oraz wzmocnić konkurencję i innowacje, organy sektora publicznego powinny mieć możliwość wprowadzenia specjalnych warunków w licencjach dotyczących ponownego wykorzystywania danych i dokumentów przez bardzo duże przedsiębiorstwa. Wszelkie takie warunki powinny być proporcjonalne, oparte na obiektywnych kryteriach, z uwzględnieniem siły gospodarczej, zdolności podmiotu do pozyskiwania danych lub wyznaczenia jako strażnika dostępu na podstawie rozporządzenia (UE) 2022/1925, a w stosownych przypadkach – innych takich kryteriów. Takie specjalne warunki mogą dotyczyć między innymi opłat i należności lub celów ponownego wykorzystywania.

(26) W duchu wspierania innowacji i utrzymania uczciwej konkurencji na unijnym rynku cyfrowym konieczne jest zapewnienie, aby dostęp do danych sektora publicznego i ich

---

[33] Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. L 265 z 12.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

ponowne wykorzystywanie przynosiły korzyści szerokiemu gronu uczestników rynku i nie wzmacniały w sposób niezamierzony istniejących pozycji dominujących. Bardzo duże przedsiębiorstwa, a w szczególności przedsiębiorstwa wskazane jako strażnicy dostępu na podstawie rozporządzenia (UE) 2022/1925, charakteryzują się znaczącą pozycją i wpływem na rynek wewnętrzny. Aby uniemożliwić takim podmiotom wykorzystanie ich istotnych środków ze szkodą dla uczciwej konkurencji i innowacji, organy sektora publicznego powinny mieć możliwość ustalania wyższych opłat za ponowne wykorzystywanie otwartych danych publicznych i danych chronionych. Takie wyższe opłaty i należności powinny być proporcjonalne i oparte na obiektywnych kryteriach, z uwzględnieniem siły gospodarczej i zdolności podmiotu do pozyskiwania danych. Środek ten służy zabezpieczeniu możliwości wprowadzania innowacji i konkurowania w gospodarce cyfrowej przez mniejsze przedsiębiorstwa i nowe podmioty wchodzące na rynek.

(27) W niniejszym rozporządzeniu proponuje się szereg ukierunkowanych zmian w rozporządzeniu (UE) 2016/679 z myślą o jego doprecyzowaniu i uproszczeniu, przy jednoczesnym zachowaniu tego samego poziomu ochrony danych. Art. 4 rozporządzenia (UE) 2016/679 stanowi, że dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy daną osobę fizyczną można zidentyfikować, należy wziąć pod uwagę wszelkie sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Biorąc pod uwagę orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej dotyczące definicji danych osobowych, konieczne jest doprecyzowanie, kiedy osobę fizyczną należy uznać za możliwą do zidentyfikowania. Istnienie dodatkowych informacji umożliwiających identyfikację osoby, której dane dotyczą, nie oznacza samo w sobie, że do celów stosowania rozporządzenia (UE) 2016/679 dane pseudonimizowane należy uznać za dane osobowe we wszystkich przypadkach i w odniesieniu do każdej osoby lub podmiotu. W szczególności należy wyjaśnić, że informacji nie należy uznawać za dane osobowe w odniesieniu do danego podmiotu, jeżeli podmiot ten nie dysponuje sposobami, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane do zidentyfikowania osoby fizycznej, której informacje te dotyczą. Ewentualne późniejsze przekazanie tych informacji osobom trzecim, które dysponują uzasadnionymi sposobami pozwalającymi im zidentyfikować osobę fizyczną, której informacje te dotyczą, takimi jak porównanie z innymi posiadanymi przez nie danymi, sprawia, że informacje te stają się danymi osobowymi wyłącznie dla tych osób trzecich, które dysponują takimi sposobami. Podmiot, dla którego informacje nie są danymi osobowymi, co do zasady nie jest objęty zakresem stosowania rozporządzenia (UE) 2016/679. W tym względzie Trybunał Sprawiedliwości Unii Europejskiej orzekł, że dany sposób nie może zostać z uzasadnionym prawdopodobieństwem zastosowany do zidentyfikowania osoby, której dane dotyczą, gdy ryzyko jej identyfikacji wydaje się w rzeczywistości znikome z uwagi na fakt, że identyfikacja tej osoby jest zakazana prawem lub niewykonalna w praktyce, przykładowo z powodu nadmiernego nakładu czasu, kosztów i pracy. Przykład zakazu deanonimizacji można znaleźć w

obowiązkach użytkowników danych dotyczących zdrowia określonych w art. 61 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/327[35]. Komisja, wraz z Europejską Radą Ochrony Danych, powinna wspierać administratorów w stosowaniu tej zaktualizowanej definicji w drodze określenia kryteriów technicznych w akcie wykonawczym.

(28) Aby ocenić, czy badania spełniają warunki badań naukowych do celów niniejszego rozporządzenia, można wziąć pod uwagę takie elementy jak metodyczne i systematyczne podejście stosowane podczas prowadzenia badań w danej dziedzinie. Badania naukowe i rozwój technologii należy prowadzić w środowisku akademickim, przemysłowym i innym, w tym w małych i średnich przedsiębiorstwach (art. 179 ust. 2 TFUE), oraz powinny zawsze charakteryzować się wysoką jakością i być zgodne z zasadami wiarygodności, uczciwości, szacunku i odpowiedzialności (weryfikowalność).

(29) Należy powtórzyć, że dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych powinno być uznawane za operacje przetwarzania zgodne z prawem i z pierwotnymi celami. W takich przypadkach nie jest konieczne ustalenie na podstawie art. 6 ust. 4 niniejszego rozporządzenia, czy cel dalszego przetwarzania jest zgodny z celem, w którym dane osobowe zostały pierwotnie zebrane.

(30) Godna zaufania AI ma kluczowe znaczenie dla zapewnienia wzrostu gospodarczego i wspierania innowacji przynoszących korzyści społeczne. Opracowywanie i wykorzystywanie systemów AI i modeli podstawowych, takich jak duże modele językowe i modele generatywnych treści wideo, opiera się na danych, w tym danych osobowych, na różnych etapach cyklu życia AI, takich jak etap trenowania, testowania i walidacji, które w niektórych przypadkach mogą zostać zachowane w systemie AI lub modelu AI. Przetwarzanie danych osobowych w tym kontekście może zatem w stosownych przypadkach odbywać się w celach wynikających z prawnie uzasadnionego interesu w rozumieniu art. 6 rozporządzenia (UE) 2016/679. Nie ma to wpływu na spoczywający na administratorze obowiązek zapewnienia, aby rozwój lub wykorzystywanie (wdrażanie) AI w konkretnym kontekście lub do konkretnych celów były zgodne z innymi przepisami prawa Unii lub prawa krajowego, lub obowiązek zapewnienia zgodności, w przypadku gdy jej wykorzystanie jest wyraźnie zabronione prawem. Nie ma to również wpływu na obowiązek zapewnienia, by spełniono wszystkie pozostałe warunki określone w art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679, a także wszystkie inne wymogi i zasady tego rozporządzenia.

(31) Jeżeli administrator, w świetle podejścia opartego na analizie ryzyka, które uwzględnia skalowalność obowiązków wynikających z niniejszego rozporządzenia, równoważy prawnie uzasadniony interes realizowany przez administratora lub stronę trzecią oraz interesy, prawa i wolności osoby, której dane dotyczą, należy rozważyć, czy interes realizowany przez administratora jest korzystny dla osoby, której dane

---

[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (Dz.U. L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)

dotyczą, i ogółu społeczeństwa, co może mieć miejsce na przykład w przypadku, gdy przetwarzanie danych osobowych jest niezbędne do wykrywania i usuwania stronniczości, a tym samym ochrony osób, których dane dotyczą, przed dyskryminacją, lub gdy przetwarzanie danych osobowych ma na celu zapewnienie dokładnych i bezpiecznych wyników dla dobrego wykorzystania, np. w celu poprawy dostępności niektórych usług. Należy również wziąć pod uwagę m.in. uzasadnione oczekiwania osoby, której dane dotyczą, oparte na jej powiązaniach z administratorem, odpowiednie zabezpieczenia w celu zminimalizowania wpływu na prawa osób, których dane dotyczą, takie jak zapewnienie większej przejrzystości osobom, których dane dotyczą, zapewnienie bezwarunkowego prawa sprzeciwu wobec przetwarzania ich danych osobowych, poszanowanie wskazań technicznych wbudowanych w usługę ograniczających wykorzystanie danych do rozwoju AI przez osoby trzecie, wykorzystanie innych najnowocześniejszych technik ochrony prywatności na potrzeby trenowania AI oraz odpowiednie środki techniczne w celu skutecznego zminimalizowania ryzyka wynikającego na przykład z zawracania, wycieku danych i innych zamierzonych lub przewidywalnych działań.

(32) Przetwarzanie danych osobowych do celów badań naukowych i stosowanie przepisów RODO dotyczących badań naukowych jest uzależnione od przyjęcia odpowiednich zabezpieczeń dla praw i wolności osób, których dane dotyczą, zgodnie z art. 89 ust. 1 RODO. W tym celu RODO równoważy prawo do ochrony danych osobowych zgodnie z art. 8 Karty praw podstawowych Unii Europejskiej z wolnością nauki zgodnie z art. 13 Karty praw podstawowych Unii Europejskiej. Przetwarzanie danych osobowych do celów badań naukowych służy zatem realizacji prawnie uzasadnionego interesu w rozumieniu art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679, pod warunkiem że takie badania nie są sprzeczne z prawem Unii lub prawem państwa członkowskiego. Pozostaje to bez uszczerbku dla spoczywającego na administratorze obowiązku zapewnienia spełnienia wszystkich pozostałych warunków określonych w art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679, a także wszystkich innych wymogów i zasad tego rozporządzenia.

(33) Rozwój niektórych systemów AI i modeli AI może wiązać się z gromadzeniem dużych ilości danych, w tym danych osobowych i ich szczególnych kategorii. Szczególne kategorie danych osobowych mogą rezydualnie istnieć w zbiorach danych do celów trenowania, testowania i walidacji lub mogą być zatrzymywane w systemie AI lub modelu AI, chociaż szczególne kategorie danych osobowych nie są niezbędne do celów przetwarzania. Aby nie utrudniać w nieproporcjonalny sposób rozwoju i eksploatacji AI oraz biorąc pod uwagę zdolności administratora do identyfikowania i usuwania szczególnych kategorii danych osobowych, należy zezwolić na odstępstwo od zakazu przetwarzania szczególnych kategorii danych osobowych na podstawie art. 9 ust. 2 rozporządzenia (UE) 2016/679. Odstępstwo to powinno mieć zastosowanie wyłącznie w przypadku, gdy administrator skutecznie wdrożył odpowiednie środki techniczne i organizacyjne, aby uniknąć przetwarzania tych danych, wprowadził odpowiednie środki w całym cyklu życia systemu AI lub modelu AI oraz, po zidentyfikowaniu takich danych, skutecznie je usunął. Jeżeli usunięcie danych wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku gdy usunięcie szczególnych kategorii danych zapamiętanych w systemie AI lub modelu AI wymagałoby przeprojektowania systemu AI lub modelu AI, administrator powinien skutecznie chronić takie dane przed wykorzystaniem ich do wywnioskowania wyników, ich ujawnieniem lub udostępnieniem w inny sposób osobom trzecim. Odstępstwo to nie powinno mieć zastosowania w przypadku, gdy przetwarzanie szczególnych kategorii danych osobowych jest niezbędne do celów przetwarzania. W

takim przypadku administrator powinien powołać się na odstępstwa na podstawie art. 9 ust. 2 lit. a)–j) rozporządzenia (UE) 2016/679.

(34) Dane biometryczne zdefiniowane w art. 4 pkt 14 rozporządzenia (UE) 2016/679 oznaczają przetwarzanie określonych cech osoby fizycznej za pomocą specjalnych środków technicznych, umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby. Pojęcie danych biometrycznych obejmuje dwie odrębne funkcje, a mianowicie identyfikację osoby fizycznej lub weryfikację (zwaną również uwierzytelnianiem) jej deklarowanej tożsamości, które opierają się na różnych procesach technicznych. Proces identyfikacji opiera się na wyszukiwaniu „jeden do wielu" danych biometrycznych osoby, której dane dotyczą, w bazie danych, natomiast proces weryfikacji opiera się na porównaniu „jeden do jednego" danych biometrycznych dostarczonych przez osobę, której dane dotyczą, która tym samym deklaruje swoją tożsamość. Odstępstwa od zakazu przetwarzania danych biometrycznych na mocy art. 9 ust. 1 rozporządzenia powinny być również dozwolone w przypadku, gdy weryfikacja deklarowanej tożsamości osoby, której dane dotyczą, jest niezbędna do celu realizowanego przez administratora oraz gdy zastosowanie mają odpowiednie zabezpieczenia umożliwiające osobie, której dane dotyczą, sprawowanie wyłącznej kontroli nad procesem weryfikacji. Na przykład jeżeli dane biometryczne są bezpiecznie przechowywane wyłącznie po stronie osoby, której dane dotyczą, lub są bezpiecznie przechowywane po stronie administratora w najnowocześniejszej zaszyfrowanej formie, a klucz kryptograficzny lub równoważne środki są w posiadaniu wyłącznie osoby, której dane dotyczą, przetwarzanie to prawdopodobnie nie stwarza poważnego ryzyka dla jej podstawowych praw i wolności. Administrator nie uzyskuje wiedzy na temat danych biometrycznych lub uzyskuje ją jedynie przez bardzo ograniczony czas w trakcie procesu weryfikacji.

(35) W art. 15 rozporządzenia (UE) 2016/679 przewidziano, że osoby, których dane dotyczą, są uprawnione do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe ich dotyczące, a jeżeli ma to miejsce, są uprawnione do uzyskania dostępu do danych osobowych i pewnych informacji dodatkowych. Prawo dostępu powinno umożliwiać osobie, której dane dotyczą, uzyskanie wiedzy na temat zgodności przetwarzania z prawem i zweryfikowania tej zgodności oraz korzystanie z innych praw przysługujących jej na mocy rozporządzenia (UE) 2016/679. Natomiast w art. 12 rozporządzenia należy wyjaśnić, że prawa dostępu, które od samego początku jest korzystne dla osób, których dane dotyczą, nie należy nadużywać, w takim sensie, że osoby, których dane dotyczą, nadużywałyby go do celów innych niż ochrona ich danych. Takie nadużycie prawa dostępu miałoby miejsce na przykład wtedy, gdy osoba, której dane dotyczą, zamierza spowodować odrzucenie przez administratora żądania dostępu, aby następnie ubiegać się o wypłatę odszkodowania, potencjalnie pod groźbą wystąpienia z roszczeniem odszkodowawczym. Inne przykłady nadużyć obejmują sytuacje, w których osoby, których dane dotyczą, nadmiernie korzystają z prawa dostępu wyłącznie z zamiarem wyrządzenia szkody administratorowi lub gdy osoba fizyczna występuje z żądaniem, ale jednocześnie proponuje wycofanie go w zamian za pewną formę korzyści od administratora. Ponadto, aby w rozsądnym zakresie ograniczyć obciążenie, na administratorach powinien spoczywać mniejszy ciężar dowodu w odniesieniu do nadmiernego charakteru żądania niż w odniesieniu do ewidentnie nieuzasadnionego charakteru żądania. Wynika to z tego, że ewidentnie nieuzasadniony charakter żądania zależy od faktów, które zasadniczo leżą w sferze odpowiedzialności administratora, natomiast nadmierny charakter żądania odnosi się do zachowania osoby, której dane dotyczą, potencjalnie stanowiącego nadużycie, które zasadniczo znajduje się poza sferą

wpływu administratora, w związku z czym administrator może być w stanie udowodnić takie nadużycie jedynie w rozsądnym stopniu. W każdym przypadku, żądając dostępu na podstawie art. 15 rozporządzenia (UE) 2016/679, osoba, której dane dotyczą, powinna być jak najbardziej konkretna. Żądania o zbyt szerokim i niezróżnicowanym zakresie również należy uznać za nadmierne.

(36) W art. 13 rozporządzenia (UE) 2016/679 administratora danych zobowiązano do udzielenia osobie, której dane dotyczą, pewnych informacji na temat przetwarzania jej danych osobowych, a także pewnych dalszych informacji niezbędnych do zapewnienia rzetelności i przejrzystości przetwarzania, jak określono w ust. 1, 2 i 3 tego przepisu. Zgodnie z art. 13 ust. 4 rozporządzenia (UE) 2016/679 obowiązek ten nie ma zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami. Aby jeszcze bardziej zmniejszyć obciążenie administratorów danych, bez uszczerbku dla możliwości wykonywania przez osobę, której dane dotyczą, praw przysługujących jej na mocy rozdziału III rozporządzenia, odstępstwo to należy rozszerzyć na sytuacje, w których przetwarzanie prawdopodobnie nie spowoduje wysokiego ryzyka w rozumieniu art. 35 rozporządzenia oraz istnieją uzasadnione podstawy, by przypuszczać, że osoba, której dane dotyczą, posiada już informacje, o których mowa w ust. 1 lit. a) i c), z uwzględnieniem kontekstu, w którym dane osobowe zostały zebrane, w szczególności w odniesieniu do powiązania między osobami, których dane dotyczą, a administratorem. Powinny to być sytuacje, w których kontekst powiązania między administratorem a osobą, której dane dotyczą, jest bardzo jasny i ograniczony, a działalność administratora nie wymaga intensywnego przetwarzania danych, jak na przykład w przypadku powiązania między rzemieślnikiem a jego klientami, w ramach którego zakres przetwarzania jest ograniczony do minimum danych niezbędnych do świadczenia usługi. Działalność administratora nie wymaga intensywnego przetwarzania danych, jeżeli gromadzi on niewielką ilość danych osobowych, a jego operacje przetwarzania nie są złożone, co nie ma miejsca na przykład w dziedzinie zatrudnienia. W takich okolicznościach, tj. gdy przetwarzanie nie jest intensywne i nie jest złożone oraz gdy administrator gromadzi niewielką ilość danych osobowych, należy racjonalnie oczekiwać na przykład, że osoba, której dane dotyczą, posiada informacje na temat tożsamości i danych kontaktowych administratora, a także na temat celu przetwarzania, gdy przetwarzanie to odbywa się na potrzeby wykonania umowy, której stroną jest osoba, której dane dotyczą, lub gdy osoba, której dane dotyczą, wyraziła zgodę na to przetwarzanie, zgodnie z wymogami określonymi w rozporządzeniu (UE) 2016/679. To samo powinno mieć zastosowanie do stowarzyszeń i klubów sportowych, w których przetwarzanie danych osobowych ogranicza się do zarządzania członkostwem, komunikacji z członkami i organizacji działalności. Niemniej jednak to odstępstwo od obowiązków określonych w art. 13 pozostaje bez uszczerbku dla niezależnych obowiązków administratora wynikających z art. 15 tego rozporządzenia, który ma zastosowanie w przypadku, gdy osoba, której dane dotyczą, żąda dostępu na podstawie tego ostatniego przepisu. W przypadku gdy odstępstwo od obowiązków określonych w art. 13 nie ma zastosowania, aby zrównoważyć potrzebę kompletności i łatwego zrozumienia przez osobę, której dane dotyczą, administratorzy mogą przyjąć podejście warstwowe przy dostarczaniu żądanych informacji, w szczególności umożliwiając użytkownikom przechodzenie do dalszych informacji.

(37) Jeżeli przetwarzanie odbywa się do celów badań naukowych, a udzielenie informacji osobie, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, udzielenie informacji przewidzianych w art. 13 niniejszego rozporządzenia nie powinno być konieczne. Administrator powinien dołożyć

należytych starań, aby uzyskać dane kontaktowe, jeżeli są one łatwo dostępne, a ich pozyskanie nie wymagałoby niewspółmiernie dużego wysiłku. Udzielenie informacji wymagałoby niewspółmiernie dużego wysiłku w szczególności, gdy administrator w momencie gromadzenia danych osobowych nie wiedział ani nie przewidywał, że będzie przetwarzał dane osobowe do celów badań naukowych na późniejszym etapie, w którym to przypadku może nie mieć łatwo dostępnych danych kontaktowych osób, których dane dotyczą. W takich sytuacjach administrator powinien pośrednio poinformować osoby, których dane dotyczą, np. przez podanie informacji do wiadomości publicznej. Udzielenie takich informacji powinno zapewnić dotarcie do jak największej liczby zainteresowanych osób, których dane dotyczą. Odpowiednie środki publicznego udostępniania informacji należy określić w zależności od kontekstu projektu badawczego i zaangażowanych osób, których dane dotyczą.

(38) Art. 22 rozporządzenia (UE) 2016/679 zawiera przepisy regulujące przetwarzanie danych osobowych, w przypadku gdy administrator danych podejmuje decyzje mające skutki prawne lub podobnie istotne skutki dla osoby, której dane dotyczą, oparte wyłącznie na zautomatyzowanym przetwarzaniu. W celu zapewnienia większej pewności prawa należy wyjaśnić, że decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu są dozwolone, jeżeli spełniono szczególne warunki, jak określono w rozporządzeniu (UE) 2016/679. Należy również wyjaśnić, że przy ocenie, czy decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, jak określono w art. 22 ust. 2 lit. a) rozporządzenia (UE) 2016/679, nie należy wymagać, aby decyzję można było podjąć tylko w drodze wyłącznie zautomatyzowanego przetwarzania. Oznacza to, że fakt, iż decyzję może podjąć również człowiek, nie uniemożliwia administratorowi podjęcia decyzji w drodze wyłącznie zautomatyzowanego przetwarzania. Jeżeli istnieje kilka równie skutecznych rozwiązań w zakresie zautomatyzowanego przetwarzania, administrator powinien zastosować mniej inwazyjne rozwiązanie.

(39) Aby zmniejszyć obciążenie administratorów, a jednocześnie zapewnić organom nadzorczym dostęp do odpowiednich informacji i możliwość podejmowania działań w związku z naruszeniami rozporządzenia, próg powodujący obowiązek zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu na podstawie art. 33 rozporządzenia (UE) 2016/679 należy dostosować do progu powodującego obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych na podstawie art. 34 tego rozporządzenia. W przypadku naruszenia ochrony danych, które prawdopodobnie nie spowoduje wysokiego ryzyka naruszenia praw i wolności osób fizycznych, administrator nie powinien być zobowiązany do zgłaszania naruszenia właściwemu organowi nadzorczemu. Wyższy próg powodujący obowiązek zgłoszenia naruszenia ochrony danych organowi nadzorczemu nie ma wpływu na spoczywający na administratorze obowiązek udokumentowania naruszenia zgodnie z art. 33 ust. 5 rozporządzenia (UE) 2016/679 ani na spoczywający na nim obowiązek wykazania przestrzegania tego rozporządzenia, zgodnie z jego art. 5 ust. 2. Aby ułatwić administratorom przestrzeganie przepisów i zharmonizowane podejście w Unii, Europejska Rada Ochrony Danych powinna przygotować wspólny wzór zgłaszania naruszeń ochrony danych właściwemu organowi nadzorczemu oraz wspólny wykaz okoliczności, w których naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej. Komisja powinna należycie uwzględnić wniosek przygotowany przez Radę i, w razie potrzeby, dokonać jego przeglądu przed przyjęciem. Aby uwzględnić nowe zagrożenia dla bezpieczeństwa informacji, wspólny wzór i wykaz należy poddawać przeglądowi co najmniej raz na trzy lata i w razie potrzeby aktualizować. Brak wspólnego wykazu

okoliczności, w których naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej, nie powinien wpływać na obowiązki administratorów w zakresie zgłaszania tych naruszeń.

(40) W art. 35 tego rozporządzenia (UE) 2016/679 zobowiązano administratorów do przeprowadzenia oceny skutków dla ochrony danych, jeżeli przetwarzanie danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Od organów nadzorczych utworzonych zgodnie z tym rozporządzeniem wymaga się ustanowienia i podania do publicznej wiadomości wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Ponadto w rozporządzeniu przewidziano, że organy nadzorcze mogą ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Aby skutecznie przyczynić się do osiągnięcia celu konwergencji gospodarek i skutecznie zapewnić swobodny przepływ danych osobowych między państwami członkowskimi, zwiększyć pewność prawa, ułatwić administratorom przestrzeganie przepisów i zapewnić zharmonizowaną interpretację pojęcia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą, należy ustanowić jednolity wykaz operacji przetwarzania na szczeblu UE, który zastąpi istniejące wykazy krajowe. Ponadto należy wprowadzić obowiązek publikowania wykazu rodzajów operacji przetwarzania, w przypadku których nie jest wymagana ocena skutków dla ochrony danych, co obecnie ma charakter opcjonalny. Wykazy operacji przetwarzania powinna przygotowywać Europejska Rada Ochrony Danych, a Komisja powinna przyjmować je w drodze aktu wykonawczego. Aby ułatwić administratorom przestrzeganie przepisów, Rada powinna również przygotować wspólny wzór i wspólną metodykę przeprowadzania ocen skutków dla ochrony danych, które ma przyjąć Komisja w drodze aktu wykonawczego. Komisja powinna należycie uwzględnić wnioski przygotowane przez Radę i w razie potrzeby dokonać ich przeglądu przed przyjęciem. Aby uwzględnić rozwój technologiczny, wykazy oraz wspólny wzór i metodykę należy poddawać przeglądowi co najmniej raz na trzy lata i w razie potrzeby aktualizować.

(41) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie (UE) 2018/1725 Parlamentu Europejskiego i Rady[36]. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680[37] ma zastosowanie do przetwarzania danych osobowych przez właściwe

---

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

[37] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań

organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar. Rozporządzenie (UE) 2018/1725 i dyrektywę (UE) 2016/680 należy dostosować do zmian w rozporządzeniu (UE) 2016/679 wprowadzonych niniejszym rozporządzeniem.

(42) Jak wyjaśniono w motywie 5 rozporządzenia (UE) 2018/1725, w każdym przypadku, w którym przepisy rozporządzenia (UE) 2018/1725 opierają się na tych samych założeniach co przepisy rozporządzenia (UE) 2016/679, przepisy obu aktów należy, zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej, interpretować tak samo. System w rozporządzeniu (UE) 2018/1725 powinien być uznawany za równoważny z systemem w rozporządzeniu (UE) 2016/679. W związku z tym niniejsze rozporządzenie zmienia również przepisy rozporządzenia (UE) 2018/1725, których dotyczą zmiany rozporządzenia (UE) 2016/679, w zakresie, w jakim zmiany te są również istotne w kontekście przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii.

(43) Aby zapewnić solidne i spójne ramy ochrony danych w Unii, po przyjęciu niniejszego rozporządzenia należy dokonać niezbędnych dostosowań dyrektywy (UE) 2016/680 i wszelkich innych aktów prawnych Unii mających zastosowanie do takiego przetwarzania danych osobowych, aby umożliwić ich stosowanie jak najbliżej momentu rozpoczęcia stosowania zmian w rozporządzeniu (UE) 2016/679 i rozporządzeniu (UE) 2018/1725.

(44) Przechowywanie danych osobowych lub uzyskanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu oraz dalsze przetwarzanie takich danych powinny regulować jednolite ramy prawne, a mianowicie rozporządzenie (UE) 2016/679, w przypadku gdy abonent usługi łączności elektronicznej lub użytkownik końcowego urządzenia jest osobą fizyczną. Zmiany przedstawione w niniejszym rozporządzeniu nadal zapewniają najwyższy poziom ochrony danych osobowych, upraszczając jednocześnie doświadczenia osób, których dane dotyczą, w zakresie korzystania z przysługujących im praw i wyrażania swoich wyborów w internecie. Zmiany dotyczą w szczególności przechowywania informacji w tym urządzeniu, uzyskiwania dostępu do informacji z tego urządzenia lub gromadzenia ich w inny sposób z tego urządzenia, co wiąże się z przetwarzaniem danych osobowych za pomocą plików cookie lub podobnych technologii w celu uzyskania informacji z końcowego urządzenia. Odpowiednie przepisy powinny mieć również zastosowanie niezależnie od tego, czy końcowe urządzenie jest własnością osoby fizycznej, czy innej osoby prawnej lub fizycznej.

Przechowywanie danych osobowych lub uzyskanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu powinno być nadal dozwolone wyłącznie na podstawie zgody. Podobnie jak w przypadku podejścia przyjętego w dyrektywie 2002/58/WE wymóg ten nie powinien wykluczać przechowywania danych osobowych

---

przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

lub uzyskania dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej, jeżeli opiera się ono na prawie Unii lub prawie państwa członkowskiego w rozumieniu art. 6 rozporządzenia (UE) 2016/679 i jeżeli spełnia wszystkie warunki zgodności z prawem określone w tym przepisie oraz odbywa się w celach określonych w art. 23 ust. 1 rozporządzenia (UE) 2016/679.

W celu zmniejszenia obciążenia regulacyjnego i zapewnienia administratorom jasności prawa oraz biorąc pod uwagę, że niektóre cele przetwarzania powodują niskie ryzyko naruszenia praw i wolności osób, których dane dotyczą, lub że takie przetwarzanie może być niezbędne do świadczenia usługi żądanej przez osobę, której dane dotyczą, konieczne jest opracowanie wyczerpującego wykazu celów, w przypadku których przetwarzanie powinno być dozwolone bez zgody. Jeżeli chodzi o przechowywanie danych osobowych lub uzyskanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu oraz dalsze przetwarzanie, które jest niezbędne do tych celów, niniejsze rozporządzenie powinno stanowić, że przetwarzanie jest zgodne z prawem. Administrator, taki jak dostawca usług medialnych, może upoważnić podmiot przetwarzający, taki jak przedsiębiorstwo zajmujące się badaniem rynku, do przetwarzania w jego imieniu.

Do dalszego przetwarzania danych osobowych do celów innych niż cele określone w wyczerpującym wykazie należy stosować art. 6 oraz, w stosownych przypadkach, art. 9 rozporządzenia (UE) 2016/679. W świetle zasady rozliczalności do administratora należy wybór odpowiedniej podstawy prawnej zamierzonego przetwarzania. Aby móc powołać się na prawnie uzasadniony interes na mocy art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679 jako podstawę dalszego przetwarzania danych osobowych, administrator musi wykazać, że realizuje on prawnie uzasadniony interes administratora lub stron trzecich, przetwarzanie jest niezbędne do osiągnięcia celu tego prawnie uzasadnionego interesu, a interesy lub prawa podstawowe osoby, której dane dotyczą, nie mają charakteru nadrzędnego wobec interesów realizowanych przez administratora. W tym kontekście administratorzy powinni w jak największym stopniu uwzględnić następujące elementy: czy osoba, której dane dotyczą, jest dzieckiem; uzasadnione oczekiwania osoby, której dane dotyczą; wpływ na osobę fizyczną ze względu na skalę przetwarzanych danych albo wrażliwość przetwarzanych danych; skalę danego przetwarzania w takim sensie, że nie może ono być szczególnie rozległe ani ze względu na ilość, ani ze względu na zakres kategorii danych; przetwarzanie powinno opierać się na danych ograniczonych do tego, co niezbędne, i nie może opierać się na monitorowaniu dużej części działalności internetowej osób, których dane dotyczą; oraz, w stosownych przypadkach, inne istotne czynniki. Przetwarzanie nie powinno prowadzić do ciągłego monitorowania życia prywatnego osoby, której dane dotyczą.

Jeżeli administrator nie może powołać się na prawnie uzasadniony interes jako podstawę prawną dalszego przetwarzania, przetwarzanie powinno opierać się na innej podstawie określonej w art. 6 ust. 1, w szczególności na zgodzie zgodnie z art. 6 i 7 rozporządzenia (UE) 2016/679, pod warunkiem że przestrzega się wszystkich zasad określonych w rozporządzeniu (UE) 2016/679.

(45) Osoby, których dane dotyczą, które odrzuciły wniosek o wyrażenie zgody, często otrzymują nowe zapytanie o zgodę za każdym razem, gdy ponownie odwiedzają usługę online tego samego administratora. Może to mieć szkodliwe skutki dla osób, których dane dotyczą, które mogą wyrazić zgodę wyłącznie w celu uniknięcia powtarzających się zapytań. Administrator powinien być zatem zobowiązany do

poszanowania decyzji osoby, której dane dotyczą, o odrzuceniu żądania wyrażenia zgody co najmniej przez określony czas.

(46) Osoby, których dane dotyczą, powinny mieć możliwość polegania na zautomatyzowanych i nadających się do odczytu maszynowego wskazaniach, że chcą wyrazić zgodę lub odrzucić wniosek o wyrażenie zgody lub sprzeciwić się przetwarzaniu danych. Takie środki powinny opierać się na najnowocześniejszych rozwiązaniach. Można je wdrożyć w ustawieniach przeglądarki internetowej lub w europejskim portfelu tożsamości cyfrowej określonym w rozporządzeniu (UE) nr 914/2014 lub za pomocą wszelkich innych odpowiednich środków. Przepisy określone w niniejszym rozporządzeniu powinny wspierać powstawanie rozwiązań rynkowych z odpowiednimi interfejsami. Administrator powinien być zobowiązany do przestrzegania zautomatyzowanych i nadających się do odczytu maszynowego wskazań wyborów dokonanych przez osobę, której dane dotyczą, gdy tylko dostępne będą normy. W świetle znaczenia niezależnego dziennikarstwa w społeczeństwie demokratycznym oraz aby nie podważać jego podstawy ekonomicznej, dostawcy usług medialnych nie powinni być zobowiązani do przestrzegania nadających się do odczytu maszynowego wskazań wyborów osoby, której dane dotyczą. Spoczywający na dostawcach przeglądarek internetowych obowiązek zapewnienia osobom, których dane dotyczą, środków technicznych umożliwiających im dokonywanie wyborów w odniesieniu do przetwarzania nie powinien ograniczać możliwości zwrócenia się przez dostawców usług medialnych o zgodę do osób, których dane dotyczą.

(47) Dyrektywa 2002/58/WE o prywatności i łączności elektronicznej („dyrektywa o e-prywatności”), ostatnio zmieniona w 2009 r., zapewnia ramy ochrony prawa do prywatności, w tym poufności komunikacji. Wskazano w niej również rozporządzenie (UE) 2016/679 w odniesieniu do przetwarzania danych osobowych w kontekście usług łączności elektronicznej. Chroni ona prywatność i integralność końcowego urządzenia użytkownika lub abonenta wykorzystywanego do takiej komunikacji. Obecny przepis art. 5 ust. 3 dyrektywy 2002/58/WE powinien nadal mieć zastosowanie, o ile abonent lub użytkownik nie jest osobą fizyczną, a przechowywane informacje lub informacje, do których uzyskuje się dostęp, nie stanowią przetwarzania danych osobowych ani nie prowadzą do ich przetwarzania.

(48) Należy uchylić art. 4 dyrektywy 2002/58/WE. W art. 4 dyrektywy 2002/58/WE określono wymogi dla dostawców publicznie dostępnych usług łączności elektronicznej w odniesieniu do zapewnienia bezpieczeństwa ich usług oraz wymogi dotyczące powiadamiania. Następnie w dyrektywie (UE) 2022/2555 ustanowiono nowe wymogi dla tych dostawców dotyczące środków zarządzania ryzykiem w cyberprzestrzeni i zgłaszania incydentów. Aby ograniczyć nakładanie się obowiązków podmiotów w sektorze łączności elektronicznej, należy uchylić art. 4 dyrektywy 2002/58/WE. Jeżeli chodzi o bezpieczeństwo przetwarzania danych osobowych zgodnie z art. 4 ust. 1 i 1a tej dyrektywy oraz zgłaszanie naruszeń ochrony danych osobowych zgodnie z art. 4 ust. 3–5 dyrektywy 2002/58/WE, w rozporządzeniu (UE) 2016/679 przewidziano już kompleksowe i aktualne przepisy. Przepisy te powinny zatem mieć zastosowanie do dostawców publicznie dostępnych usług łączności elektronicznej i dostawców publicznych sieci łączności, dzięki czemu jeden system miałby zastosowanie do administratorów i podmiotów przetwarzających.

(49) W kilku horyzontalnych lub sektorowych aktach prawnych Unii wymaga się powiadomienia różnych organów o tym samym zdarzeniu za pomocą różnych środków i kanałów technicznych. Pojedynczy punkt kontaktowy do zgłaszania incydentów powinien umożliwiać podmiotom wypełnianie obowiązków

sprawozdawczych wynikających z dyrektywy (UE) 2022/2555, rozporządzenia (UE) 2016/679, rozporządzenia (UE) 2022/2554, rozporządzenia (UE) nr 910/2014 i dyrektywy (UE) 2022/2557 przez przekazywanie zgłoszeń do jednego interfejsu. Ponadto pojedynczy punkt kontaktowy powinien umożliwiać podmiotom wyszukiwanie informacji, które wcześniej przekazały za pośrednictwem pojedynczego punktu kontaktowego, pomagając tym samym podmiotom w monitorowaniu wypełniania obowiązków sprawozdawczych w związku z konkretnymi incydentami.

(50) Aby zapewnić bezpieczeństwo pojedynczego punktu kontaktowego, ENISA powinna wprowadzić odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa pojedynczego punktu kontaktowego oraz informacji przekazywanych lub rozpowszechnianych za pośrednictwem pojedynczego punktu kontaktowego. Oceniając ryzyko oraz adekwatność i proporcjonalność tych środków, ENISA powinna wziąć pod uwagę wrażliwość informacji przekazywanych lub rozpowszechnianych zgodnie z odpowiednimi aktami prawnymi Unii. ENISA powinna konsultować się z właściwymi organami na mocy odpowiednich aktów prawnych Unii podczas opracowywania środków technicznych, operacyjnych i organizacyjnych niezbędnych do ustanowienia, utrzymania i bezpiecznej obsługi pojedynczego punktu kontaktowego, korzystając z istniejących grup współpracy i sieci państw członkowskich ustanowionych na mocy tych aktów.

(51) Przed umożliwieniem zgłaszania incydentów ENISA powinna przeprowadzić pilotaż funkcjonowania pojedynczego punktu kontaktowego, który powinien obejmować dokładne przetestowanie specyfiki i wymogów dotyczących zgłoszeń w odniesieniu do odpowiednich aktów prawnych Unii. Na podstawie wyników pilotażu Komisja powinna ocenić właściwe funkcjonowanie, niezawodność, integralność i poufność pojedynczego punktu kontaktowego. Podczas przeprowadzania oceny Komisja powinna konsultować się z siecią CSIRT i właściwymi organami na podstawie odpowiednich aktów prawnych Unii, wykorzystując istniejące grupy współpracy i sieci państw członkowskich ustanowione na podstawie tych aktów. W przypadku gdy Komisja stwierdzi, że pojedynczy punkt kontaktowy zapewnia właściwe funkcjonowanie, niezawodność, integralność i poufność, powinna opublikować zawiadomienie w tej sprawie w *Dzienniku Urzędowym Unii Europejskiej*. W przypadku gdy Komisja uzna, że nie zapewniono właściwego funkcjonowania, niezawodności, integralności i poufności, ENISA powinna podjąć wszelkie niezbędne środki naprawcze, a następnie Komisja powinna dokonać ponownej oceny.

(52) Aby zapewnić ciągłość i interoperacyjność z istniejącymi krajowymi rozwiązaniami technicznymi, które ułatwiają zgłaszanie incydentów, ENISA powinna w miarę możliwości uwzględniać takie krajowe rozwiązania techniczne przy opracowywaniu specyfikacji dotyczących środków technicznych, operacyjnych i organizacyjnych niezbędnych do ustanowienia, utrzymania i bezpiecznej obsługi pojedynczego punktu kontaktowego. Ponadto ENISA powinna rozważyć protokoły i narzędzia techniczne, takie jak interfejsy programowania aplikacji i standardy nadające się do odczytu maszynowego, które umożliwiają podmiotom włączenie obowiązków sprawozdawczych do procesów biznesowych, a organom połączenie pojedynczego punktu kontaktowego z ich krajowymi systemami zgłaszania.

(53) W celu zapewnienia, aby pojedynczy punkt kontaktowy umożliwiał odpowiednim podmiotom przekazywanie rodzajów informacji i formatów wymaganych na podstawie odpowiednich aktów prawnych Unii, ENISA powinna przeprowadzić konsultacje z Komisją i właściwymi organami na podstawie tych aktów. W przypadku

gdy akt prawny Unii nie jest w pełni zharmonizowany w odniesieniu do rodzaju informacji i formatu zgłoszeń, państwa członkowskie powinny poinformować ENISA o swoich przepisach krajowych.

(54) Na podstawie rozporządzenia (UE) 2022/2554 sektor finansowy odgrywa wiodącą rolę we wdrażaniu zharmonizowanych, kompleksowych i skutecznych ram, w tym w odniesieniu do zgłaszania incydentów. Aby uprościć przestrzeganie przepisów, należy dostosować ramy zgłaszania incydentów ustanowione na mocy rozporządzenia (UE) 2022/2554 do pojedynczego punktu kontaktowego, przy jednoczesnym zapewnieniu ciągłości i stabilności istniejących ram zgłaszania oraz biorąc pod uwagę, że pojedynczy punkt kontaktowy zostałby uruchomiony po dokonaniu oceny i stwierdzeniu, że zapewnia on właściwe funkcjonowanie, niezawodność, integralność i poufność. Ponadto rozporządzeniem (UE) 2022/2554 wprowadzono standardowe wzory na potrzeby zgłaszania, które upraszczają treść zgłoszeń dotyczących poważnych incydentów związanych z ICT w sektorze finansowym. Doświadczenia zdobyte podczas przyjmowania tych wzorów dostarczają cennych spostrzeżeń i najlepszych praktyk, które należy wziąć pod uwagę przy określaniu rodzaju informacji, formatu i procedury zgłoszenia do celów zgłaszania do pojedynczego punktu kontaktowego na podstawie, odpowiednio, dyrektywy (UE) 2022/2555, dyrektywy (UE) 2022/2557 lub rozporządzenia (UE) 2016/679. W tym celu Komisja powinna należycie uwzględnić regulacyjne standardy techniczne przyjęte na podstawie rozporządzenia (UE) 2022/2554, które określają treść wstępnego powiadomienia oraz sprawozdań śródokresowych i końcowych dotyczących poważnych incydentów związanych z ICT. Podejście to ma na celu zapewnienie spójności, promowanie synergii i zmniejszenie obciążenia administracyjnego podmiotów dzięki zminimalizowaniu liczby pól danych, które podmioty są zobowiązane wypełnić, a tym samym ułatwieniu bardziej wydajnych i usprawnionych procesów zgłaszania.

(55) Zgodnie z odpowiednimi aktami prawnymi Unii na późniejszym etapie właściwe organy mają wymieniać między sobą niektóre informacje dotyczące konkretnych incydentów w celu ułatwienia skutecznego nadzoru i koordynacji. W związku z tym pojedynczy punkt kontaktowy należy zaprojektować w taki sposób, aby umożliwiał i wspierał wymianę informacji na tym poziomie w odniesieniu do każdego odpowiedniego aktu prawnego Unii, zapewniając, aby odpowiedni przepływ danych między organami był możliwy w sposób bezpieczny, terminowy i skuteczny, jeżeli państwa członkowskie zdecydują się skorzystać z tej dodatkowej funkcji.

(56) Aby zapewnić zgłaszanie incydentów za pośrednictwem pojedynczego punktu kontaktowego, należy zatem odpowiednio zmienić dyrektywę (UE) 2022/2555, rozporządzenie (UE) 2016/679, rozporządzenie (UE) 2022/2554, rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2022/2557. Pojedynczy punkt kontaktowy należy zacząć wykorzystywać do celów zgłaszania na podstawie tych aktów w terminie 18 miesięcy od wejścia w życie niniejszego rozporządzenia. W przypadku gdy Komisja uruchamia mechanizmy przewidziane w zawiadomieniu opóźniające datę rozpoczęcia stosowania do 24 miesięcy od wejścia w życie rozporządzenia, odpowiednie przepisy dyrektywy (UE) 2022/2555, rozporządzenia (UE) nr 910/2014, rozporządzenia (UE) 2022/2554 i dyrektywy (UE) 2022/2557 powinny nadal mieć zastosowanie do celów wypełnienia obowiązków w zakresie zgłaszania określonych w tych przepisach.

(57) W wyjątkowym przypadku, gdy brak technicznej możliwości uniemożliwia przesyłanie zgłoszeń incydentów za pośrednictwem pojedynczego punktu kontaktowego, podmioty powinny wypełniać swoje obowiązki w zakresie zgłaszania

za pomocą alternatywnych środków. W tym celu adresaci zgłoszeń incydentów na podstawie odpowiednich aktów prawnych Unii powinni zapewnić możliwość otrzymywania takich zgłoszeń incydentów za pomocą alternatywnych środków oraz powinni podawać do wiadomości publicznej informacje o tych alternatywnych środkach.

(58) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[38] skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia [DATA] r. Zgodnie z art. 42 ust. 2 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejską Radą Ochrony Danych, która wydała opinię dnia [DATA] r.

(59) W rozporządzeniu (UE) 2019/1150 ustanowiono ukierunkowany zestaw obowiązkowych zasad na poziomie Unii, aby zapewnić istnienie sprawiedliwego, przewidywalnego, zrównoważonego i budzącego zaufanie otoczenia biznesowego w internecie w ramach rynku wewnętrznego. Rozporządzenie (UE) 2022/2065 i rozporządzenie (UE) 2022/1925 zapewniają kompleksowe ramy regulacyjne na rzecz bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego dla wszystkich użytkowników końcowych usług online oraz ustanawiają równe warunki działania dla przedsiębiorstw na rynkach cyfrowych. W celu uproszczenia przepisów Unii w dziedzinie usług pośrednictwa internetowego i platform internetowych oraz biorąc pod uwagę, że cele i istotne przepisy rozporządzenia w sprawie stosunków między platformami a przedsiębiorcami w dużej mierze obejmuje akt o usługach cyfrowych i akt o rynkach cyfrowych, należy uchylić rozporządzenie (UE) 2019/1050. Rozporządzenie (UE) 2022/2065 i rozporządzenie (UE) 2022/1925 przyczyniają się do tworzenia w pełni zharmonizowanych ram regulacyjnych dotyczących usług cyfrowych i rynków cyfrowych dzięki zbliżeniu środków krajowych dotyczących wymogów dla dostawców usług pośrednictwa oraz kontestowalności i uczciwości podstawowych usług platformowych świadczonych przez strażników dostępu. Ze względu na pewność prawa wybrane definicje zawarte w art. 2, przepisy dotyczące ograniczeń i zawieszeń zawarte w art. 4, a także przepisy dotyczące wewnętrznego systemu rozpatrywania skarg zawarte w art. 11 rozporządzenia (UE) 2019/1150, do których odsyłają inne akty prawne, w szczególności dyrektywa (UE) 2023/2831 w sprawie poprawy warunków pracy za pośrednictwem platform, oraz art. 15 zapewniający egzekwowanie, będą miały nadal zastosowanie do czasu zmiany pierwotnych aktów.

(60) Biorąc pod uwagę techniczny charakter zmian proponowanych w niniejszym rozporządzeniu oraz pilną potrzebę opracowania uproszczonych ram prawnych, niniejsze rozporządzenie powinno wejść w życie natychmiast po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*. W stosownych przypadkach państwom

---

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

członkowskim i podmiotom objętym regulacją należy przyznać okresy przejściowe na dostosowanie się do przepisów,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zmiany w rozporządzeniu (UE) 2023/2854

W rozporządzeniu (UE) 2023/2854 wprowadza się następujące zmiany:

1. w art. 1 wprowadza się następujące zmiany:

(a) w ust. 1 dodaje się litery w brzmieniu:

„ea) dobrowolnej rejestracji usług pośrednictwa danych;

eb) dobrowolnej rejestracji podmiotów, które gromadzą i przetwarzają dane udostępniane z pobudek altruistycznych;

ec) ustanowienia Europejskiej Rady ds. Innowacji w zakresie Danych;

ed) wymogów w zakresie lokalizacji danych i dostępności danych dla właściwych organów;

ee) ponownego wykorzystywania niektórych danych i dokumentów będących w posiadaniu organów sektora publicznego lub niektórych przedsiębiorstw publicznych oraz danych badawczych;”;

(b) w ust. 2 dodaje się litery w brzmieniu:

„g) rozdział VIIa ma zastosowanie do danych osobowych i nieosobowych;

h) rozdział VIIb ma zastosowanie do wszelkich danych nieosobowych;

i) rozdział VIIc ma zastosowanie do danych osobowych i nieosobowych, a mianowicie:

(i) dokumentów będących w posiadaniu organów sektora publicznego państw członkowskich, o których mowa:

1) w art. 32i ust. 1 lit. a), lub przedsiębiorstw publicznych, o których mowa:

2) w art. 32i ust. 1 lit. b);

(ii) danych badawczych, o których mowa w art. 32i ust. 1 lit. c);

(iii) niektórych kategorii danych chronionych, o których mowa w art. 32i ust. 1 lit. a).”;

(c) ust. 3 lit. g) otrzymuje brzmienie:

„g) uczestników przestrzeni danych.”;

(d) uchyla się ust. 7;

(e) dodaje się ust. 11, 12 i 13 w brzmieniu:

„11. Rozdział VIIb niniejszego rozporządzenia pozostaje bez uszczerbku dla przepisów ustawowych, wykonawczych i administracyjnych, które dotyczą

wewnętrznej organizacji państw członkowskich i które przyznają organom publicznym i podmiotom prawa publicznego uprawnienia i obowiązki w zakresie przetwarzania danych bez wynikającego ze stosunku umownego wynagrodzenia na rzecz podmiotów prawa prywatnego, a także dla przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich przewidujących zasady wykonywania takich uprawnień i obowiązków.

12. Jeżeli sektorowe prawo Unii lub sektorowe prawo krajowe wymagają od organów sektora publicznego, dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych spełnienia szczególnych dodatkowych wymogów technicznych, administracyjnych lub organizacyjnych, które odnoszą się do rozdziałów VIIa i VIIb, w tym poprzez system zezwoleń lub certyfikacji, stosuje się również te przepisy danego sektorowego prawa Unii lub sektorowego prawa krajowego. Wszelkie takie szczególne dodatkowe wymogi muszą być niedyskryminujące, proporcjonalne i obiektywnie uzasadnione.

13. W odniesieniu do danych i dokumentów, które są objęte zakresem rozdziału VIIc sekcja II, rozdział VIIc niniejszego rozporządzenia nie ma wpływu na możliwość przyjęcia przez państwa członkowskie bardziej szczegółowych lub bardziej rygorystycznych przepisów, pod warunkiem że przepisy te umożliwiają ponowne wykorzystywanie danych i dokumentów na większą skalę.”;

2. w art. 2 wprowadza się następujące zmiany:

(a) dodaje się pkt 4a, 4b i 4c w brzmieniu:

„4a) »zgoda« oznacza zgodę zdefiniowaną w art. 4 pkt 11 rozporządzenia (UE) 2016/679;

4b) »pozwolenie« oznacza przyznanie użytkownikom danych prawa do przetwarzania danych nieosobowych;

4c) »dostęp« oznacza wykorzystywanie danych zgodnie ze szczegółowymi wymogami technicznymi, prawnymi lub organizacyjnymi, które niekoniecznie musi się wiązać z przesyłaniem lub pobieraniem danych;”;

(b) pkt 13 otrzymuje brzmienie:

„13) »posiadacz danych«” oznacza osobę fizyczną lub prawną, która ma prawo lub obowiązek – zgodnie z niniejszym rozporządzeniem, mającym zastosowanie prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii – wykorzystywać i udostępniać dane, w tym o ile zostało to przewidziane umową, dane z produktu lub dane z usługi powiązanej pobrane lub wygenerowane przez nią podczas świadczenia powiązanej usługi;”;

(c) dodaje się pkt 28a i 28b w brzmieniu:

„28a) »podmioty prawa publicznego« oznaczają podmioty, które posiada wszystkie poniższe cechy:

a) zostały utworzone w konkretnym celu zaspokajania potrzeb w interesie ogólnym, które nie mają charakteru przemysłowego ani handlowego;

b) posiadają osobowość prawną;

c) są finansowane w przeważającej części przez państwo, władze regionalne lub lokalne lub inne podmioty prawa publicznego; lub ich zarządy podlegają nadzorowi ze strony tych władz lub podmiotów bądź ponad połowa członków ich organów administrujących, zarządzających lub nadzorczych została wyznaczona przez państwo, instytucje regionalne lub lokalne, lub przez inne podmioty prawa publicznego;

28b) »przedsiębiorstwo publiczne« oznacza każde przedsiębiorstwo, na które organ sektora publicznego może wywierać, bezpośrednio lub pośrednio, dominujący wpływ z racji bycia jego właścicielem, posiadania w nim wkładu finansowego lub na mocy przepisów, które regulują działalność tego przedsiębiorstwa. Zakłada się istnienie dominującego wpływu ze strony organów sektora publicznego w dowolnym z poniższych przypadków, gdy organy te bezpośrednio lub pośrednio:

a) posiadają większość kapitału subskrybowanego przedsiębiorstwa;

b) kontrolują większość głosów związanych z akcjami wyemitowanymi przez przedsiębiorstwo;

c) mogą powołać więcej niż połowę organu administracyjnego, zarządzającego lub nadzorczego przedsiębiorstwa;";

(d) dodaje się pkt 38a i 38b w brzmieniu:

„38a) »usługa pośrednictwa danych« oznacza usługę, która ma na celu ustanowienie – za pomocą środków technicznych, prawnych lub innych – stosunków o charakterze handlowym między nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych oraz użytkownikami danych do celów dzielenia się danymi, w tym do celów wykonywania praw osób, których dane dotyczą, w odniesieniu do danych osobowych, oraz:

1) której głównym celem nie jest pośrednictwo w zakresie treści chronionych prawem autorskim;

2) która nie jest wspólnie zamawiana przez kilka osób prawnych do wyłącznego użytku między nimi;

38b) »altruizm danych« oznacza dobrowolne dzielenie się danymi na podstawie wyrażonej przez osoby, których dane dotyczą, zgody na przetwarzanie dotyczących ich danych osobowych lub na podstawie udzielonego przez posiadaczy danych pozwolenia na wykorzystywanie ich danych nieosobowych, bez żądania ani otrzymania za to wynagrodzenia wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych do celów leżących w interesie ogólnym określonych – w stosownych przypadkach – w prawie krajowym, takich jak opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie polityki publicznej lub do celów badań naukowych leżących w interesie ogólnym;";

(e) dodaje się pkt 44–63 w brzmieniu:

„44) »średnie przedsiębiorstwo« oznacza średnie przedsiębiorstwo zdefiniowane w art. 2 załącznika I do zalecenia 2003/361/WE;

45) »mała spółka o średniej kapitalizacji« oznacza małą spółkę o średniej kapitalizacji zdefiniowaną w pkt 2 załącznika do zalecenia Komisji (UE) 2025/1099;

46) »uniwersytet« oznacza organ sektora publicznego, który oferuje kształcenie na poziomie wyższym pomaturalnym zakończone uzyskaniem stopnia akademickiego;

47) »licencja standardowa« oznacza zbiór z góry określonych warunków ponownego wykorzystywania w formacie cyfrowym, najlepiej kompatybilny ze standardowymi licencjami publicznymi, dostępnymi w internecie;

48) »dokument« oznacza:

a) wszelkie treści niecyfrowe, bez względu na nośnik (papier lub nagranie dźwiękowe, wizualne lub audiowizualne); lub

b) każdą dowolną część takiej treści;

50) »dane dynamiczne« oznaczają dane i dokumenty w formie cyfrowej, podlegające częstym aktualizacjom lub aktualizacjom w czasie rzeczywistym, w szczególności ze względu na ich zmienność lub szybkie starzenie się; dane wygenerowane przez czujniki zasadniczo uznaje się za dane dynamiczne;

51) »dane badawcze« oznaczają dane, inne niż publikacje naukowe, które są gromadzone lub produkowane w ramach działalności badawczo-naukowej i są wykorzystywane jako dowody w procesie badawczym bądź też są powszechnie akceptowane w środowisku naukowym jako konieczne do weryfikacji poprawności ustaleń i wyników badań;

52) »ponowne wykorzystywanie« oznacza wykorzystywanie przez osoby fizyczne lub podmioty prawne dokumentów będących w posiadaniu:

a) organów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla którego to celu dokumenty te zostały wyprodukowane, z wyjątkiem wymiany dokumentów między organami sektora publicznego służącej wyłącznie wykonywaniu ich zadań publicznych; lub

b) przedsiębiorstw publicznych, na podstawie rozdziału VIIc sekcja 2, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w zakresie świadczenia usług w interesie ogólnym, dla którego to celu dokumenty te zostały wyprodukowane, z wyjątkiem wymiany dokumentów między przedsiębiorstwami publicznymi a organami sektora publicznego służącej wyłącznie wykonywaniu zadań publicznych organów sektora publicznego;

53) »zbiory danych o wysokiej wartości« oznaczają dane i dokumenty, których ponowne wykorzystywanie wiąże się z istotnymi korzyściami dla społeczeństwa, środowiska i gospodarki, w szczególności ze względu na ich przydatność do tworzenia usług i zastosowań o wartości dodanej oraz nowych godnych miejsc pracy wysokiej jakości, a także ze względu na liczbę potencjalnych beneficjentów usług i zastosowań o wartości dodanej opartych na tych danych i dokumentach;

54) »niektóre kategorie danych chronionych« oznaczają dane i dokumenty będące w posiadaniu organów sektora publicznego, które są chronione ze względu na:

a) poufność informacji handlowych, w tym tajemnicę handlową, zawodową i tajemnicę przedsiębiorstwa;

b) poufność informacji statystycznych;

c) ochronę praw własności intelektualnej osób trzecich; lub

d) ochronę danych osobowych w zakresie, w jakim dane te nie wchodzą w zakres rozdziału VIIc sekcja 2;

56) »bezpieczne środowisko przetwarzania« oznacza środowisko fizyczne lub wirtualne oraz środki organizacyjne służące zapewnieniu przestrzegania prawa Unii, w szczególności pod względem praw osób, których dane dotyczą, praw własności intelektualnej oraz poufności informacji handlowych i statystycznych, integralności i dostępności, jak również mającego zastosowanie prawa krajowego oraz umożliwiające podmiotowi zapewniającemu bezpieczne środowisko przetwarzania określenie i nadzorowanie wszystkich działań związanych z przetwarzaniem danych, w tym wyświetlania, przechowywania, pobierania i eksportowania danych oraz obliczania danych pochodnych za pomocą algorytmów obliczeniowych;

57) »ponowny użytkownik« oznacza osobę fizyczną lub prawną, której przyznano prawo do ponownego wykorzystywania danych lub dokumentów będących w posiadaniu organu sektora publicznego lub przedsiębiorstwa publicznego na podstawie rozdziału VIIc lub do danych badawczych lub niektórych kategorii danych chronionych;

58) »format nadający się do odczytu maszynowego« oznacza format pliku ustrukturyzowany tak, aby aplikacje mogły łatwo zidentyfikować, rozpoznać i pozyskać określone dane, w tym poszczególne stwierdzenia faktów, i ich wewnętrzną strukturę;

59) »format otwarty« oznacza format pliku, który nie jest powiązany z platformą oraz jest udostępniany obywatelom bez żadnych ograniczeń, które utrudniałyby ponowne wykorzystywanie dokumentów;

60) »otwarty standard formalny« oznacza standard określony w formie pisemnej, wyszczególniający specyfikacje wymogów dotyczących sposobu zapewnienia interoperacyjności oprogramowania;

61) »rozsądny zwrot z inwestycji« oznacza odsetek całkowitej opłaty ponad kwotę, która jest konieczna do odzyskania kwalifikujących się kosztów, w wysokości nieprzekraczającej określonej przez EBC stałej stopy oprocentowania powiększonej o maksymalnie 5 punktów procentowych;

62) »wymóg dotyczący lokalizacji danych« oznacza każdy obowiązek, zakaz, warunek, ograniczenie lub innego rodzaju wymóg określony w przepisach ustawowych, wykonawczych lub administracyjnych państwa członkowskiego lub wynikający z powszechnych i spójnych praktyk administracyjnych w państwie członkowskim i w podmiotach prawa publicznego, w tym w dziedzinie zamówień publicznych, bez uszczerbku dla dyrektywy 2014/24/UE, który narzuca wymóg przetwarzania danych na terytorium danego państwa

członkowskiego lub utrudnia przetwarzanie danych w jakimkolwiek innym państwie członkowskim;

63) »pseudonimizacja« oznacza pseudonimizację, o której mowa w art. 4 pkt 5 rozporządzenia (UE) 2016/679.”;

3. art. 4 ust. 8 otrzymuje brzmienie:

„8. W wyjątkowych okolicznościach, gdy posiadacz danych będący posiadaczem tajemnicy przedsiębiorstwa może wykazać, że mimo środków technicznych i organizacyjnych zastosowanych przez użytkownika zgodnie z ust. 6 niniejszego artykułu ujawnienie tajemnic przedsiębiorstwa z dużym prawdopodobieństwem poskutkuje poważną szkodą ekonomiczną lub że ujawnienie tajemnic przedsiębiorstwa użytkownikowi stwarza wysokie ryzyko bezprawnego pozyskiwania, wykorzystywania lub ujawniania podmiotom z państw trzecich lub podmiotom mającym siedzibę w Unii i znajdującym się pod bezpośrednią lub pośrednią kontrolą takich podmiotów, które podlegają jurysdykcjom zapewniającym słabszą lub nierównoważną ochronę w porównaniu z ochroną przewidzianą w prawie Unii, ten posiadacz danych może w tym konkretnym przypadku odrzucić wniosek o dostęp do tych konkretnych danych. Wykazane informacje muszą być należycie uzasadnione na podstawie obiektywnych elementów, takich jak egzekwowalność tajemnic przedsiębiorstwa w państwach trzecich, charakter i poziom poufności żądanych danych oraz niepowtarzalność i nowatorskość produktu skomunikowanego. Informacje te przekazuje się użytkownikowi na piśmie bez zbędnej zwłoki. W przypadku gdy posiadacz danych odmawia dzielenia się danymi na podstawie niniejszego ustępu, powiadamia on właściwy organ wyznaczony zgodnie z art. 37.”;

4. art. 5 ust. 11 otrzymuje brzmienie:

„11. W wyjątkowych okolicznościach, gdy posiadacz danych będący posiadaczem tajemnicy przedsiębiorstwa może wykazać, że mimo środków technicznych i organizacyjnych zastosowanych przez stronę trzecią zgodnie z ust. 9 niniejszego artykułu ujawnienie tajemnic przedsiębiorstwa z dużym prawdopodobieństwem poskutkuje poważną szkodą ekonomiczną lub że ujawnienie tajemnic przedsiębiorstwa osobie trzeciej stwarza wysokie ryzyko bezprawnego pozyskiwania, wykorzystywania lub ujawniania podmiotom z państw trzecich lub podmiotom mającym siedzibę w Unii i znajdującym się pod bezpośrednią lub pośrednią kontrolą takich podmiotów, które podlegają jurysdykcjom zapewniającym słabszą lub nierównoważną ochronę w porównaniu z ochroną przewidzianą w prawie Unii, ten posiadacz danych może w tym konkretnym przypadku odrzucić wniosek o dostęp do tych konkretnych danych. Wykazane informacje muszą być należycie uzasadnione na podstawie obiektywnych elementów, takich jak egzekwowalność tajemnic przedsiębiorstwa w państwach trzecich, charakter i poziom poufności żądanych danych oraz niepowtarzalność i nowatorskość produktu skomunikowanego. Informacje te przekazuje się osobie trzeciej na piśmie bez zbędnej zwłoki. W przypadku gdy posiadacz danych odmawia dzielenia się danymi na podstawie niniejszego ustępu, powiadamia on właściwy organ wyznaczony zgodnie z art. 37.”;

5. tytuł rozdziału V otrzymuje brzmienie:

„UDOSTĘPNIANIE DANYCH ORGANOM SEKTORA PUBLICZNEGO, KOMISJI, EUROPEJSKIEMU BANKOWI CENTRALNEMU I ORGANOM UNII NA PODSTAWIE NIEBEZPIECZEŃSTWA PUBLICZNEGO”;

6. uchyla się art. 14 i 15;

7. dodaje się art. 15a w brzmieniu:

„Artykuł 15a

Obowiązek udostępniania danych przez posiadaczy danych na podstawie niebezpieczeństwa publicznego

1. W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii wykażą wyjątkową potrzebę wykorzystania niektórych danych do wykonywania swoich obowiązków ustawowych w interesie publicznym podczas reagowania na niebezpieczeństwo publiczne, łagodzenia go lub wsparcia przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego, mogą zwrócić się do posiadaczy danych będących osobami prawnymi innymi niż organy sektora publicznego o udostępnienie tych danych, w tym metadanych niezbędnych do interpretacji i wykorzystania tych danych. Na taki należycie uzasadniony wniosek posiadacze danych udostępniają dane i metadane wnioskującemu organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii. Wnioski takie można również składać w przypadku, gdy w związku z niebezpieczeństwem publicznym wymaga się sporządzania statystyk publicznych.

2. Jeżeli żądane dane są niezbędne do zareagowania na niebezpieczeństwo publiczne, a organ wnioskujący zgodnie z ust. 1 nie jest w stanie uzyskać takich danych terminowo i skutecznie w inny sposób na równoważnych warunkach, wniosek dotyczy danych nieosobowych. W przypadku gdy przekazanie danych nieosobowych jest niewystarczające do zareagowania na niebezpieczeństwo publiczne, można również żądać danych osobowych i, w miarę możliwości, udostępnić je w formie pseudonimizowanej, z zastrzeżeniem odpowiednich środków technicznych i organizacyjnych zapewniających ich ochronę.

3. W przypadku gdy żądane dane są niezbędne do łagodzenia niebezpieczeństwa publicznego lub wsparcia przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego, organ wnioskujący na podstawie ust. 1, działający na podstawie prawa Unii lub prawa krajowego, może zwrócić się o konkretne dane nieosobowe, których brak uniemożliwia mu łagodzenia niebezpieczeństwa publicznego lub wsparcie przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego. Takich wniosków nie kieruje się do mikroprzedsiębiorstw i małych przedsiębiorstw.”;

8. art. 16 ust. 2 otrzymuje brzmienie:

„2. Niniejszy rozdział nie ma zastosowania do działań wykonywanych przez organy sektora publicznego, Komisję, Europejski Bank Centralny ani organy Unii związanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem lub ściganiem czynów zabronionych lub przestępstw administracyjnych lub wykonywaniem sankcji karnych ani do

administracji celnej lub podatkowej. Niniejszy rozdział nie wpływa na prawo Unii ani prawo krajowe regulujące takie działania.”;

9. w art. 17 wprowadza się następujące zmiany:

a) w ust. 1 wprowadza się następujące zmiany:

(i) formuła wprowadzająca otrzymuje brzmienie:

„Występując z wnioskiem o dane na podstawie art. 15a, organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii:”;

(ii) lit. b) i c) otrzymują brzmienie:

„b) wykazują, że spełnione zostały warunki złożenia wniosku na podstawie art. 15a;

c) wyjaśniają cel wniosku, planowane wykorzystanie żądanych danych, w tym, w stosownym przypadku, przez osobę trzecią zgodnie z ust. 4 niniejszego artykułu, czas tego wykorzystywania oraz w stosownym przypadku sposób, w jaki przetwarzanie danych osobowych ma odpowiedzieć na niebezpieczeństwo publiczne;”;

b) w ust. 2 wprowadza się następujące zmiany:

(i) lit. c) otrzymuje brzmienie:

„c) jest proporcjonalny do niebezpieczeństwa publicznego i należycie uzasadniony w odniesieniu do szczegółowości i ilości żądanych danych oraz częstotliwości dostępu do żądanych danych;”;

(ii) uchyla się lit. e);

c) uchyla się ust. 5 i 6;

10. w art. 18 wprowadza się następujące zmiany:

a) w ust. 2 wyrażenie wprowadzające otrzymuje brzmienie:

„2. Bez uszczerbku dla określonych w prawie Unii lub prawie krajowym szczególnych potrzeb w zakresie dostępności danych posiadacz danych może odmówić zastosowania się do wniosku o udostępnienie danych przewidzianego w niniejszym rozdziale lub wystąpić o jego zmianę bez zbędnej zwłoki i w żadnym razie nie później niż pięć dni roboczych od otrzymania wniosku zgodnie z art. 15a ust. 2 oraz bez zbędnej zwłoki i w żadnym razie nie później niż 30 dni roboczych od otrzymania wniosku zgodnie z art. 15a ust. 3, powołując się na jeden z następujących powodów:”;

b) skreśla się ust. 5;

11. w art. 19 wprowadza się następujące zmiany:

a) w ust. 1 zdanie wprowadzające otrzymuje brzmienie:

„Organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii, które otrzymały dane zgodnie z wnioskiem złożonym na podstawie art. 15a:”;

b) ust. 3 otrzymuje brzmienie:

„3. Ujawnienie tajemnicy przedsiębiorstwa organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii jest

wymagane wyłącznie w zakresie, w jakim jest to bezwzględnie konieczne do osiągnięcia celu wniosku złożonego na podstawie art. 15a. W takim przypadku posiadacz danych lub, jeżeli nie jest tą samą osobą, posiadacz tajemnicy przedsiębiorstwa identyfikują dane chronione, w tym w stosownych metadanych, jako tajemnice przedsiębiorstwa. Przed ujawnieniem tajemnic przedsiębiorstwa organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii stosują wszelkie niezbędne i odpowiednie środki techniczne i organizacyjne, aby chronić poufność tajemnic przedsiębiorstwa, w tym w stosownym przypadku używają modelowych postanowień umownych, norm technicznych oraz kodeksów postępowania.”;

12. art. 20 otrzymuje brzmienie:

„Artykuł 20

Rekompensata za udostępnienie danych na podstawie rozdziału V

1. Posiadacze danych udostępniają nieodpłatnie dane niezbędne do zareagowania na niebezpieczeństwo publiczne zgodnie z art. 15a ust. 2. Organ sektora publicznego, Komisja, Europejski Banki Centralny lub organ Unii, które otrzymały dane, zapewniają publiczne uznanie posiadaczowi danych, jeżeli posiadacz danych o to wystąpi.

2. Posiadacz danych jest uprawniony do zasadnej rekompensaty za udostępnienie danych zgodnie z wnioskiem złożonym na podstawie art. 15a ust. 3. Rekompensata taka pokrywa koszty techniczne i organizacyjne poniesione w celu zastosowania się do wniosku, w tym w stosownym przypadku koszty anonimizacji, pseudonimizacji, agregacji i dostosowania technicznego, powiększone o rozsądną marżę. Na żądanie organu sektora publicznego, Komisji, Europejskiego Banku Centralnego lub organu Unii posiadacz danych przedstawia informacje o podstawie obliczenia kosztów i rozsądnej marży.

3. Na zasadzie odstępstwa od ust. 1 niniejszego artykułu posiadacz danych będący mikroprzedsiębiorstwem lub małym przedsiębiorstwem może ubiegać się o rekompensatę za udostępnienie danych w odpowiedzi na wniosek na podstawie art. 15a ust. 2, zgodnie z warunkami określonymi w ust. 2 niniejszego artykułu.

4. Posiadacze danych nie mogą domagać się rekompensaty za udostępnienie danych zgodnie z wnioskiem wystosowanym na podstawie art. 15a ust. 3, jeżeli konkretnym zadaniem realizowanym w interesie publicznym jest tworzenie statystyki publicznej i jeżeli prawo krajowe nie zezwala na sprzedaż danych. Państwa członkowskie powiadamiają Komisję, jeżeli prawo krajowe nie zezwala na sprzedaż danych na potrzeby tworzenia statystyki publicznej.”;

13. w art. 21 wprowadza się następujące zmiany:

a) tytuł otrzymuje brzmienie:

„**Dzielenie się danymi pozyskanymi w kontekście niebezpieczeństwa publicznego z organizacjami badawczymi lub urzędami statystycznymi**”;

b) ust. 5 otrzymuje brzmienie:

„5. W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii zamierzają przekazać lub udostępnić dane na podstawie ust. 1, bez zbędnej zwłoki powiadamiają o tym posiadacza danych, od którego otrzymano dane, podając następujące informacje:

a) dane identyfikacyjne i kontaktowe organizacji lub osoby fizycznej otrzymujących dane;

b) cel przekazania lub udostępnienia danych;

c) okres, przez który dane będą wykorzystywane, oraz techniczne środki ochrony;

d) zastosowane środki organizacyjne, w tym jeżeli w grę wchodzą dane osobowe lub tajemnice przedsiębiorstwa.”;

14. przed rozdziałem VI dodaje się art. 22a w brzmieniu:

„Artykuł 22a

Prawo do wniesienia skargi

W przypadku powstania sporu dotyczącego wniosku o dane na podstawie art. 15a, w tym odmowy, zmiany, poziomu rekompensaty lub przekazania, lub udostępnienia danych, posiadacz danych, organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii mogą wnieść skargę do właściwego organu państwa członkowskiego, w którym posiadacz danych ma siedzibę, wyznaczonego zgodnie z art. 37.”;

15. w art. 31 dodaje się ust. 1a i 1b w brzmieniu:

„1a. Obowiązki określone w rozdziale VI, z wyjątkiem art. 29, i w art. 34 nie mają zastosowania do usług przetwarzania danych innych niż te, o których mowa w art. 30 ust. 1, w przypadku gdy większość cech i funkcji usługi przetwarzania danych została dostosowana przez dostawcę do szczególnych potrzeb klienta, jeżeli świadczenie takich usług opiera się na umowie zawartej przed dniem 12 września 2025 r. lub w tym dniu.

Dostawca takich usług przetwarzania danych nie jest zobowiązany do renegocjowania ani zmiany umowy o świadczenie tych usług przed jej wygaśnięciem, jeżeli umowa ta została zawarta przed dniem 12 września 2025 r. lub w tym dniu. Każde postanowienie umowne zawarte w tej umowie, które jest sprzeczne z art. 29 ust. 1, 2 lub 3, uznaje się za nieważne.

1b. Dostawca usług przetwarzania danych może zawrzeć postanowienia dotyczące proporcjonalnych kar za wcześniejsze rozwiązanie umowy w umowie na czas określony o świadczenie usług przetwarzania danych innych niż te, o których mowa w art. 30 ust. 1.

W przypadku gdy dostawca usług przetwarzania danych jest małym i średnim przedsiębiorstwem lub małą spółką o średniej kapitalizacji, obowiązki określone w rozdziale VI, z wyjątkiem art. 29, i w art. 34 nie mają zastosowania do usług przetwarzania danych innych niż te, o których mowa w art. 30 ust. 1, jeżeli świadczenie takich usług opiera się na umowie zawartej przed dniem 12 września 2025 r. lub w tym dniu.

W przypadku gdy dostawcą usług przetwarzania danych jest małe i średnie przedsiębiorstwo lub mała spółka o średniej kapitalizacji, dostawca nie jest

zobowiązany do renegocjowania ani zmiany umowy o świadczenie usług przetwarzania danych innych niż ta, o której mowa w art. 30 ust. 1, przed jej wygaśnięciem, jeżeli umowa ta została zawarta przed dniem 12 września 2025 r. lub w tym dniu. Każde postanowienie umowne zawarte w tej umowie, które jest sprzeczne z art. 29 ust. 1, 2 lub 3, uznaje się za nieważne.”;

16. w art. 32 wprowadza się następujące zmiany:

a) ust. 1 i 2 otrzymują brzmienie:

„1. Dostawcy usług przetwarzania danych, organ sektora publicznego udostępniający dane lub dokumenty zgodnie z rozdziałem VIIc sekcja 3, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych lub dokumentów zgodnie z rozdziałem VIIc sekcja 3, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych stosują wszelkie odpowiednie środki techniczne, organizacyjne i prawne, w tym umowy, w celu zapobiegania międzynarodowemu dostępowi administracji rządowej państw trzecich do danych nieosobowych przechowywanych na terenie Unii oraz międzynarodowemu przekazywaniu takich danych nieosobowych, w przypadku gdy takie przekazywanie lub taki dostęp byłyby sprzeczne z prawem Unii lub prawem krajowym danego państwa członkowskiego, bez uszczerbku dla ust. 2 lub 3.

2. Orzeczenia lub wyroki sądu lub trybunału państwa trzeciego oraz decyzje organu administracyjnego państwa trzeciego nakazujące dostawcy usług przetwarzania danych, organowi sektora publicznego udostępniającemu dane lub dokumenty zgodnie z rozdziałem VIIc sekcja 3, osobie fizycznej lub prawnej, której przyznano prawo do ponownego wykorzystywania danych lub dokumentów zgodnie z rozdziałem VIIc sekcja 3, dostawcy usług pośrednictwa danych lub uznanej organizacji altruizmu danych przekazanie przechowywanych na terenie Unii danych nieosobowych objętych zakresem stosowania niniejszego rozporządzenia lub udzielenie dostępu do tych danych uznaje się lub wykonuje w jakikolwiek sposób wyłącznie wtedy, gdy są oparte na umowie międzynarodowej, takiej jak traktat o pomocy prawnej, obowiązującej między państwem trzecim, które występuje z wnioskiem, a Unią, lub na umowie tego rodzaju między państwem trzecim, które występuje z wnioskiem, a państwem członkowskim.”;

b) w ust. 3 akapit pierwszy formuła wprowadzająca otrzymuje brzmienie:

„3. W przypadku braku umowy międzynarodowej, o której mowa w ust. 2, jeżeli dostawca usług przetwarzania danych, organ sektora publicznego udostępniający dane lub dokumenty zgodnie z rozdziałem VIIc sekcja 3, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych lub dokumentów zgodnie z rozdziałem VIIc sekcja 3, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych jest adresatem orzeczenia lub wyroku sądu lub trybunału państwa trzeciego lub decyzji organu administracyjnego państwa trzeciego nakazujących przekazanie przechowywanych na terenie Unii danych nieosobowych objętych zakresem stosowania niniejszego rozporządzenia lub udzielenie dostępu do tych danych, a zastosowanie się do takiego orzeczenia lub takiej decyzji wiązałoby się z ryzykiem naruszenia przez adresata prawa Unii lub prawa krajowego stosownego państwa członkowskiego, przekazanie takich danych temu

organowi państwa trzeciego lub udzielenie mu dostępu do takich danych odbywa się wyłącznie, gdy:”;

c) ust. 4 i 5 otrzymują brzmienie:

„4. Jeżeli spełnione są warunki określone w ust. 2 lub 3, dostawca usług przetwarzania danych, organ sektora publicznego udostępniający dane lub dokumenty zgodnie z rozdziałem VIIc sekcja 3, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych lub dokumentów zgodnie z rozdziałem VIIc sekcja 3, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych w odpowiedzi na wniosek dostarcza jak najmniejszą ilość danych dozwoloną w oparciu o racjonalną interpretację tego wniosku dokonaną przez dostawcę lub właściwy krajowy podmiot lub organ, o którym mowa w ust. 3 akapit drugi.

5. Przed zastosowaniem się do wniosku dostawca usług przetwarzania danych, organ sektora publicznego udostępniający dane lub dokumenty zgodnie z rozdziałem VIIc sekcja 3, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych lub dokumentów zgodnie z rozdziałem VIIc sekcja 3, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych informują osobę fizyczną lub prawną, której prawa i interesy mogą zostać naruszone, o wniosku organu państwa trzeciego o dostęp do jego danych, z wyjątkiem przypadków, w których wniosek służy do celów ścigania przestępstw i tak długo, jak jest to niezbędne do zachowania skuteczności działań w tym zakresie.”;

17. uchyla się art. 36 rozporządzenia;

18. dodaje się rozdziały VIIa, VIIb i VIIc w brzmieniu:

„ROZDZIAŁ VIIa
USŁUGI POŚREDNICTWA DANYCH I ORGANIZACJE ALTRUIZMU DANYCH

Artykuł 32a

Publiczne rejestry unijne

1) Komisja prowadzi i regularnie aktualizuje publiczne rejestry unijne:

   a) uznanych dostawców usług pośrednictwa danych; oraz

   b) uznanych organizacji altruizmu danych.

2) Dostawcy usług pośrednictwa danych zarejestrowani w publicznym rejestrze unijnym, o którym mowa w ust. 1 lit. a), mogą używać znaku »uznany w Unii dostawca usług pośrednictwa danych« w komunikacji pisemnej i ustnej, a także wspólnego logo, o którym mowa w ust. 4.

3) Organizacje altruizmu danych zarejestrowane w publicznym rejestrze unijnym, o którym mowa w ust. 1 lit. b), mogą używać znaku »uznana w Unii organizacja altruizmu danych« w komunikacji pisemnej i ustnej, a także wspólnego logo, o którym mowa w ust. 4.

4) Aby zapewnić łatwą rozpoznawalność uznanych w Unii dostawców usług pośrednictwa danych w całej Unii, Komisja jest uprawniona do przyjmowania aktów

wykonawczych ustanawiających projekt wspólnego logo. Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 46 ust. 1a.

Artykuł 32b

Właściwe organy odpowiedzialne za rejestrację dostawców usług pośrednictwa danych i organizacji altruizmu danych

1) Każde państwo członkowskie wyznacza właściwy organ lub właściwe organy odpowiedzialne za stosowanie i egzekwowanie niniejszego rozdziału zgodnie z art. 37 ust. 1.

2) Właściwe organy ustanawia się w taki sposób, aby zagwarantować ich niezależność od wszelkich uznanych dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych.

Artykuł 32c

Ogólne wymogi dotyczące rejestracji uznanych dostawców usług pośrednictwa danych

Aby kwalifikować się do rejestracji w publicznym rejestrze unijnym, o którym mowa w art. 32a ust. 1 lit. a), dostawca usług pośrednictwa danych musi spełniać wszystkie następujące wymogi:

a) nie wykorzystuje danych, w odniesieniu do których świadczy usługi pośrednictwa danych, do celów innych niż oddanie ich do dyspozycji użytkowników danych;

b) dane, które gromadzi w odniesieniu do jakiejkolwiek działalności osoby fizycznej lub prawnej do celów świadczenia usługi pośrednictwa danych, w tym dane dotyczące daty, godziny i geolokalizacji, czasu trwania działalności i połączeń z innymi osobami fizycznymi lub prawnymi ustanowionymi przez osobę korzystającą z usługi pośrednictwa danych, są wykorzystywane wyłącznie do rozwoju tej usługi pośrednictwa danych;

c) w przypadku gdy oferuje posiadaczom danych lub osobom, których dane dotyczą, dodatkowe narzędzia i usługi w konkretnym celu ułatwiania wymiany danych, takie jak tymczasowe przechowywanie, selekcjonowanie, konwersja, szyfrowanie, anonimizacja i pseudonimizacja, takie narzędzia i usługi wykorzystuje się wyłącznie na wyraźny wniosek lub za zgodą posiadacza danych lub osoby, której dane dotyczą;

d) w przypadku gdy dostawcy usług pośrednictwa danych, którzy nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami, oferują swoim klientom usługi o wartości dodanej inne niż usługi, o których mowa w lit. c), spełniają następujące warunki:

   (i) usługi o wartości dodanej są wyraźnie żądane przez użytkownika;

   (ii) dane nie są wykorzystywane do celów innych niż wykonanie usługi o wartości dodanej;

   (iii) usługi o wartości dodanej oferuje się za pośrednictwem funkcjonalnie odrębnego podmiotu;

   (iv) przedsiębiorstwo zamierzające oferować usługi o wartości dodanej nie zostało wskazane jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925;

   (v) warunki handlowe, w tym ceny, dotyczące świadczenia usług pośrednictwa danych na rzecz posiadacza danych lub użytkownika

danych nie zależą od tego, czy posiadacz danych lub użytkownik danych korzysta z usług o wartości dodanej świadczonych przez dostawcę usług pośrednictwa danych lub przez podmiot powiązany;

e) dostawca usług pośrednictwa danych oferujący usługi osobom, których dane dotyczą, działa w najlepszym interesie tych osób w przypadku gdy ułatwia wykonywanie przysługujących im praw, w szczególności zapewniając – zanim osoby, których dane dotyczą, wyrażą zgodę – informacje oraz, w stosownych przypadkach, doradztwo w zwięzły, przejrzysty, zrozumiały i łatwo dostępny sposób co do zamierzonego wykorzystywania danych przez użytkowników danych oraz co do standardowych warunków związanych z takim wykorzystywaniem.

Artykuł 32d

Ogólne wymogi dotyczące rejestracji uznanych organizacji altruizmu danych

Aby kwalifikować się do rejestracji w publicznym rejestrze unijnym, o którym mowa w art. 32a ust. 1 lit. b), organizacja altruizmu danych musi spełniać wszystkie następujące wymogi:

a) prowadzi działalność w zakresie altruizmu danych;

b) jest osobą prawną ustanowioną zgodnie z prawem krajowym do realizacji celów leżących w interesie ogólnym określonych, w stosownych przypadkach, w prawie krajowym;

c) prowadzi działalność o charakterze niekomercyjnym i jest prawnie niezależna od jakiegokolwiek podmiotu nastawionego na zysk;

d) prowadzi działalność w zakresie altruizmu danych, wykorzystując do tego celu strukturę funkcjonalnie odrębną od pozostałej działalności tego podmiotu.

Artykuł 32e

Rejestracja

1) Dostawca usług pośrednictwa danych, który spełnia wymogi określone w art. 32c, może złożyć wniosek o rejestrację w publicznym rejestrze unijnym uznanych dostawców usług pośrednictwa danych do właściwego organu, o którym mowa w art. 32b, w państwie członkowskim, w którym ma główną jednostkę organizacyjną.

Organizacja altruizmu danych, która spełnia wymogi określone w art. 32d, może złożyć wniosek o rejestrację w publicznym rejestrze unijnym uznanych organizacji altruizmu danych do właściwego organu, o którym mowa w art. 32b, w państwie członkowskim, w którym ma główną jednostkę organizacyjną.

2) Dostawcy usług pośrednictwa danych i organizacje altruizmu danych, które nie mają głównej jednostki organizacyjnej w Unii, wyznaczają przedstawiciela prawnego w jednym z państw członkowskich. Przedstawiciel prawny jest upoważniony do tego, by właściwe organy lub osoby, których dane dotyczą, i posiadacze danych zwracali się do niego, oprócz lub zamiast do dostawcy usług pośrednictwa danych lub organizacji altruizmu danych. Przedstawiciel prawny współpracuje z właściwymi organami i na żądanie szczegółowo przedstawia im działania i przepisy wprowadzone przez dostawcę usług pośrednictwa danych lub organizację altruizmu danych w celu zapewnienia przestrzegania niniejszego rozporządzenia.

Uznaje się, że dostawca usług pośrednictwa danych lub organizacja altruizmu danych podlegają jurysdykcji państwa członkowskiego, w którym znajduje się przedstawiciel prawny. Wyznaczenie przedstawiciela prawnego pozostaje bez

uszczerbku dla wszelkich działań prawnych, które można podjąć przeciwko dostawcy usług pośrednictwa danych lub organizacji altruizmu danych.

3) Właściwe organy ustanawiają niezbędne formularze wniosków.

4) W przypadku gdy dostawca usług pośrednictwa danych przedłożył wszystkie niezbędne informacje zgodnie z ust. 3 niniejszego artykułu i spełnia wymogi określone w art. 32c, właściwy organ w terminie 12 tygodni od otrzymania wniosku o rejestrację podejmuje decyzję, czy dostawca spełnia kryteria określone w art. 32c. Jeżeli dostawca spełnia kryteria, właściwy organ przekazuje odpowiednie informacje Komisji, która rejestruje dostawców w publicznym rejestrze unijnym jako uznanych dostawców usług pośrednictwa danych.

Akapit pierwszy ma również zastosowanie w przypadku, gdy organizacja altruizmu danych przedłożyła wszystkie niezbędne informacje zgodnie z ust. 2 i spełnia wymogi rejestracji określone w art. 32d.

Rejestracja w publicznym rejestrze unijnym jest ważna we wszystkich państwach członkowskich.

5) Właściwy organ może pobierać opłaty za rejestrację zgodnie z prawem krajowym. Opłaty te są proporcjonalne i obiektywne oraz opierają się na kosztach administracyjnych związanych z monitorowaniem zgodności. W przypadku spółek o małej i średniej kapitalizacji, małych i średnich przedsiębiorstw oraz przedsiębiorstw typu start-up właściwy organ może pobierać obniżoną opłatę lub zrezygnować z opłaty.

6) Zarejestrowane podmioty powiadamiają właściwy organ o wszelkich późniejszych zmianach w informacjach przekazanych w trakcie procesu składania wniosku lub o zaprzestaniu działalności w zakresie pośrednictwa danych lub altruizmu danych w Unii.

7) Właściwy organ niezwłocznie i drogą elektroniczną powiadamia Komisję o każdym powiadomieniu na podstawie ust. 6. Komisja bez zbędnej zwłoki aktualizuje publiczny rejestr unijny.

Artykuł 32f

Obowiązki uznanych organizacji altruizmu danych

1) Uznane organizacje altruizmu danych informują w jasny i łatwo zrozumiały sposób osoby, których dane dotyczą, lub posiadaczy danych, przed przetwarzaniem ich danych, o następujących kwestiach:

a) celach leżących w interesie ogólnym oraz, w stosownych przypadkach, o konkretnym, wyraźnym i zgodnym z prawem celu przetwarzania danych osobowych, dla których uznana organizacja altruizmu danych pozwala na przetwarzanie danych osób, których dane dotyczą, lub posiadaczy danych przez użytkowników danych;

b) miejscu przetwarzania oraz celach leżących w interesie ogólnym, dla których uznana organizacja altruizmu danych pozwala na przetwarzanie w państwie trzecim, jeżeli przetwarzania dokonuje uznana organizacja altruizmu danych.

2) Uznane organizacje altruizmu danych nie mogą wykorzystywać danych do celów innych niż cele leżące w interesie ogólnym, w odniesieniu do których osoba, której dane dotyczą, lub posiadacz danych zezwolili na przetwarzanie. Uznana organizacja

altruizmu danych nie może stosować wprowadzających w błąd praktyk marketingowych, by nakłaniać do przekazywania danych.

3) Uznane organizacje altruizmu danych zapewniają środki elektroniczne umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnionych przez posiadaczy danych, a także ich wycofanie.

4) Uznane organizacje altruizmu danych niezwłocznie informują posiadaczy danych, w przypadku gdy nastąpiły niedozwolone przekazanie, dostęp lub wykorzystanie danych nieosobowych, którymi się podzieliły.

5) W przypadku gdy uznane organizacje altruizmu danych ułatwiają osobom trzecim przetwarzanie danych, w tym poprzez zapewnianie narzędzi umożliwiających uzyskanie zgody od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnionych przez posiadaczy danych, określają – w stosownych przypadkach – państwo trzecie, w którym ma się odbywać wykorzystywanie danych.

Artykuł 32g

Monitorowanie zgodności

1) Właściwe organy, o których mowa w art. 32b, z własnej inicjatywy albo na wniosek osoby fizycznej lub prawnej, monitorują i nadzorują, czy uznani dostawcy usług pośrednictwa danych i uznane organizacje altruizmu danych spełniają wymogi określone w niniejszym rozdziale, w tym czy nadal spełniają określone w nim wymogi dotyczące rejestracji.

2) Właściwe organy są uprawnione do wnioskowania od uznanych dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych, lub ich przedstawicieli prawnych, wszelkich informacji niezbędnych do weryfikacji zgodności z wymogami określonymi w niniejszym rozdziale. Każdy wniosek o informacje musi być proporcjonalny do wykonywanego zadania i musi być uzasadniony.

3) W przypadku ustalenia przez właściwy organ, że uznany dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych nie spełniają co najmniej jednego wymogu określonego w niniejszym rozdziale, organ ten powiadamia dany podmiot lub jego przedstawiciela prawnego o swoich ustaleniach i daje mu możliwość przedstawienia swojego stanowiska w terminie 30 dni od dnia otrzymania powiadomienia.

4) Właściwy organ uprawniony jest do żądania zaprzestania nieprzestrzegania przepisów, o którym mowa w ust. 3, niezwłocznie albo w rozsądnym terminie, a także przyjmuje odpowiednie i proporcjonalne środki służące zapewnieniu przestrzegania przepisów.

5) Jeżeli uznany dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych nie spełnia co najmniej jednego wymogu określonego w niniejszym rozdziale, nawet po otrzymaniu powiadomienia zgodnie z ust. 3, podmiot ten:

   a) traci prawo do używania znaku, o którym mowa w art. 32a, w komunikacji pisemnej i ustnej;

   b) jest usuwany z publicznego rejestru unijnego, o którym mowa w art. 32a.

Każda decyzja o cofnięciu prawa do używania znaku, o którym mowa w akapicie pierwszym lit. a), jest podawana do wiadomości publicznej przez właściwy organ.

„ROZDZIAŁ VIIb

Swobodny przepływ danych nieosobowych w Unii

„Artykuł 32h

Zakaz stosowania wymogów dotyczących lokalizacji w odniesieniu do danych nieosobowych w Unii

1) Zakazuje się stosowania wymogów dotyczących lokalizacji danych w odniesieniu do danych nieosobowych, chyba że są one uzasadnione względami bezpieczeństwa publicznego zgodnie z zasadą proporcjonalności lub ustanowione na podstawie prawa Unii.

2) Państwa członkowskie niezwłocznie przekazują Komisji każdy projekt aktu, który wprowadza nowy wymóg dotyczący lokalizacji danych lub zmiany w istniejącym wymogu dotyczącym lokalizacji danych zgodnie z procedurami określonymi w art. 5, 6 i 7 dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady.

ROZDZIAŁ VIIc

Ponowne wykorzystywanie danych i dokumentów będących w posiadaniu organów sektora publicznego

SEKCJA 1

PRZEPISY OGÓLNE

Artykuł 32i

Przedmiot i zakres

1) W niniejszym rozdziale ustanawia się zbiór przepisów regulujących ponowne wykorzystywanie oraz praktyczne ustalenia ułatwiające ponowne wykorzystywanie:

   a) istniejących danych i dokumentów będących w posiadaniu organów sektora publicznego państw członkowskich, w tym niektórych kategorii danych chronionych;

   b) istniejących danych i dokumentów będących w posiadaniu przedsiębiorstw publicznych, które:

      (i) prowadzą działalność w obszarach, o których mowa w rozdziale II dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE;

      (ii) działają w charakterze podmiotów świadczących usługi publiczne zgodnie z art. 2 rozporządzenia (WE) nr 1370/2007 Parlamentu Europejskiego i Rady;

(iii) działają w charakterze przewoźników lotniczych wykonujących obowiązki użyteczności publicznej zgodnie z art. 16 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1008/2008; lub

(iv) działają w charakterze armatorów Wspólnoty wykonujących zobowiązania z tytułu świadczenia usług publicznych zgodnie z art. 4 rozporządzenia Rady (EWG) nr 3577/92;

c) danych badawczych, na warunkach określonych w art. 32t.

2) Niniejszy rozdział nie ma zastosowania do:

a) danych i dokumentów, których wydawanie jest działalnością wykraczającą poza zakres zadań publicznych zainteresowanych organów sektora publicznego określonych przepisami ustawowymi lub innymi wiążącymi przepisami w państwie członkowskim lub, w przypadku braku takich przepisów, określonych zgodnie z powszechną praktyką administracyjną w zainteresowanym państwie członkowskim, o ile zakres zadań publicznych jest przejrzysty i podlega przeglądowi;

b) danych i dokumentów będących w posiadaniu przedsiębiorstw publicznych oraz:

(i) wyprodukowanych poza zakresem świadczenia usług w interesie ogólnym, jak określono w przepisach ustawowych lub innych wiążących przepisach państwa członkowskiego;

(ii) związanych z działalnością bezpośrednio narażoną na konkurencję i z tego względu – zgodnie z art. 34 dyrektywy 2014/25/UE – nieobjętych zasadami udzielania zamówień publicznych;

c) danych i dokumentów, takich jak dane wrażliwe, które są wyłączone z dostępu na podstawie systemów dostępu państwa członkowskiego ze względu na ochronę bezpieczeństwa narodowego (mianowicie bezpieczeństwa państwa), obronność lub bezpieczeństwo publiczne;

d) danych i dokumentów będących w posiadaniu publicznych nadawców radiowych i telewizyjnych oraz ich jednostek zależnych, a także innych podmiotów lub ich jednostek zależnych realizujących misję nadawców publicznych;

3) Sekcja 2 niniejszego rozdziału nie ma zastosowania do:

a) danych i dokumentów, takich jak dane lub dokumenty wrażliwe, które są wyłączone z dostępu na podstawie systemów dostępu państwa członkowskiego, w tym ze względu na:

(i) poufność informacji statystycznych;

(ii) poufność informacji handlowych (w tym tajemnicę handlową, zawodową lub przedsiębiorstwa);

b) danych lub dokumentów, do których dostęp jest ograniczony na mocy systemów dostępu państw członkowskich:

(i) w tym przypadków, w których obywatele lub podmioty prawne muszą udowodnić szczególny interes w uzyskaniu dostępu do dokumentów;

(ii) ze względu na ochronę danych osobowych oraz części danych lub dokumentów dostępnych na mocy tych systemów, które zawierają dane

osobowe, których ponowne wykorzystywanie zostało określone w prawie jako niezgodne z prawem dotyczącym ochrony osób fizycznych w związku z przetwarzaniem danych osobowych lub jako naruszające ochronę prywatności i integralności osoby fizycznej, w szczególności zgodnie z prawem Unii lub prawem krajowym dotyczącym ochrony danych osobowych; logo, herbów i symboli;

c) danych lub dokumentów, do których prawa własności intelektualnej należą do osób trzecich;

d) danych lub dokumentów będących w posiadaniu instytucji kulturalnych innych niż biblioteki, w tym biblioteki uniwersyteckie, muzea i archiwa;

e) danych lub dokumentów będących w posiadaniu instytucji edukacyjnych na poziomie średnim i niższym oraz – w przypadku wszystkich innych instytucji edukacyjnych – danych innych niż te, o których mowa w ust. 1 lit. c);

f) danych lub dokumentów innych niż te, o których mowa w ust. 1 lit. c), będących w posiadaniu organizacji prowadzących badania naukowe i organizacji finansujących badania naukowe, w tym organizacji utworzonych na potrzeby transferu wyników badań naukowych;

g) danych lub dokumentów, do których dostęp jest wykluczony lub ograniczony ze względu na informacje dotyczące ochrony podmiotu krytycznego lub infrastruktury krytycznej zdefiniowanych w art. 2 pkt 1 i 4 dyrektywy (UE) 2022/2557.

4) Sekcja 3 niniejszego rozdziału nie ma zastosowania do:

a) danych i dokumentów, które nie są niektórymi kategoriami danych chronionych;

b) danych lub dokumentów będących w posiadaniu przedsiębiorstw publicznych;

c) danych lub dokumentów będących w posiadaniu instytucji kulturalnych i placówek edukacyjnych;

d) danych i dokumentów objętych sekcją 2 niniejszego rozdziału.

5) Niniejszy rozdział opiera się na unijnych i krajowych systemach dostępu i pozostaje bez uszczerbku dla tych systemów, w szczególności w odniesieniu do udzielania dostępu do dokumentów urzędowych i ich ujawniania.

6) Obowiązki nałożone zgodnie z niniejszym rozdziałem należy stosować tylko w zakresie, w jakim są zgodne z postanowieniami umów międzynarodowych o ochronie praw własności intelektualnej, w szczególności z Konwencją berneńską o ochronie dzieł literackich i artystycznych (»konwencja berneńska«), Porozumieniem w sprawie handlowych aspektów praw własności intelektualnej (»porozumienie TRIPS«) i Traktatem Światowej Organizacji Własności Intelektualnej o prawie autorskim (»WCT«).

7) Prawo producenta bazy danych przewidziane w art. 7 ust. 1 dyrektywy 96/9/WE nie może być wykonywane przez organy sektora publicznego w celu uniemożliwienia ponownego wykorzystywania danych i dokumentów lub ograniczenia ponownego wykorzystywania w zakresie wykraczającym poza ograniczenia określone w niniejszym rozdziale.

8) Niniejszy rozdział reguluje ponowne wykorzystywanie istniejących danych i dokumentów będących w posiadaniu organów sektora publicznego i przedsiębiorstw publicznych państw członkowskich, w tym danych i dokumentów, do których ma zastosowanie dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady.

9) Niniejszy rozdział pozostaje bez uszczerbku dla prawa Unii i prawa krajowego oraz umów międzynarodowych, których Unia lub państwa członkowskie są stronami, dotyczących ochrony kategorii danych lub dokumentów, o których mowa w art. 2 pkt 54.

Artykuł 32j

Niedyskryminacja

1) Wszelkie mające zastosowanie warunki ponownego wykorzystywania danych lub dokumentów muszą być niedyskryminacyjne, przejrzyste, proporcjonalne i obiektywnie uzasadnione w odniesieniu do kategorii danych lub dokumentów i celów ponownego wykorzystywania oraz charakteru danych lub dokumentów, których ponowne wykorzystywanie jest dozwolone. Warunki te nie mogą być stosowane do ograniczania konkurencji. Zasada ta ma również zastosowanie do porównywalnych kategorii ponownego wykorzystywania, w tym do ponownego wykorzystywania transgranicznego.

2) Jeśli dane lub dokumenty są ponownie wykorzystywane przez organ sektora publicznego jako materiał wejściowy służący jego działalności komercyjnej leżącej poza zakresem jego zadań publicznych, przy dostarczaniu danych lub dokumentów przeznaczonych do tej działalności stosuje się takie same opłaty i inne warunki, jakie stosuje się w odniesieniu do innych ponownych użytkowników.

Artykuł 32k

Uzgodnienia dotyczące wyłączności

1) Ponowne wykorzystywanie danych lub dokumentów jest otwarte dla wszystkich potencjalnych uczestników rynku, nawet jeżeli jeden lub kilku jego uczestników już wykorzystuje oparte na tych danych lub dokumentach produkty o wartości dodanej. Zakazane są umowy lub inne uzgodnienia lub praktyki dotyczące ponownego wykorzystywania danych lub dokumentów, których celem lub skutkiem jest przyznanie praw wyłącznych lub ograniczenie dostępności danych lub dokumentów do ponownego wykorzystywania przez podmioty inne niż strony takich umów, uzgodnień lub praktyk.

2) Na zasadzie odstępstwa od ust. 1, w przypadku gdy prawo wyłączne jest niezbędne do świadczenia usługi w interesie ogólnym, prawo takie można przyznać w zakresie niezbędnym do świadczenia usługi lub dostarczania produktu na następujących warunkach:

   a) prawo wyłączne przyznaje się w drodze aktu administracyjnego lub umowy zgodnie z mającym zastosowanie prawem unijnym i krajowym oraz zgodnie z zasadami przejrzystości, równego traktowania i niedyskryminacji;

   b) umowy przyznające prawo wyłączne, w tym powody, dla których konieczne jest przyznanie takiego prawa, są przejrzyste i podawane do wiadomości

publicznej w internecie, w formie zgodnej z odpowiednim prawem Unii dotyczącym zamówień publicznych i prawem krajowym;

c) z wyjątkiem praw wyłącznych związanych z digitalizacją zasobów kultury ważność powodu przyznania praw wyłącznych dotyczących danych i dokumentów objętych zakresem sekcji 2 podlega regularnemu przeglądowi, a w każdym razie przeglądowi co trzy lata;

d) uzgodnienia dotyczące wyłączności zawarte w dniu 16 lipca 2019 r. lub po tej dacie podaje się do publicznej wiadomości w internecie na co najmniej dwa miesiące przed ich wejściem w życie. Ostateczne warunki takich uzgodnień muszą być przejrzyste i podawane do publicznej wiadomości w internecie.

3) Na zasadzie odstępstwa od ust. 1, jeżeli prawo wyłączne dotyczy digitalizacji zasobów kultury, okres wyłączności co do zasady nie przekracza 10 lat. W przypadku gdy okres ten przekracza 10 lat, musi on być zgodny z mającym zastosowanie prawem unijnym i krajowym oraz podlega przeglądowi w 11. roku, a następnie, w stosownych przypadkach, co siedem lat.

4) W przypadku prawa wyłącznego, o którym mowa w ust. 3, w ramach tych uzgodnień zainteresowany organ sektora publicznego otrzymuje bezpłatnie egzemplarz poddanych digitalizacji zasobów kultury. Egzemplarz ten jest udostępniany do ponownego wykorzystywania z końcem okresu obowiązywania prawa wyłącznego.

5) W przypadku niektórych kategorii danych chronionych okres obowiązywania prawa wyłącznego do ponownego wykorzystywania danych nie może przekraczać 12 miesięcy. W przypadku zawarcia umowy okres obowiązywania zawartej umowy musi być taki sam jak okres, na który przyznano prawo wyłączne.

6) Umowy lub inne uzgodnienia lub praktyki, które, choć wprost nie przyznają prawa wyłącznego, mają na celu ograniczenie dostępności danych i dokumentów do ponownego wykorzystywania zgodnie z zakresem sekcji 2 przez podmioty inne niż strony takich uzgodnień, podaje się do wiadomości publicznej w internecie na co najmniej dwa miesiące przed ich wejściem w życie. Wpływ takich uzgodnień prawnych lub praktycznych na dostępność danych do ponownego wykorzystywania podlega regularnym przeglądom, a w każdym razie przeglądu dokonuje się co trzy lata. Ostateczne warunki takich uzgodnień są przejrzyste i podawane do publicznej wiadomości w internecie.

7) W odniesieniu do istniejących uzgodnień dotyczących wyłączności stosuje się następujące zasady:

a) uzgodnienia dotyczące wyłączności odnoszące się do danych i dokumentów objętych zakresem sekcji 2, istniejące w dniu 17 lipca 2013 r., które nie kwalifikują się do wyjątków określonych w ust. 2 i 3 oraz które zostały zawarte przez organy sektora publicznego, wygasają wraz z końcem obowiązywania umowy, a w każdym razie nie później niż w dniu 18 lipca 2043 r.;

b) uzgodnienia dotyczące wyłączności odnoszące się do danych i dokumentów objętych zakresem sekcji 2, istniejące w dniu 16 lipca 2019 r., które nie kwalifikują się do wyjątków określonych w ust. 2 i 3 oraz które zostały zawarte przez przedsiębiorstwa publiczne, wygasają wraz z końcem obowiązywania umowy, a w każdym razie nie później niż w dniu 17 lipca 2049 r.

Artykuł 32l

Ogólne zasady dotyczące pobierania opłat

1) Wszelkie opłaty określone w sekcji 2 lub sekcji 3 muszą być przejrzyste, niedyskryminacyjne, proporcjonalne i obiektywnie uzasadnione oraz nie mogą ograniczać konkurencji.

2) W przypadku standardowych opłat za ponowne wykorzystywanie danych lub dokumentów mające zastosowanie warunki i faktyczne kwoty opłat, w tym podstawa ich obliczania, są określane z wyprzedzeniem i publikowane – w miarę możliwości i stosownie do przypadku – przy wykorzystaniu środków elektronicznych.

3) W przypadku opłat za ponowne wykorzystywanie, innych niż te, o których mowa w ust. 1, czynniki, które są brane pod uwagę przy obliczaniu tych opłat, określa się z góry. Dany posiadacz danych lub dokumentów przedstawia również, na żądanie, sposób obliczenia tych opłat w odniesieniu do konkretnego wniosku o ponowne wykorzystywanie.

4) Podmioty sektora publicznego zapewniają możliwość uiszczania opłat także przez internet za pośrednictwem powszechnie dostępnej transgranicznej usługi płatniczej, bez dyskryminacji ze względu na miejsce prowadzenia działalności przez dostawcę usług płatniczych, miejsce wydania instrumentu płatniczego lub lokalizację rachunku płatniczego w Unii.

Artykuł 32m

Informacje na temat środków odwoławczych

Organy sektora publicznego zapewniają, aby wnioskujący o ponowne wykorzystywanie danych lub dokumentów byli informowani o dostępnych środkach odwoławczych od decyzji lub praktyk, które na nich wpływają.

SEKCJA 2

PONOWNE WYKORZYSTYWANIE OTWARTYCH DANYCH PUBLICZNYCH

Podsekcja 1 Zakres i zasady ogólne

Artykuł 32n

Ogólna zasada ponownego wykorzystywania otwartych danych publicznych

1) Dane lub dokumenty objęte zakresem niniejszej sekcji można ponownie wykorzystywać do celów komercyjnych lub niekomercyjnych zgodnie z sekcją 1 i sekcją 2 podsekcja 3.

2) W przypadku danych lub dokumentów, do których prawa własności intelektualnej mają biblioteki, w tym biblioteki uniwersyteckie, muzea i archiwa, oraz danych lub dokumentów będących w posiadaniu przedsiębiorstw publicznych, w sytuacji gdy dozwolone jest ponowne wykorzystywanie takich danych lub dokumentów, te dane lub dokumenty można ponownie wykorzystywać do celów komercyjnych lub niekomercyjnych zgodnie z sekcją 1 i sekcją 2 podsekcja 3.

Podsekcja 2

Wnioski o ponowne wykorzystywanie

Artykuł 32o

Przetwarzanie wniosków o ponowne wykorzystywanie

1) Organy sektora publicznego przetwarzają, w miarę możliwości i stosownie do przypadku przy wykorzystaniu środków elektronicznych, wnioski o ponowne wykorzystywanie i udostępniają wnioskodawcy dokumenty do ponownego wykorzystywania lub, jeżeli potrzebna jest licencja, przedstawiają wnioskodawcy końcową ofertę licencji w rozsądnym terminie zgodnym z terminami określonymi dla przetwarzania wniosków o dostęp do danych lub dokumentów.

2) Jeżeli nie określono takich terminów ani nie ustanowiono innych przepisów regulujących terminowe udostępnianie danych lub dokumentów, organy sektora publicznego rozpatrują wnioski i dostarczają wnioskodawcy dane lub dokumenty do ponownego wykorzystywania lub, jeżeli potrzebna jest licencja, przedstawiają wnioskodawcy końcową ofertę licencji możliwie jak najszybciej, a w każdym przypadku w ciągu 20 dni roboczych od otrzymania wniosku. W przypadku obszernych lub złożonych wniosków termin ten może być przedłużony o kolejne 20 dni roboczych. W takich przypadkach możliwie jak najszybciej, a w każdym razie w ciągu trzech tygodni od daty pierwotnego wniosku zawiadamia się wnioskodawcę, że przetwarzanie jego wniosku wymaga więcej czasu, wskazując przyczyny.

3) W przypadku decyzji odmownej organy sektora publicznego informują wnioskodawcę o powodach odmowy w oparciu o odpowiednie przepisy systemu dostępu tego państwa członkowskiego lub przepisy niniejszego rozporządzenia, w szczególności art. 32i ust. 2 lit. a)–c) oraz art. 32i ust. 3 lit. a)–d) lub art. 32n (sekcja dotycząca zasady ogólnej dyrektywy w sprawie otwartych danych). Jeżeli podstawą decyzji odmownej jest art. 32i ust. 3 lit. d), organ sektora publicznego zamieszcza odniesienie do osoby fizycznej lub prawnej, do której należą prawa własności intelektualnej (jeżeli jest znana), lub do licencjodawcy, od którego organ sektora publicznego uzyskał dany materiał. Do zamieszczenia takiego odniesienia nie są zobowiązane biblioteki, w tym biblioteki uniwersyteckie, muzea ani archiwa.

4) Środki odwoławcze obejmują możliwość kontroli przez bezstronny organ odwoławczy posiadający odpowiednią wiedzę specjalistyczną – taki jak krajowy organ ochrony konkurencji, odpowiedni organ regulujący dostęp do danych lub dokumentów, organ nadzorczy ustanowiony zgodnie z rozporządzeniem (UE) 2016/679 lub krajowy organ sądowy – którego decyzje są wiążące dla danego organu sektora publicznego.

5) Na potrzeby niniejszego artykułu państwa członkowskie ustanawiają rozwiązania praktyczne ułatwiające skuteczne ponowne wykorzystywanie danych lub dokumentów. Rozwiązania te mogą w szczególności obejmować sposoby udostępniania odpowiednich informacji o prawach przewidzianych w niniejszym rozporządzeniu oraz sposoby udzielania stosownej pomocy i porad.

6) Niniejszy artykuł nie ma zastosowania do następujących podmiotów:

   a) przedsiębiorstw publicznych;

   b) instytucji edukacyjnych, organizacji prowadzących badania naukowe i organizacji finansujących badania naukowe.

Podsekcja 3

Warunki ponownego wykorzystywania

Artykuł 32p

Dostępne formaty

1) Bez uszczerbku dla podsekcji 5 organy sektora publicznego i przedsiębiorstwa publiczne udostępniają swoje dane lub dokumenty w dowolnym istniejącym formacie lub języku, a w miarę możliwości i stosownie do przypadku, za pomocą środków elektronicznych – w formatach, które są otwarte, nadają się do odczytu maszynowego, są dostępne, możliwe do znalezienia i możliwe do ponownego wykorzystywania, wraz z ich metadanymi. W miarę możliwości zarówno format, jak i metadane muszą być zgodne z otwartymi standardami formalnymi.

2) Państwa członkowskie zachęcają organy sektora publicznego i przedsiębiorstwa publiczne, by produkowały i udostępniały dane lub dokumenty objęte zakresem stosowania niniejszej sekcji zgodnie z zasadą »otwartości w fazie projektowania i otwartości domyślnej«.

3) Ust. 1 nie zobowiązuje organów sektora publicznego do tworzenia lub dostosowywania dokumentów ani do dostarczania wyciągów z danych lub dokumentów, aby zapewnić zgodność z przepisami tego ustępu, w przypadku gdy wymagałoby to nieproporcjonalnie dużego wysiłku, wykraczającego poza prostą czynność.

4) Od organów sektora publicznego nie wymaga się, by kontynuowały produkowanie i przechowywanie określonego rodzaju danych lub dokumentów w celu ponownego ich wykorzystywania przez organizację sektora prywatnego lub publicznego.

5) Organy sektora publicznego udostępniają dane dynamiczne do ponownego wykorzystywania natychmiast po ich zgromadzeniu, za pośrednictwem odpowiednich interfejsów API, oraz, w odpowiednich przypadkach, do zbiorczego pobrania.

6) Jeżeli udostępnianie danych dynamicznych do ponownego wykorzystywania natychmiast po ich zgromadzeniu, o czym mowa w ust. 5, przekraczałoby możliwości finansowe i techniczne organu sektora publicznego, stanowiąc tym samym nieproporcjonalnie duży wysiłek, te dane dynamiczne udostępnia się do ponownego wykorzystywania w terminie lub z czasowymi ograniczeniami technicznymi, które nie powodują nadmiernego ograniczenia możliwości wykorzystania ich potencjału gospodarczego i społecznego.

7) Ust. 1–6 mają zastosowanie do istniejących danych lub dokumentów będących w posiadaniu przedsiębiorstw publicznych, które to dokumenty są dostępne do ponownego wykorzystywania.

8) Zbiory danych o wysokiej wartości, których wykaz określa się zgodnie z art. 32v ust. 1, są udostępniane do ponownego wykorzystywania w formacie nadającym się do odczytu maszynowego, za pośrednictwem odpowiednich interfejsów API oraz, w odpowiednich przypadkach, do zbiorczego pobrania.

Artykuł 32q

Zasady pobierania opłat za otwarte dane publiczne

1) Ponowne wykorzystywanie danych lub dokumentów objętych zakresem niniejszej sekcji jest bezpłatne. Można jednak zezwolić na odzyskanie kosztów krańcowych przez organ sektora publicznego będący w posiadaniu danych, poniesionych w związku z reprodukowaniem, dostarczaniem i rozpowszechnianiem takich danych

lub dokumentów, a także w związku z anonimizacją danych osobowych oraz środkami przedsięwziętymi w celu ochrony poufnych informacji handlowych.

2) Ust. 1 nie stosuje się do następujących podmiotów:

   a) organów sektora publicznego, które muszą uzyskiwać dochody w celu pokrycia znacznej części kosztów związanych z wykonywaniem swoich zadań publicznych;

   b) bibliotek, w tym bibliotek uniwersyteckich, muzeów i archiwów;

   c) przedsiębiorstw publicznych.

3) Państwa członkowskie publikują w internecie wykaz organów sektora publicznego, o których mowa w ust. 2 lit. a).

4) W przypadkach, o których mowa w ust. 2 lit. a) i c), łączne opłaty oblicza się na podstawie obiektywnych, przejrzystych i sprawdzalnych kryteriów. Takie kryteria zostaną określone przez państwa członkowskie. Całkowity przychód z wydawania danych lub dokumentów i zezwalania na ich ponowne wykorzystywanie we właściwym okresie obrachunkowym nie może przekraczać kosztów ich gromadzenia, produkowania, reprodukowania, rozpowszechniania i przechowywania danych, z uwzględnieniem rozsądnego zwrotu z inwestycji, oraz – w stosownych przypadkach – anonimizacji danych osobowych oraz kosztów środków zastosowanych w celu ochrony poufnych informacji handlowych. Opłaty są obliczane zgodnie z mającymi zastosowanie zasadami rachunkowości.

5) Jeżeli opłaty pobierane są przez organy sektora publicznego, o których mowa w ust. 2 lit. b), całkowity przychód z wydawania dokumentów i zezwalania na ich ponowne wykorzystywanie we właściwym okresie obrachunkowym nie może przekraczać kosztów gromadzenia, produkowania, reprodukowania, rozpowszechniania i zabezpieczenia, przechowywania danych i weryfikacji praw oraz – w stosownych przypadkach – kosztów anonimizacji danych osobowych oraz kosztów środków zastosowanych w celu ochrony poufnych informacji handlowych, z uwzględnieniem rozsądnego zwrotu z inwestycji. Opłaty są obliczane zgodnie z zasadami rachunkowości mającymi zastosowanie do danych organów sektora publicznego.

6) Organy sektora publicznego mogą ustanowić wyższe opłaty za ponowne wykorzystywanie danych i dokumentów przez bardzo duże przedsiębiorstwa niż opłaty przewidziane w ust. 1, 4 i 5. Wszelkie takie opłaty muszą być proporcjonalne i oparte na obiektywnych kryteriach, z uwzględnieniem siły gospodarczej danego podmiotu lub jego zdolności do pozyskiwania danych, w tym w szczególności wskazania go jako strażnika dostępu na podstawie rozporządzenia (UE) 2022/1925. Oprócz elementów wymienionych w ust. 1 niniejszego artykułu takie opłaty mogą pokrywać koszty gromadzenia, produkowania, reprodukowania, rozpowszechniania i przechowywania danych oraz, w stosownych przypadkach, koszty anonimizacji lub środków na potrzeby ochrony poufności danych lub dokumentów, wraz z rozsądnym zwrotem z inwestycji.

7) Ponowne wykorzystywanie jest dla użytkownika bezpłatne w przypadku:

   a) zbiorów danych o wysokiej wartości, których wykaz określa się zgodnie z art. 32v ust. 1, z zastrzeżeniem ust. 3, 4 i 5 tego artykułu;

   b) danych badawczych, o których mowa w art. 32i ust. 1 lit. c).

Artykuł 32r

Licencje standardowe

1) Ponowne wykorzystywanie danych lub dokumentów nie podlega warunkom, chyba że warunki takie są obiektywne, proporcjonalne, niedyskryminacyjne i uzasadnione celem interesu publicznego.

2) Jeżeli ponowne wykorzystywanie podlega warunkom, warunki te nie mogą niepotrzebnie ograniczać możliwości ponownego wykorzystywania i nie mogą być stosowane do ograniczania konkurencji.

3) W państwach członkowskich, w których stosowane są licencje, organy sektora publicznego zapewniają, aby licencje standardowe na ponowne wykorzystywanie danych lub dokumentów sektora publicznego, które można dostosować do określonych wniosków o licencje, były dostępne w formacie cyfrowym i mogły być przetwarzane elektronicznie.

4) Organy sektora publicznego mogą ustanowić specjalne warunki ponownego wykorzystywania danych i dokumentów przez bardzo duże przedsiębiorstwa. Warunki te są proporcjonalne i powinny opierać się na obiektywnych kryteriach. Ustala się je z uwzględnieniem siły gospodarczej lub zdolności podmiotu do pozyskiwania danych, w tym w szczególności wskazania go jako strażnika dostępu na podstawie rozporządzenia (UE) 2022/1925.

Artykuł 32s

Ustalenia praktyczne

1) Państwa członkowskie wprowadzają ustalenia praktyczne ułatwiające wyszukiwanie danych lub dokumentów dostępnych do ponownego wykorzystywania, takie jak wykazy najważniejszych zasobów danych lub dokumentów wraz z odpowiednimi metadanymi, dostępne – jeżeli jest to możliwe i w stosownych przypadkach – w internecie i w formatach nadających się do odczytu maszynowego, oraz portale połączone z wykazami zasobów. W miarę możliwości państwa członkowskie ułatwiają wielojęzyczne wyszukiwanie danych lub dokumentów, w szczególności poprzez umożliwienie agregacji metadanych na szczeblu Unii.

Państwa członkowskie zachęcają także organy sektora publicznego do wprowadzania uzgodnień praktycznych ułatwiających zachowanie danych lub dokumentów dostępnych do ponownego wykorzystywania.

2) Państwa członkowskie we współpracy z Komisją podejmują dalsze starania w celu uproszczenia dostępu do zbiorów danych, w szczególności przez stworzenie pojedynczego punktu dostępu oraz stopniowe udostępnianie odpowiednich zbiorów danych będących w posiadaniu organów sektora publicznego, w odniesieniu do dokumentów, do których niniejsza sekcja ma zastosowanie, jak również w odniesieniu do danych będących w posiadaniu instytucji unijnych, w formatach, które są dostępne, możliwe do znalezienia i możliwe do ponownego wykorzystywania za pomocą środków elektronicznych.

Podsekcja 4

Dane badawcze

Artykuł 32t

Dane badawcze

1) Państwa członkowskie wspierają dostępność danych badawczych poprzez przyjęcie polityki krajowej oraz podejmowanie odpowiednich działań mających na celu zapewnienie powszechnej dostępności danych badawczych finansowanych ze środków publicznych („polityka otwartego dostępu”), zgodnie z zasadą „otwartości domyślnej” i zgodnie z zasadami FAIR. W tym kontekście należycie uwzględnia się kwestie związane z prawami własności intelektualnej, ochroną danych osobowych i poufnością, bezpieczeństwem i uzasadnionymi interesami handlowymi zgodnie z zasadą „otwarty jak to najbardziej możliwe, zamknięty jak to konieczne”. Wspomnianą politykę otwartego dostępu kieruje się do organizacji prowadzących badania naukowe i organizacji finansujących badania naukowe.

2) Bez uszczerbku dla art. 32n ust. 3 lit. d) dane badawcze udostępnia się do ponownego wykorzystywania w celach komercyjnych lub niekomercyjnych zgodnie z sekcją 1 i sekcją 2 podsekcja 3, w zakresie, w jakim dane te są finansowane ze środków publicznych i zostały już publicznie udostępnione przez naukowców, organizacje prowadzące badania naukowe lub organizacje finansujące badania naukowe za pośrednictwem repozytorium instytucjonalnego lub tematycznego. W tym kontekście uwzględnia się uzasadnione interesy handlowe, działania związane z transferem wiedzy oraz istniejące już prawa własności intelektualnej.

Podsekcja 5

Zbiory danych o wysokiej wartości

Artykuł 32u

Kategorie tematyczne zbiorów danych o wysokiej wartości

1) Kategorie tematyczne zbiorów danych o wysokiej wartości określono w załączniku I.

2) Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 45 ust. 2a w celu wprowadzania zmian w załączniku I poprzez dodawanie nowych tematycznych kategorii zbiorów danych o wysokiej wartości, tak aby odzwierciedlić rozwój technologii i rynku.

Artykuł 32v

Szczególne zbiory danych o wysokiej wartości oraz warunki ich publikacji i ponownego wykorzystywania

1) Komisja przyjmuje akty wykonawcze ustanawiające wykaz będących w posiadaniu organów sektora publicznego lub przedsiębiorstw publicznych szczególnych zbiorów danych o wysokiej wartości należących do kategorii określonych w załączniku I, spośród dokumentów, do których niniejsza sekcja ma zastosowanie.

Taki szczególny zbiór danych o wysokiej wartości:

a) udostępniany jest bezpłatnie, z zastrzeżeniem ust. 3, 4 i 5;

b) jest w formacie nadającym się do odczytu maszynowego;

c) jest udostępniany za pośrednictwem interfejsów API; oraz

d) w odpowiednich przypadkach, jest udostępniany do zbiorczego pobrania.

W tych aktach wykonawczych mogą zostać określone warunki publikacji i ponownego wykorzystywania zbiorów danych o wysokiej wartości. Takie warunki muszą być zgodne z postanowieniami otwartych licencji standardowych.

Mogą one obejmować warunki mające zastosowanie do ponownego wykorzystywania, formatów danych i metadanych oraz do technicznych warunków rozpowszechniania. Inwestycje dokonane przez państwa członkowskie w odniesieniu do sposobów podejścia do otwartych danych, takie jak inwestycje w rozwój i upowszechnianie niektórych standardów, należy uwzględnić i wyważyć względem potencjalnych korzyści z włączenia do wykazu.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 46 ust. 2.

2) Identyfikacji szczególnych zbiorów danych o wysokiej wartości na podstawie ust. 1 dokonuje się w oparciu o ocenę ich potencjału w zakresie:

   a) generowania istotnych korzyści społeczno-ekonomicznych lub środowiskowych oraz innowacyjnych usług;

   b) przydatności dla dużej liczby użytkowników, w szczególności MŚP i małych spółek o średniej kapitalizacji;

   c) pomagania w generowaniu dochodów; oraz

   d) łączenia ich z innymi zbiorami danych.

W celu identyfikacji takich szczególnych zbiorów danych o wysokiej wartości Komisja przeprowadza stosowne konsultacje, w tym na poziomie ekspertów, przeprowadza ocenę skutków i zapewnia komplementarność z istniejącymi aktami prawnymi, takimi jak dyrektywa Parlamentu Europejskiego i Rady 2010/40/UE, w odniesieniu do ponownego wykorzystywania danych lub dokumentów. Ta ocena skutków obejmuje analizę kosztów i korzyści oraz analizę tego, czy bezpłatne udostępnianie zbiorów danych o wysokiej wartości przez organy sektora publicznego, które muszą uzyskiwać dochody w celu pokrycia znacznej części kosztów związanych z wykonywaniem swoich zadań publicznych, miałoby istotny wpływ na budżet takich organów. W odniesieniu do zbiorów danych o wysokiej wartości będących w posiadaniu przedsiębiorstw publicznych w ocenie skutków szczególną uwagę poświęca się roli, jaką przedsiębiorstwa publiczne odgrywają w konkurencyjnym otoczeniu gospodarczym.

3) Na zasadzie odstępstwa od ust. 1 akapit drugi lit. a) akty wykonawcze, o których mowa w tym ustępie, muszą stanowić, że bezpłatna dostępność zbiorów danych o wysokiej wartości ma nie mieć zastosowania do szczególnych zbiorów danych o wysokiej wartości będących w posiadaniu przedsiębiorstw publicznych, jeżeli prowadziłoby to do zakłócenia konkurencji na odpowiednich rynkach.

4) Wymóg bezpłatnego udostępniania zbiorów danych o wysokiej wartości zgodnie z ust. 1 akapit drugi lit. a) nie ma zastosowania do bibliotek, w tym bibliotek uniwersyteckich, muzeów ani archiwów.

5) W przypadkach gdy bezpłatne udostępnianie zbiorów danych o wysokiej wartości przez organy sektora publicznego, które muszą uzyskiwać dochody w celu pokrycia znacznej części kosztów związanych z wykonywaniem swoich zadań publicznych, miałoby istotny wpływ na budżet danych organów, państwa członkowskie mogą – na okres nieprzekraczający dwóch lat od wejścia w życie odpowiedniego aktu wykonawczego przyjętego zgodnie z ust. 1 – zwolnić te organy z wymogu bezpłatnego udostępniania tych zbiorów danych o wysokiej wartości.

Sekcja 3

Ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu podmiotów sektora publicznego

Artykuł 32w

Warunki ponownego wykorzystywania

1) Organy sektora publicznego, które na mocy prawa krajowego są właściwe do udzielania lub odmowy udzielania dostępu do celów ponownego wykorzystywania danych lub dokumentów należących do niektórych kategorii danych chronionych muszą udostępniać publicznie warunki, które muszą zostać spełnione w celu zezwolenia na takie ponowne wykorzystywanie, oraz procedurę występowania z wnioskiem o ponowne wykorzystywanie za pośrednictwem pojedynczego punktu informacyjnego, o którym mowa w art. 32aa. Podmiotom sektora publicznego mogą pomagać w udzielaniu lub odmowie udzielania dostępu do celów ponownego wykorzystania właściwe podmioty określone w art. 32z ust. 1.

   Państwa członkowskie zapewniają, aby podmioty sektora publicznego były wyposażone w niezbędne zasoby w celu przestrzegania niniejszego artykułu i art. 32x.

2) Ponowne wykorzystywanie danych lub dokumentów nie ma wpływu na chroniony charakter tych danych lub dokumentów i jest dozwolone wyłącznie:

   a) zgodnie z prawami własności intelektualnej;

   b) jeżeli dane, które uznaje się za poufne zgodnie z prawem Unii lub prawem krajowym dotyczącym poufności informacji handlowych i statystycznych, nie zostaną ujawnione w wyniku zezwolenia na ponowne wykorzystywanie, chyba że takie ponowne wykorzystywanie jest dozwolone na podstawie zgody osoby, której dane dotyczą, lub pozwolenia posiadacza danych zgodnie z ust. 5;

   c) zgodnie z rozporządzeniem (UE) 2016/679.

3) Aby zapewnić zachowanie chronionego charakteru, o którym mowa w ust. 2, organy sektora publicznego mogą ustanowić następujące wymogi:

   a) dostępu do celów ponownego wykorzystywania danych lub dokumentów udziela się wyłącznie w przypadku, gdy organ sektora publicznego lub właściwy organ, w następstwie wniosku o ponowne wykorzystywanie, dopilnował, aby te dane lub dokumenty:

      (i) zostały zanonimizowane – w przypadku danych osobowych;

      (ii) zostały poddane innym formom przygotowania danych osobowych;

      (iii) zostały zmodyfikowane, zagregowane lub przekształcone za pomocą innej metody zapobiegającej ujawnieniu – w przypadku poufnych informacji handlowych, w tym tajemnic handlowych lub treści chronionych prawami własności intelektualnej;

   b) dostęp do danych lub dokumentów i ich ponowne wykorzystywanie odbywa się w sposób zdalny w bezpiecznym środowisku przetwarzania zapewnianym lub kontrolowanym przez podmiot sektora publicznego;

   c) jeżeli nie można zezwolić na dostęp zdalny bez stwarzania zagrożenia dla praw i interesów osób trzecich, dostęp do danych lub dokumentów i ich ponowne wykorzystywanie odbywa się w obrębie obiektów fizycznych, w których

panuje bezpieczne środowisko przetwarzania zgodnie z rygorystycznymi normami bezpieczeństwa.

W przypadku ponownego wykorzystywania dozwolonego zgodnie z akapitem pierwszym lit. a) ppkt (i) ponowne wykorzystywanie danych lub dokumentów podlega przepisom dotyczącym otwartych danych publicznych określonym w sekcji 2. Pozostaje to bez uszczerbku dla art. 32y, który ma pierwszeństwo w przypadku konfliktu.

W przypadku ponownego wykorzystywania, na które zezwolono zgodnie z akapitem pierwszym lit. b) i c), organy sektora publicznego nakładają warunki, które pozwalają zachować integralność funkcjonowania systemów technicznych wykorzystywanego bezpiecznego środowiska przetwarzania.

4) Organ sektora publicznego zastrzega sobie prawo do weryfikacji procesu, środków i wszelkich wyników przetwarzania danych lub dokumentów przez ponownego użytkownika w celu zachowania integralności ochrony danych lub dokumentów. Zastrzega sobie również prawo do zakazania wykorzystywania wyników zawierających informacje zagrażające prawom i interesom osób trzecich. Decyzja o zakazie wykorzystywania wyników musi być zrozumiała i przejrzysta dla ponownego użytkownika.

O ile w prawie krajowym nie ustanowiono szczególnych zabezpieczeń dotyczących mających zastosowanie obowiązków w zakresie zachowania poufności w odniesieniu do ponownego wykorzystywania niektórych kategorii danych chronionych, organ sektora publicznego uzależnia ponowne wykorzystywanie danych lub dokumentów przekazanych zgodnie z ust. 3 od przestrzegania przez ponownego użytkownika obowiązku w zakresie zachowania poufności, zgodnie z którym zakazane jest ujawnianie informacji, które stwarzają zagrożenie dla praw i interesów osób trzecich, a które pomimo wprowadzonych zabezpieczeń mogłyby się znaleźć w posiadaniu ponownego użytkownika. W przypadku niedozwolonego ponownego wykorzystywania danych nieosobowych ponowny użytkownik ma obowiązek, bez zwłoki i – w stosownych przypadkach – z pomocą organu sektora publicznego, poinformować osoby fizyczne lub prawne, na których prawa i interesy może to mieć wpływ.

5) W przypadku gdy ponowne wykorzystywanie danych lub dokumentów nie może być dozwolone zgodnie z ust. 3 i 4, ponowne wykorzystywanie jest możliwe wyłącznie:

a) w przypadku gdy nie istnieje podstawa prawna inna niż zgoda na przekazanie danych na podstawie rozporządzenia (UE) 2016/679, za zgodą osób, których dane dotyczą;

b) za pozwoleniem posiadaczy danych, na których prawa i interesy takie ponowne wykorzystywanie może mieć wpływ.

Organ sektora publicznego dokłada wszelkich starań, zgodnie z prawem Unii i prawem krajowym, aby zapewnić potencjalnym ponownym użytkownikom pomoc w uzyskaniu zgody osób, których dane dotyczą, lub pozwolenia od posiadaczy danych, na których prawa i interesy takie ponowne wykorzystywanie może mieć wpływ, jeżeli jest to wykonalne bez nieproporcjonalnego obciążenia organu sektora publicznego.

Podmiotowi sektora publicznego mogą pomagać w udzielaniu takiej pomocy właściwe podmioty, o których mowa w art. 32z.

Artykuł 32x

Wymogi dotyczące przekazywania danych nieosobowych do państw trzecich przez ponownych użytkowników

1) W przypadku gdy ponowny użytkownik zamierza przekazać do państwa trzeciego niektóre kategorie danych chronionych, które są danymi nieosobowymi, informuje o swoim zamiarze przekazania takich danych organ sektora publicznego, podając w momencie składania wniosku o ponowne wykorzystywanie danych również cel tego przekazania. W przypadku ponownego wykorzystywania na podstawie pozwolenia posiadacza danych ponowny użytkownik, w stosownych przypadkach z pomocą organu sektora publicznego, informuje osobę fizyczną lub prawną, na której prawa i interesy może to mieć wpływ, o swoim zamiarze, celu oraz o odpowiednich zabezpieczeniach. Organ sektora publicznego nie zezwala na ponowne wykorzystywanie, o ile dana osoba fizyczna lub prawna nie udzieli pozwolenia na przekazanie.

2) Podmioty sektora publicznego przesyłają poufne dane nieosobowe lub dane chronione prawami własności intelektualnej ponownemu użytkownikowi, który zamierza przekazać te dane do państwa trzeciego innego niż państwo wyznaczone zgodnie z ust. 7 wyłącznie wtedy, gdy ponowny użytkownik zobowiąże się na podstawie umowy do:

   a) wypełniania obowiązków nałożonych zgodnie z prawami własności intelektualnej oraz prawem Unii lub prawem krajowym dotyczącym poufności informacji handlowych i statystycznych nawet po przekazaniu danych do państwa trzeciego;

   b) uznania jurysdykcji sądów lub trybunałów państwa członkowskiego organu sektora publicznego przesyłającego dane w odniesieniu do wszelkich sporów związanych z przestrzeganiem praw własności intelektualnej oraz prawa Unii lub prawa krajowego dotyczącego poufności informacji handlowych i statystycznych.

3) Komisja może przyjmować akty wykonawcze ustanawiające wzory klauzul umownych w celu wypełnienia obowiązków, o których mowa w ust. 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 46 ust. 2.

4) Podmioty sektora publicznego, w stosownych przypadkach i w miarę swoich zdolności, udzielają ponownym użytkownikom wskazówek oraz udzielają pomocy w wypełnianiu obowiązków, o których mowa w ust. 2.

5) Jeżeli jest to uzasadnione ze względu na znaczącą liczbę wniosków składanych w całej Unii dotyczących ponownego wykorzystywania danych nieosobowych w określonych państwach trzecich, Komisja może przyjąć akty wykonawcze, w których stwierdza, że stosowane przez dane państwo trzecie rozwiązania prawne, w zakresie nadzoru i egzekwowania przepisów:

   a) zapewniają ochronę własności intelektualnej i tajemnic przedsiębiorstwa w sposób zasadniczo równoważny z ochroną zapewnianą na podstawie prawa Unii;

   b) są skutecznie stosowane i egzekwowane; oraz

   c) zapewniają skuteczne sądowe środki zaskarżenia.

6) Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 46 ust. 2.

7) Na podstawie szczególnych aktów ustawodawczych Unii można do celów niniejszego artykułu uznać niektóre kategorie danych nieosobowych będące w posiadaniu podmiotów sektora publicznego za szczególnie chronione w najwyższym stopniu, w przypadku gdy ich przekazanie do państw trzecich może zagrozić celom polityki publicznej Unii, takim jak bezpieczeństwo i zdrowie publiczne, lub może prowadzić do ryzyka deanonimizacji zanonimizowanych danych nieosobowych. W przypadku gdy taki akt zostanie przyjęty, Komisja przyjmuje zgodnie z art. 45 akty delegowane uzupełniające niniejsze rozporządzenie poprzez ustanowienie warunków szczególnych mających zastosowanie do przekazywania takich danych do państw trzecich.

Jeżeli wymaga tego szczególny akt ustawodawczy Unii, o którym mowa w akapicie pierwszym, takie warunki szczególne mogą obejmować warunki mające zastosowanie do przekazywania lub uzgodnień technicznych w tym zakresie, ograniczenia dotyczące ponownego wykorzystywania danych w państwach trzecich lub kategorii osób, które są uprawnione do przekazywania takich danych do państw trzecich, lub, w wyjątkowych przypadkach, ograniczenia dotyczące przekazywania do państw trzecich.

Ponowny użytkownik, któremu przyznano prawo do ponownego wykorzystywania danych nieosobowych, może przekazywać te dane tylko do tych państw trzecich, w przypadku których spełnione są wymogi określone w ust. 2, 4 i 5.

Artykuł 32y
Opłaty

1) Organy sektora publicznego, które zezwalają na ponowne wykorzystywanie niektórych kategorii danych chronionych, mogą pobierać opłaty za zezwolenie na ponowne wykorzystywanie takich danych.

2) Jeżeli organy sektora publicznego pobierają opłaty, podejmują one działania mające na celu stwarzanie zachęt do ponownego wykorzystywania niektórych kategorii danych chronionych do celów niekomercyjnych, takich jak cele badań naukowych, oraz przez przedsiębiorstwa typu start-up, MŚP i małe spółki o średniej kapitalizacji zgodnie z unijnymi zasadami pomocy państwa. W związku z tym organy sektora publicznego mogą również udostępniać dane za obniżoną opłatą lub nieodpłatnie, w szczególności przedsiębiorstwom typu start-up, MŚP i małym spółkom o średniej kapitalizacji, społeczeństwu obywatelskiemu oraz placówkom badawczym i edukacyjnym. W tym celu podmioty sektora publicznego mogą sporządzić wykaz kategorii ponownych użytkowników, którym udostępnia się dane lub dokumenty do ponownego wykorzystywania za obniżoną opłatą lub nieodpłatnie. Wykaz ten wraz z kryteriami stosowanymi do jego sporządzenia podaje się do wiadomości publicznej.

3) Opłaty muszą wynikać z kosztów związanych z prowadzeniem procedur dotyczących wniosków o ponowne wykorzystywanie niektórych kategorii danych chronionych oraz ograniczać się do niezbędnych kosztów związanych z:

a) powielaniem, dostarczaniem i rozpowszechnianiem danych;

b) weryfikacją praw;

c) anonimizacją lub innymi formami przygotowania danych osobowych i danych poufnych ze względów handlowych, jak przewidziano w art. 32w ust. 3 [warunki ponownego wykorzystywania];

d) utrzymaniem bezpiecznego środowiska przetwarzania;

e) nabywaniem przez osoby trzecie spoza sektora publicznego prawa do zezwalania na ponowne wykorzystywanie zgodnie z niniejszą sekcją; oraz udzielaniem pomocy ponownym użytkownikom w uzyskiwaniu zgody osób, których dane dotyczą, oraz pozwolenia posiadaczy danych, w przypadku gdy takie ponowne wykorzystywanie może mieć wpływ na prawa i interesy tych osób i posiadaczy.

4) Kryteria i metodyka obliczania opłat są określane przez państwa członkowskie i publikowane. Podmiot sektora publicznego publikuje opis głównych kategorii kosztów oraz zasad stosowanych przy ich rozdziale.

5) Organy sektora publicznego mogą pobierać od bardzo dużych przedsiębiorstw opłaty wyższe niż opłaty dozwolone zgodnie z ust. 2 i 3 niniejszego artykułu, w oparciu o obiektywne kryteria, biorąc pod uwagę siłę gospodarczą lub zdolność podmiotu do pozyskiwania danych, w tym w szczególności wskazanie go jako strażnika dostępu na podstawie rozporządzenia (UE) 2022/1925. Wszelkie takie obliczone opłaty muszą być proporcjonalne. Oprócz elementów wymienionych w ust. 3 niniejszego artykułu mogą one pokrywać koszty gromadzenia i produkowania danych, wraz z rozsądnym zwrotem z inwestycji.

Artykuł 32z

Właściwe organy

1) Na potrzeby wykonywania zadań, o których mowa w niniejszym artykule, każde państwo członkowskie wyznacza jeden lub większą liczbę właściwych organów zgodnie z art. 37 ust. 1, którymi mogą być podmioty właściwe w zakresie szczególnych sektorów, ale które łącznie muszą obejmować wszystkie sektory, aby wspierać organy sektora publicznego udzielające lub odmawiające dostępu do celów ponownego wykorzystywania niektórych kategorii danych chronionych. Państwa członkowskie mogą ustanowić jeden nowy właściwy podmiot lub większą ich liczbę albo opierać się na istniejących podmiotach sektora publicznego lub na wewnętrznych służbach podmiotów sektora publicznego spełniających warunki określone w niniejszej sekcji.

2) Właściwe podmioty mogą zostać upoważnione do udzielania dostępu do celów ponownego wykorzystywania niektórych kategorii danych chronionych zgodnie z prawem Unii lub prawem krajowym, w którym przewidziano udzielenie takiego dostępu. W przypadku udzielenia lub odmowy dostępu do celów ponownego wykorzystywania te właściwe organy podlegają przepisom art. 32k, 32w, 32x, 32y i 32ab.

3) Właściwym podmiotom należy zapewnić odpowiednie zasoby prawne, finansowe, techniczne i ludzkie do wykonywania powierzonych im zadań, w tym niezbędną wiedzę techniczną, aby były w stanie przestrzegać odpowiednich przepisów prawa Unii lub prawa krajowego dotyczących systemów dostępu do kategorii danych chronionych, o których mowa w art. 2 pkt 54.

4) Pomoc, o której mowa w ust. 1, obejmuje, w razie potrzeby:

a) zapewnienie wsparcia technicznego poprzez udostępnienie bezpiecznego środowiska przetwarzania na potrzeby zapewnienia dostępu do celów ponownego wykorzystywania danych lub dokumentów;

b) udzielenie wskazówek i zapewnianie wsparcia technicznego w zakresie jak najlepszego ustrukturyzowania danych i ich przechowywania w celu zapewnienia łatwego dostępu do tych danych lub dokumentów;

c) zapewnienie wsparcia technicznego w zakresie anonimizacji, pseudonimizacji i najnowocześniejszych metod ochrony prywatności, nie tylko danych osobowych, ale również poufnych informacji handlowych, w tym tajemnic przedsiębiorstwa lub treści chronionych prawami własności intelektualnej;

d) udzielanie pomocy, w stosownych przypadkach, podmiotom sektora publicznego w zapewnianiu wsparcia ponownym użytkownikom w występowaniu do osób, których dane dotyczą, o zgodę na ponowne wykorzystywanie danych oraz do posiadaczy danych – o pozwolenie, zgodnie z ich konkretnymi decyzjami, w tym odnośnie do jurysdykcji, w której ma się odbywać przetwarzanie danych, oraz – w sytuacji, gdy jest to wykonalne w praktyce – udzielanie pomocy podmiotom sektora publicznego w ustanawianiu mechanizmów technicznych umożliwiających przekazywanie wniosków ponownych użytkowników o wyrażenie zgody lub udzielenie pozwolenia.

e) udzielenie pomocy podmiotom sektora publicznego w zakresie oceny adekwatności zobowiązań umownych zaciągniętych przez ponownego użytkownika zgodnie z art. 32x ust. 2.

Artykuł 32aa

Pojedynczy punkt informacyjny

1) Każde państwo członkowskie wyznacza pojedynczy punkt informacyjny. Punkt ten udostępnia łatwo dostępne informacje dotyczące stosowania art. 32w, 32x i 32y.

2) Pojedynczy punkt informacyjny jest właściwy do przyjmowania zapytań lub wniosków o ponowne wykorzystywanie niektórych kategorii danych chronionych i przekazuje je, jeśli jest to możliwe i odpowiednie za pomocą zautomatyzowanych środków, właściwym organom sektora publicznego lub, w stosownych przypadkach, właściwym podmiotom, o których mowa w art. 32z ust. 1.

3) Pojedynczy punkt informacyjny może obejmować odrębny, uproszczony i dobrze udokumentowany kanał informacyjny dla MŚP, małych spółek o średniej kapitalizacji, przedsiębiorstw typu start-up i ośrodków badań naukowych odpowiadający ich potrzebom i zdolnościom w zakresie składania wniosków o ponowne wykorzystywanie kategorii danych, o których mowa w art. 2 pkt 54.

4) Pojedynczy punkt informacyjny udostępnia za pomocą środków elektronicznych przeszukiwalny wykaz zasobów zawierający przegląd wszystkich dostępnych zasobów_dokumentów, w tym – w stosownych przypadkach – tych zasobów dokumentów, które są dostępne w sektorowych, regionalnych lub lokalnych punktach informacyjnych, wraz z odpowiednimi informacjami opisującymi dostępne dane lub dokumenty, w tym przynajmniej format i rozmiar danych oraz warunki ich ponownego wykorzystywania.

5) Komisja ustanawia europejski pojedynczy punkt dostępu oferujący elektroniczny przeszukiwalny rejestr danych lub dokumentów dostępnych w krajowych pojedynczych punktach informacyjnych oraz dalsze informacje na temat sposobu wnioskowania o dane lub dokumenty za pośrednictwem tych krajowych pojedynczych punktów informacyjnych.

Artykuł 32ab

Procedura składania wniosków o ponowne wykorzystywanie

1) O ile zgodnie z prawem krajowym nie zostały określone krótsze terminy, właściwe organy sektora publicznego lub właściwe podmioty, o których mowa w art. 32z ust. 1, przyjmują decyzję w sprawie wniosku o ponowne wykorzystywanie niektórych kategorii danych chronionych w terminie dwóch miesięcy od dnia otrzymania wniosku.

2) W przypadku wyjątkowo obszernych i złożonych wniosków o ponowne wykorzystywanie, termin dwóch tygodni może zostać przedłużony do 30 dni. W takich przypadkach właściwe organy sektora publicznego lub właściwe podmioty, o których mowa w art. 32z ust. 1, powiadamiają jak najszybciej wnioskodawcę o tym, że do przeprowadzenia procedury potrzeba więcej czasu, wraz z uzasadnieniem tego opóźnienia.

3) Każda osoba fizyczna lub prawna, której bezpośrednio dotyczy decyzja, o której mowa w ust. 1, ma prawo do skutecznego środka zaskarżenia w państwie członkowskim, w którym znajduje się dany podmiot. Takie prawo do środka zaskarżenia musi zostać ustanowione w prawie krajowym i obejmować możliwość kontroli przez bezstronny podmiot posiadający odpowiednią wiedzę fachową – taki jak krajowy organ ochrony konkurencji, odpowiedni organ regulujący dostęp do dokumentów, organ nadzorczy ustanowiony zgodnie z rozporządzeniem (UE) 2016/679 lub krajowy organ sądowy – którego decyzje są wiążące dla danego podmiotu sektora publicznego lub właściwego podmiotu.”;

19. art. 38 otrzymuje brzmienie:

1) „Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej osoby fizyczne i prawne mają prawo wnieść skargę, indywidualnie lub w stosownym przypadku zbiorowo:

   a) do stosownego właściwego organu w państwie członkowskim, w którym mają miejsce zwykłego pobytu, miejsce pracy lub siedzibę, jeżeli sądzą, że ich prawa wynikające z niniejszego rozporządzenia zostały naruszone;

   b) w przypadku wszelkich kwestii objętych zakresem niniejszego rozporządzenia, w szczególności przeciwko uznanemu dostawcy usług pośrednictwa danych lub uznanej organizacji altruizmu danych, do stosownego organu właściwego do spraw rejestracji usług pośrednictwa danych lub odpowiedniego organu właściwego do spraw rejestracji organizacji altruizmu danych.

2) Koordynator danych na wniosek przedstawia osobom fizycznym i prawnym wszelkie informacje niezbędne do wniesienia skargi do odpowiedniego właściwego organu.

3) Właściwy organ, do którego wniesiono skargę, informuje skarżącego, zgodnie z prawem krajowym, o:

   a) przebiegu postępowania i podjętej decyzji; oraz

b) środkach ochrony prawnej przed sądem określonych w art. 39.”;

20. w art. 40 dodaje się ust. 6 w brzmieniu:

„6. Niniejszy artykuł nie ma zastosowania do rozdziału VIIc.”;

21. po art. 41 dodaje się tytuł w brzmieniu:

„ROZDZIAŁ IXa

Europejska Rada ds. Innowacji w zakresie Danych”;

22. dodaje się art. 41a w brzmieniu:

„Artykuł 41a

Europejska Rada ds. Innowacji w zakresie Danych

1) Ustanawia się Europejską Radę ds. Innowacji w zakresie Danych, która ma doradzać Komisji i wspierać ją w koordynowaniu egzekwowania niniejszego rozporządzenia oraz służyć jako forum dyskusji na temat rozwoju europejskiej gospodarki opartej na danych i polityki w zakresie danych.

2) W jej skład wchodzą co najmniej przedstawiciele państw członkowskich odpowiedzialni za kwestie związane z danymi, organy właściwe do egzekwowania przepisów rozdziałów II, III, V, VIIa i VIIc niniejszego rozporządzenia, Europejska Rada Ochrony Danych, Europejski Inspektor Ochrony Danych, ENISA, pełnomocnik UE ds. MŚP lub przedstawiciel wyznaczony przez sieć pełnomocników ds. MŚP. Komisja może podjąć decyzję o dodaniu dodatkowych kategorii członków. Przy powoływaniu poszczególnych ekspertów Komisja dąży do osiągnięcia wśród członków grupy równowagi płci i równowagi geograficznej.

3) Komisja decyduje o strukturze poszczególnych składów, w których Rada będzie wykonywać swoje zadania.

4) Posiedzeniom Europejskiej Rady ds. Innowacji w zakresie Danych przewodniczy Komisja.”;

23. Art. 42 otrzymuje brzmienie:

„Artykuł 42

Rola Europejskiej Rady ds. Innowacji w zakresie Danych

1) Europejska Rada ds. Innowacji w zakresie Danych zapewnia spójne stosowanie niniejszego rozporządzenia przez:

a) pełnienie roli forum strategicznych dyskusji na temat polityki w zakresie danych, zarządzania danymi, międzynarodowych przepływów danych i zmian międzysektorowych istotnych dla europejskiej gospodarki opartej na danych;

b) doradzanie i pomoc Komisji w odniesieniu do stworzenia spójnej praktyki właściwych organów w egzekwowaniu rozdziałów II, III, V i VII, VIIa i VIIc;

c) ułatwianie współpracy między właściwymi organami dzięki budowaniu zdolności i wymianie informacji;

d) wspieranie wymiany doświadczeń i dobrych praktyk między państwami członkowskimi w dziedzinie ponownego wykorzystywania informacji sektora

publicznego we współpracy z innymi odpowiednimi organami zarządzającymi.”;

24. w art. 45 wprowadza się następujące zmiany:

a) ust. 2 otrzymuje brzmienie:

„2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 29 ust. 7, art. 32u ust. 2 i art. 33 ust. 2, powierza się Komisji na czas nieokreślony.”;

b) ust. 3 otrzymuje brzmienie:

„3. Przekazanie uprawnień, o którym mowa w art. 29 ust. 7, art. 32u ust. 2 i art. 33 ust. 2, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.”;

c) ust. 6 otrzymuje brzmienie:

„6. Akt delegowany przyjęty na podstawie art. 29 ust. 7, art. 32u ust. 2 lub art. 33 ust. 2 wchodzi w życie wyłącznie wtedy, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.”;

25. w art. 46 wprowadza się następujące zmiany:

a) ust. 1 zdanie pierwsze otrzymuje brzmienie:

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

b) dodaje się ust. 1a w brzmieniu:

„1a. W przypadku odesłania do niniejszego ustępu stosuje się art. 4 rozporządzenia (UE) nr 182/2011.”;

26. w art. 49 wprowadza się następujące zmiany:

a) w ust. 1 wprowadza się następujące zmiany:

(i) formuła wprowadzająca otrzymuje brzmienie:

„1. Do dnia 12 września 2028 r. Komisja przeprowadzi ocenę rozdziałów II, III, IV, V, VI, VII i VIII oraz przedłoży Parlamentowi Europejskiemu i Radzie, a także Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie na temat głównych ustaleń. Ocena ta obejmuje w szczególności:”;

(ii) lit. m) otrzymuje brzmienie:

„m) wpływ niniejszego rozporządzenia na MŚP i małe spółki o średniej kapitalizacji w odniesieniu do ich innowacyjności i do dostępności usług przetwarzania danych dla unijnych użytkowników oraz do obciążeń związanych z przestrzeganiem nowych obowiązków.”;

b) dodaje się ust. 2a w brzmieniu:

„2a. Do dnia [data = wejście w życie plus 5 lat] r. Komisja przeprowadzi ocenę rozdziałów VIIa, VIIb i VIIc niniejszego rozporządzenia oraz przedłoży Parlamentowi Europejskiemu i Radzie, a także Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie na temat głównych ustaleń.

W sprawozdaniu ocenia się w szczególności:

a) stan rejestracji usług pośrednictwa danych oraz rodzaj oferowanych przez nie usług;

b) rodzaj zarejestrowanych organizacji altruizmu danych oraz przegląd celów leżących w interesie ogólnym, którym służy dzielenie się danymi, z myślą o ustanowieniu jasnych kryteriów w tym zakresie;

c) zakres oraz skutki społeczne i gospodarcze rozdziału VIIc sekcja 2, w tym:

d) zakres wzrostu ponownego wykorzystywania dokumentów sektora publicznego, do których ma zastosowanie rozdział VIIc sekcja 2, w szczególności przez MŚP i małe spółki o średniej kapitalizacji;

e) wpływu zbiorów danych o wysokiej wartości;

f) interakcji między przepisami w zakresie ochrony danych a możliwościami ponownego wykorzystywania;

g) Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania tego sprawozdania.”;

c) ust. 5 otrzymuje brzmienie:

„5. Na podstawie sprawozdań, o których mowa w ust. 1, 2 i 2a, Komisja może w stosownym przypadku przedłożyć Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy dotyczący zmiany niniejszego rozporządzenia.”;

27. dodaje się załącznik I w brzmieniu określonym w załączniku II do niniejszego rozporządzenia.

Artykuł 2

Zmiany w rozporządzeniu (UE) 2018/1724

W tabeli w załączniku II do rozporządzenia (UE) 2018/1724 wpis „Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej” otrzymuje brzmienie:

Zdarzenia życiowe	Procedury	Oczekiwany wynik z zastrzeżeniem, w stosownych przypadkach, oceny wniosku przez właściwy organ zgodnie z prawem krajowym
Rozpoczęcie, prowadzenie	Powiadomienie o działalności gospodarczej, zezwolenie na prowadzenie działalności gospodarczej,	Potwierdzenie otrzymania zgłoszenia

i zakończenie działalności gospodarczej	zmiana działalności gospodarczej i zakończenie takiej działalności nieobejmujące procedur dotyczących niewypłacalności lub likwidacji, z wyłączeniem procedur dotyczących początkowej rejestracji działalności gospodarczej w rejestrze przedsiębiorców oraz z wyłączeniem procedur dotyczących zakładania spółek oraz późniejszego zgłaszania składania dokumentów przez spółki, w rozumieniu art. 54 akapit drugi TFUE	lub zmiany działalności gospodarczej, lub wniosku o zezwolenie na prowadzenie działalności gospodarczej
	Rejestracja pracodawcy (osoby fizycznej) w obowiązkowych systemach emerytalno-rentowych i ubezpieczeniowych	Potwierdzenie rejestracji lub numer rejestracyjny ubezpieczenia społecznego
	Rejestracja pracowników w obowiązkowych systemach emerytalno-rentowych i ubezpieczeniowy	Potwierdzenie rejestracji lub numer rejestracyjny ubezpieczenia społecznego
	Złożenie deklaracji podatkowej dotyczącej podatku od osób prawnych	Potwierdzenie przyjęcia deklaracji podatkowej
	Zgłoszenie w systemach zabezpieczenia społecznego rozwiązania umowy z pracownikiem, z wyłączeniem procedur grupowego rozwiązywania umów z pracownikami	Potwierdzenie otrzymania zgłoszenia
	Płatność składek na ubezpieczenia społeczne pracowników	Pokwitowanie lub inna forma potwierdzenia płatności składek na ubezpieczenia społeczne pracowników
	Rejestracja jako dostawca usług pośrednictwa danych	Potwierdzenie rejestracji
	Rejestracja jako uznana w Unii organizacja altruizmu danych	Potwierdzenie rejestracji

Artykuł 3

Zmiany w rozporządzeniu (UE) 2016/679 (GDPR)

W rozporządzeniu (UE) 2016/679 wprowadza się następujące zmiany:

1. w art. 4 wprowadza się następujące zmiany:

(a) w pkt 1 dodaje się zdania w brzmieniu:

„Informacje dotyczące osoby fizycznej niekoniecznie są danymi osobowymi dla każdej innej osoby lub każdego innego podmiotu z tego tylko powodu, że inny podmiot może zidentyfikować tę osobę fizyczną. Informacje nie mają charakteru danych osobowych dla danego podmiotu, jeżeli podmiot ten nie

może zidentyfikować osoby fizycznej, której dotyczą informacje, biorąc pod uwagę środki, co do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez ten podmiot. Takie informacje nie stają się dla tego podmiotu danymi osobowymi z tego tylko powodu, że potencjalny kolejny odbiorca dysponuje środkami, co do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane do zidentyfikowania osoby fizycznej, której informacje te dotyczą.”;

(b) dodaje się punkty w brzmieniu:

„32) »końcowe urządzenie« oznacza końcowe urządzenie określone w art. 1 pkt 1 dyrektywy 2008/63/WE;

33) w przypadku »sieci łączności elektronicznej« zastosowanie ma definicja zawarta w art. 2 pkt 1 dyrektywy (UE) 2018/1972;

34) »przeglądarka internetowa« oznacza przeglądarkę internetową zdefiniowaną w art. 2 pkt 11 rozporządzenia (UE) 2022/1925;

35) »usługa medialna« oznacza usługę medialną zdefiniowaną w art. 2 pkt 1 rozporządzenia (UE) 2024/1083;

36) »dostawca usług medialnych« oznacza dostawcę usług medialnych zdefiniowanego w art. 2 pkt 2 rozporządzenia (UE) 2024/1083;

37) »interfejs internetowy« oznacza interfejs internetowy zgodnie z definicją w art. 3 lit. m) rozporządzenia (UE) 2022/2065;

38) »badania naukowe« oznaczają wszelkie badania, które mogą również wspierać innowacje, takie jak rozwój technologiczny i demonstracja. Działania te przyczyniają się do rozwoju istniejącej wiedzy naukowej lub wykorzystują istniejącą wiedzę w nowatorski sposób, są prowadzone w celu przyczynienia się do rozwoju ogólnej wiedzy i dobrostanu społeczeństwa oraz są zgodne z normami etycznymi w odpowiedniej dziedzinie badań naukowych. Nie wyklucza to, że badania mogą mieć również na celu realizację interesu handlowego.”;

2. art. 5 ust. 1 lit. b) otrzymuje brzmienie:

„zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych jest uznawane w myśl art. 89 ust. 1 za zgodne z pierwotnymi celami, niezależnie od warunków określonych w art. 6 ust. 4 niniejszego rozporządzenia (»ograniczenie celu«);”;

3. w art. 9 wprowadza się następujące zmiany:

(a) w ust. 2 dodaje się litery w brzmieniu:

„k) przetwarzanie odbywa się w kontekście rozwoju i eksploatacji systemu AI zdefiniowanego w art. 3 pkt 1 rozporządzenia (UE) 2024/1689 lub modelu AI, z zastrzeżeniem warunków, o których mowa w ust. 5;

l) przetwarzanie danych biometrycznych jest niezbędne do potwierdzenia tożsamości osoby, której dane dotyczą (weryfikacja), w przypadku gdy dane

biometryczne lub środki niezbędne do weryfikacji znajdują się pod wyłączną kontrolą osoby, której dane dotyczą.”;

(b) dodaje się ustęp w brzmieniu:

„5. W odniesieniu do przetwarzania, o którym mowa w ust. 2 lit. k), wdraża się odpowiednie środki organizacyjne i techniczne, aby uniknąć gromadzenia i innego przetwarzania szczególnych kategorii danych osobowych. Jeżeli pomimo wdrożenia takich środków administrator zidentyfikuje szczególne kategorie danych osobowych w zbiorach danych wykorzystywanych do trenowania, testowania lub walidacji bądź w systemie AI lub modelu AI, usuwa takie dane. Jeżeli usunięcie tych danych wymaga niewspółmiernie dużego wysiłku, administrator w każdym przypadku skutecznie i bez zbędnej zwłoki chroni takie dane przed wykorzystaniem do uzyskania wyników, przed ujawnieniem lub udostępnieniem w inny sposób osobom trzecim.”;

4. art. 12 ust. 5 otrzymuje brzmienie:

„5. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, lub również, w przypadku żądań na podstawie art. 15, ponieważ osoba, której dane dotyczą, nadużywa praw przyznanych jej na mocy niniejszego rozporządzenia do celów innych niż ochrona jej danych, administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo

b) odmówić podjęcia działań w związku z wnioskiem.

Na administratorze spoczywa obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony charakter lub że istnieją uzasadnione podstawy, by sądzić, że jest ono nadmierne.”;

5. art. 13 ust. 4 otrzymuje brzmienie:

„4. Ust. 1, 2 i 3 nie mają zastosowania, jeżeli dane osobowe zostały zebrane w kontekście jasnych i ograniczonych powiązań między osobami, których dane dotyczą, a administratorem prowadzącym działalność, która nie wymaga intensywnego przetwarzania danych, i istnieją uzasadnione podstawy, by przypuszczać, że osoba, której dane dotyczą, posiada już informacje, o których mowa w ust. 1 lit. a) i c), chyba że administrator przekazuje dane innym odbiorcom lub kategoriom odbiorców, przekazuje dane do państwa trzeciego, dokonuje zautomatyzowanego podejmowania decyzji, w tym profilowania, o którym mowa w art. 22 ust. 1, lub przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, w rozumieniu art. 35.”;

6. w art. 13 dodaje się ust. 5;

„5. Jeżeli przetwarzanie odbywa się do celów badań naukowych, a udzielenie informacji, o których mowa w ust. 1, 2 i 3, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym

mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania, administrator nie musi udzielać informacji, o których mowa w ust. 1, 2 i 3. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie.”;

7. art. 22 ust. 1 i 2 otrzymują brzmienie:

„1. Decyzja, która wywołuje skutki prawne dla osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływa, może opierać się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, tylko wtedy, gdy decyzja ta:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem danych, niezależnie od tego, czy decyzję można by podjąć w sposób inny niż wyłącznie zautomatyzowany;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.”;

8. w art. 33 wprowadza się następujące zmiany:

(a) ust. 1 otrzymuje brzmienie:

„1. W przypadku naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 96 godzin po stwierdzeniu tego naruszenia – zgłasza je za pośrednictwem pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555 organowi nadzorczemu właściwemu zgodnie z art. 55 i 56. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 96 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

(b) dodaje się ustęp w brzmieniu:

„1a. Do czasu ustanowienia pojedynczego punktu kontaktowego na podstawie art. 23a dyrektywy (UE) 2022/2555 administratorzy nadal zgłaszają naruszenia ochrony danych osobowych bezpośrednio właściwemu organowi nadzorczemu zgodnie z art. 55 i 56.”;

(c) dodaje się ustępy w brzmieniu:

„6. Rada przygotowuje i przekazuje Komisji wniosek dotyczący wspólnego wzoru zawiadomienia o naruszeniu ochrony danych osobowych właściwego organu nadzorczego, o którym mowa w ust. 1, a także wykazu okoliczności, w których naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej. Wnioski przedkłada się Komisji w terminie do dnia [Urząd Publikacji = dziewięć miesięcy od daty rozpoczęcia stosowania niniejszego rozporządzenia] r. Komisja, po należytym

rozpatrzeniu wniosku, dokonuje jego przeglądu w razie potrzeby i jest uprawniona do przyjęcia go w drodze aktu wykonawczego zgodnie z procedurą sprawdzającą określoną w art. 93 ust. 2.

7. Wzór i wykaz, o których mowa w ust. 6, poddaje się przeglądowi co najmniej raz na trzy lata i w razie potrzeby aktualizuje. Rada przedkłada Komisji w odpowiednim czasie swoją ocenę i ewentualne propozycje aktualizacji. Po należytym rozpatrzeniu wniosków Komisja dokonuje ich przeglądu i jest uprawniona do przyjmowania wszelkich aktualizacji zgodnie z procedurą określoną w ust. 6.”;

9. w art. 35 wprowadza się następujące zmiany:

(a) ust. 4, 5 i 6 otrzymują brzmienie:

„4. Rada przygotowuje i przekazuje Komisji wniosek dotyczący wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na podstawie ust. 1.

5. Rada przygotowuje i przekazuje Komisji wniosek dotyczący wykazu rodzajów operacji przetwarzania, w przypadku których nie jest wymagana ocena skutków dla ochrony danych.

6. Rada przygotowuje i przekazuje Komisji wniosek dotyczący wspólnego wzoru i wspólnej metodyki przeprowadzania ocen skutków dla ochrony danych.”;

(b) dodaje się ustępy w brzmieniu:

„6a. Wnioski dotyczące wykazów, o których mowa w ust. 4 i 5, oraz wzoru i metodyki, o których mowa w ust. 6, przedkłada się Komisji w terminie do dnia [Urząd Publikacji = 9 miesięcy od rozpoczęcia stosowania niniejszego rozporządzenia] r. Komisja, po należytym rozpatrzeniu wniosków, dokonuje ich przeglądu w razie potrzeby i jest uprawniona do przyjęcia ich w drodze aktu wykonawczego zgodnie z procedurą sprawdzającą określoną w art. 93 ust. 2.

6b. Wykazy oraz wzór i metodykę, o których mowa w ust. 6a, poddaje się przeglądowi co najmniej raz na trzy lata i w razie potrzeby aktualizuje. Rada przedkłada Komisji w odpowiednim czasie swoją ocenę i ewentualne propozycje aktualizacji. Po należytym rozpatrzeniu wniosków Komisja dokonuje ich przeglądu i jest uprawniona do przyjmowania wszelkich aktualizacji zgodnie z procedurą określoną w ust. 6a.

6c. Wykazy rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych oraz rodzajów operacji przetwarzania, w przypadku których nie jest wymagana ocena skutków dla ochrony danych, sporządzone i podane do wiadomości publicznej przez organy nadzorcze, pozostają ważne do czasu przyjęcia przez Komisję aktu wykonawczego, o którym mowa w ust. 6a.”;

10. dodaje się artykuł w brzmieniu:

„Artykuł 41a

1) Komisja może przyjmować akty wykonawcze w celu określenia środków i kryteriów służących ustaleniu, czy dane wynikające z pseudonimizacji nie stanowią już danych osobowych dla niektórych podmiotów.

2) Na potrzeby ust. 1 Komisja:

a) ocenia aktualny stan wiedzy w zakresie dostępnych technik;

b) opracowuje kryteria lub kategorie dla administratorów i odbiorców w celu oceny ryzyka deanonimizacji w odniesieniu do typowych odbiorców danych.

3) Wdrożenie środków i kryteriów określonych w akcie wykonawczym można wykorzystać jako element do wykazania, że dane nie mogą prowadzić do deanonimizacji osób, których dane dotyczą.

4) Komisja ściśle angażuje EROD w przygotowanie aktów wykonawczych. EROD wydaje opinię na temat projektów aktów wykonawczych w terminie ośmiu tygodni od otrzymania projektu od Komisji.

5) Akt wykonawczy zostaje przyjęty zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 3.”;

11. w art. 57 ust. 1 wprowadza się następujące zmiany:

(a) uchyla się lit. k);

12. w art. 64 ust. 1 skreśla się lit. a);

13. w art. 70 ust. 1 uchyla się lit. h);

14. w art. 70 ust. 1 dodaje się litery w brzmieniu:

„ha) przygotowuje i przekazuje Komisji wniosek dotyczący wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych i operacji, w przypadku których nie jest wymagana ocena skutków dla ochrony danych, zgodnie z art. 35;

hb) przygotowuje i przekazuje Komisji wniosek dotyczący wspólnego wzoru i wspólnej metodyki przeprowadzania ocen skutków dla ochrony danych, zgodnie z art. 35;

hc) przygotowuje i przekazuje Komisji wniosek dotyczący wspólnego wzoru zawiadomienia właściwego organu nadzorczego o naruszeniu ochrony danych osobowych, a także wykazu okoliczności, w których naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej zgodnie z art. 33;”;

15. po art. 88 dodaje się artykuły w brzmieniu:

„Artykuł 88a

Przetwarzanie danych osobowych w końcowych urządzeniach osób fizycznych

1) Przechowywanie danych osobowych lub uzyskiwanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej jest dozwolone wyłącznie za zgodą tej osoby, zgodnie z niniejszym rozporządzeniem.

2) Ust. 1 nie wyklucza przechowywania danych osobowych lub uzyskiwania dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby

fizycznej na podstawie prawa Unii lub prawa państwa członkowskiego w rozumieniu art. 6 i z zastrzeżeniem warunków określonych w tym artykule, aby zabezpieczyć cele, o których mowa w art. 23 ust. 1.

3) Przechowywanie danych osobowych lub uzyskiwanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej bez zgody oraz ich dalsze przetwarzanie są zgodne z prawem w zakresie, w jakim jest to niezbędne do:

   a) wykonywania transmisji komunikatu elektronicznego za pośrednictwem sieci łączności elektronicznej;

   b) świadczenia usługi wyraźnie zażądanej przez osobę, której dane dotyczą;

   c) tworzenia zagregowanych informacji na temat korzystania z usługi online w celu pomiaru odbiorców takiej usługi, w przypadku gdy dokonuje tego administrator tej usługi online wyłącznie na swój własny użytek;

   d) utrzymania lub przywrócenia bezpieczeństwa usługi świadczonej przez administratora i żądanej przez osobę, której dane dotyczą, lub końcowego urządzenia wykorzystywanego do świadczenia takiej usługi.

4) W przypadku gdy przechowywanie danych osobowych lub uzyskiwanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej odbywa się na podstawie zgody, zastosowanie mają następujące zasady:

   a) osoba, której dane dotyczą, ma możliwość odrzucenia wniosków o wyrażenie zgody w łatwy i zrozumiały sposób za pomocą pojedynczego przycisku lub równoważnego środka;

   b) jeżeli osoba, której dane dotyczą, wyraża zgodę, administrator nie występuje z nowym wnioskiem o wyrażenie zgody w tym samym celu przez okres, w którym administrator może zgodnie z prawem polegać na zgodzie osoby, której dane dotyczą;

   c) jeżeli osoba, której dane dotyczą, odrzuci wniosek o wyrażenie zgody, administrator nie występuje z nowym wnioskiem o wyrażenie zgody w tym samym celu przez okres co najmniej sześciu miesięcy.

   Niniejszy ustęp ma również zastosowanie do dalszego przetwarzania danych osobowych na podstawie zgody.

5) Niniejszy artykuł stosuje się od dnia [Urząd Publikacji: proszę wstawić datę przypadającą 6 miesięcy po dacie wejścia w życie niniejszego rozporządzenia] r.

Artykuł 88b

Zautomatyzowane i nadające się do odczytu maszynowego wskazania wyborów dokonanych przez osobę, której dane dotyczą, w odniesieniu do przetwarzania danych osobowych w końcowym urządzeniu osób fizycznych

1) Administratorzy zapewniają, aby ich interfejsy internetowe umożliwiały osobom, których dane dotyczą:

   a) wyrażenie zgody w sposób zautomatyzowany i nadający się do odczytu maszynowego, o ile spełnione są warunki zgody określone w niniejszym rozporządzeniu;

b) odrzucenie wniosku o wyrażenie zgody i wykonanie prawa sprzeciwu zgodnie z art. 21 ust. 2 w sposób zautomatyzowany i nadający się do odczytu maszynowego.

2) Administratorzy szanują wybory dokonane przez osoby, których dane dotyczą, zgodnie z ust. 1.

3) Ust. 1 i 2 nie mają zastosowania do administratorów, którzy są dostawcami usług medialnych, podczas świadczenia usługi medialnej.

4) Zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012 Komisja zwraca się do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie norm dotyczących interpretacji nadających się do odczytu maszynowego wskazań wyborów dokonanych przez osoby, których dane dotyczą.

W przypadku interfejsów internetowych administratorów zgodnych z normami zharmonizowanymi, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, lub z ich częściami, domniemywa się, że spełniają one wymogi objęte tymi normami lub ich częściami, o których mowa w ust. 1.

5) Ust. 1 i 2 stosuje się od dnia [Urząd Publikacji: proszę wstawić datę przypadającą 24 miesiące po dacie wejścia w życie niniejszego rozporządzenia] r.

6) Dostawcy przeglądarek internetowych, którzy nie są MŚP, zapewniają środki techniczne umożliwiające osobom, których dane dotyczą, wyrażenie zgody i odrzucenie wniosku o wyrażenie zgody oraz wykonanie prawa sprzeciwu na podstawie art. 21 ust. 2 w sposób zautomatyzowany i nadający się do odczytu maszynowego, o którym mowa w ust. 1 niniejszego artykułu, stosowany zgodnie z ust. 2–5 niniejszego artykułu.

7) Ust. 6 stosuje się od dnia [Urząd Publikacji: proszę wstawić datę przypadającą 48 miesięcy po dacie wejścia w życie niniejszego rozporządzenia] r.

Artykuł 88c

Przetwarzanie w kontekście rozwoju i eksploatacji AI

Jeżeli przetwarzanie danych osobowych jest niezbędne dla interesów administratora w kontekście rozwoju i eksploatacji systemu AI zdefiniowanego w art. 3 pkt 1 rozporządzenia (UE) 2024/1689 lub modelu AI, takie przetwarzanie można prowadzić ze względu na prawnie uzasadnione interesy w rozumieniu art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679, w stosownych przypadkach, z wyjątkiem sytuacji, w których inne przepisy unijne lub krajowe wyraźnie wymagają zgody, oraz gdy_nadrzędny charakter wobec takich interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Wszelkie takie przetwarzanie podlega odpowiednim środkom organizacyjnym i technicznym oraz zabezpieczeniom praw i wolności osoby, której dane dotyczą, takim jak zapewnienie poszanowania minimalizacji danych na etapie wyboru źródeł oraz trenowania i testowania systemu AI lub modelu AI, ochrona przed nieujawnieniem rezydualnie zatrzymanych danych w systemie AI lub modelu AI w celu zapewnienia większej przejrzystości osobom, których dane dotyczą, oraz zapewnienie osobom, których dane dotyczą, bezwarunkowego prawa sprzeciwu wobec przetwarzania ich danych osobowych.”.

Artykuł 4

Zmiany w rozporządzeniu (UE) 2018/1725 (EUDPR)

W rozporządzeniu (UE) 2018/1725 wprowadza się następujące zmiany:

1. w art. 3 wprowadza się następujące zmiany:

   (a) w pkt 1 dodaje się zdania w brzmieniu:

   „Informacje dotyczące osoby fizycznej niekoniecznie są danymi osobowymi dla każdej innej osoby lub każdego innego podmiotu z tego tylko powodu, że inny podmiot może zidentyfikować tę osobę fizyczną. Informacje nie mają charakteru danych osobowych dla danego podmiotu, jeżeli podmiot ten nie może zidentyfikować osoby fizycznej, której dotyczą informacje, biorąc pod uwagę środki, co do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez ten podmiot. Takie informacje nie stają się dla tego podmiotu danymi osobowymi z tego tylko powodu, że potencjalny kolejny odbiorca dysponuje środkami, co do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane do zidentyfikowania osoby fizycznej, której informacje te dotyczą;”;

   (b) pkt 25 otrzymuje brzmienie:

   „25) w przypadku »sieci łączności elektronicznej« zastosowanie ma definicja zawarta w art. 2 pkt 1 dyrektywy (UE) 2018/1972;”;

   (c) dodaje się punkty w brzmieniu:

   „27) »aplikacja mobilna« oznacza aplikację mobilną zdefiniowaną w art. 3 pkt 2 dyrektywy (UE) 2016/2102;

   28) »interfejs internetowy« oznacza interfejs internetowy zgodnie z definicją w art. 3 lit. m) rozporządzenia (UE) 2022/2065;

   29) »badania naukowe« oznaczają wszelkie badania, które mogą również wspierać innowacje, takie jak rozwój technologiczny i demonstracja. Działania te przyczyniają się do rozwoju istniejącej wiedzy naukowej lub wykorzystują istniejącą wiedzę w nowatorski sposób, są prowadzone w celu przyczynienia się do rozwoju ogólnej wiedzy i dobrostanu społeczeństwa oraz są zgodne z normami etycznymi w odpowiedniej dziedzinie badań naukowych. Nie wyklucza to, że badania mogą mieć również na celu realizację interesu handlowego.”;

2. art. 4 ust. 1 lit. b) otrzymuje brzmienie:

   „b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych jest uznawane w myśl art. 13 za zgodne z pierwotnymi celami, niezależnie od warunków określonych w art. 6 niniejszego rozporządzenia (»ograniczenie celu«);”;

3. w art. 10 wprowadza się następujące zmiany:

   (a) w ust. 2 dodaje się litery w brzmieniu:

„k) przetwarzanie odbywa się w kontekście rozwoju i eksploatacji systemu AI zdefiniowanego w art. 3 pkt 1 rozporządzenia (UE) 2024/1689 lub modelu AI, z zastrzeżeniem warunków, o których mowa w ust. 4; -

l) przetwarzanie danych biometrycznych jest niezbędne do potwierdzenia tożsamości osoby, której dane dotyczą (weryfikacja), w przypadku gdy dane biometryczne lub środki niezbędne do weryfikacji znajdują się pod wyłączną kontrolą osoby, której dane dotyczą.”;

(b) dodaje się ust. 4 w brzmieniu:

„4. W odniesieniu do przetwarzania, o którym mowa w ust. 2 lit. k), wdraża się odpowiednie środki organizacyjne i techniczne, aby uniknąć gromadzenia i innego przetwarzania szczególnych kategorii danych osobowych. Jeżeli pomimo wdrożenia takich środków administrator zidentyfikuje szczególne kategorie danych osobowych w zbiorach danych wykorzystywanych do trenowania, testowania lub walidacji bądź w systemie AI lub modelu AI, usuwa takie dane. Jeżeli usunięcie tych danych wymaga niewspółmiernie dużego wysiłku, administrator w każdym przypadku skutecznie i bez zbędnej zwłoki chroni takie dane przed wykorzystaniem do uzyskania wyników, przed ujawnieniem lub udostępnieniem w inny sposób stronom trzecim.”;

4. art. 14 ust. 5 otrzymuje brzmienie:

„5. Informacje podawane na mocy art. 15 i 16 oraz komunikacja i działania podejmowane na mocy art. 17–24 i 35 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, lub również, w przypadku żądań na podstawie art. 17, ponieważ osoba, której dane dotyczą, nadużywa praw przyznanych jej na mocy niniejszego rozporządzenia do celów innych niż ochrona jej danych, administrator może odmówić podjęcia żądanych działań. Na administratorze spoczywa obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony charakter lub że istnieją uzasadnione podstawy, by sądzić, że jest on nadmierny.”;

5. w art. 15 dodaje się nowy ust. 5 w brzmieniu:

„5. Jeżeli przetwarzanie odbywa się do celów badań naukowych, a udzielenie informacji, o których mowa w ust. 1, 2 i 3, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 13, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania, administrator nie musi udzielać informacji, o których mowa w ust. 1, 2 i 3. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie.”;

6. art. 24 ust. 1 i 2 otrzymują brzmienie:

„1. Decyzja, która wywołuje skutki prawne dla osoby, której dane dotyczą, lub w podobny sposób istotnie na nią wpływa, może opierać się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, tylko wtedy, gdy decyzja ta:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem danych, niezależnie od tego, czy decyzję można by podjąć w sposób inny niż wyłącznie zautomatyzowany;

b) jest dozwolona prawem Unii, któremu podlega administrator i które przewiduje również właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.";

7. art. 34 ust. 1 otrzymuje brzmienie:

„1. W przypadku naruszenia ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 96 godzin po stwierdzeniu tego naruszenia – zgłasza je Europejskiemu Inspektorowi Ochrony Danych. Do zgłoszenia, które przekazano Europejskiemu Inspektorowi Ochrony Danych po upływie 96 godzin, dołącza się wyjaśnienie przyczyn opóźnienia.";

8. w art. 37 dodaje się następujące ustępy:

„2. Przechowywanie danych osobowych lub uzyskiwanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej jest dozwolone wyłącznie za zgodą tej osoby, zgodnie z niniejszym rozporządzeniem.

3. Ust. 1 nie wyklucza przechowywania danych osobowych lub uzyskiwania dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej na podstawie prawa Unii w rozumieniu art. 5 i z zastrzeżeniem warunków określonych w tym artykule, aby zabezpieczyć cele, o których mowa w art. 25 ust. 1.

4. Przechowywanie danych osobowych lub uzyskiwanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej bez zgody oraz ich dalsze przetwarzanie są zgodne z prawem w zakresie, w jakim jest to niezbędne do:

a) wykonywania transmisji komunikatu elektronicznego za pośrednictwem sieci łączności elektronicznej;

b) świadczenia usługi wyraźnie zażądanej przez osobę, której dane dotyczą;

c) tworzenia zagregowanych informacji na temat korzystania z usługi online w celu pomiaru odbiorców takiej usługi, w przypadku gdy dokonuje tego administrator tej usługi online wyłącznie na swój własny użytek;

d) utrzymania lub przywrócenia bezpieczeństwa usługi świadczonej przez administratora i żądanej przez osobę, której dane dotyczą, lub końcowego urządzenia wykorzystywanego do świadczenia takiej usługi.

5. W przypadku gdy przechowywanie danych osobowych lub uzyskiwanie dostępu do danych osobowych już przechowywanych w końcowym urządzeniu osoby fizycznej odbywa się na podstawie zgody, zastosowanie mają następujące zasady:

a) osoba, której dane dotyczą, ma możliwość odrzucenia wniosków o wyrażenie zgody w łatwy i zrozumiały sposób za pomocą pojedynczego przycisku lub równoważnego środka;

b) jeżeli osoba, której dane dotyczą, wyraża zgodę, administrator nie występuje z nowym wnioskiem o wyrażenie zgody w tym samym celu przez okres, w którym administrator może zgodnie z prawem polegać na zgodzie osoby, której dane dotyczą;

c) jeżeli osoba, której dane dotyczą, odrzuci wniosek o wyrażenie zgody, administrator nie występuje z nowym wnioskiem o wyrażenie zgody w tym samym celu przez okres co najmniej sześciu miesięcy.

Niniejszy ustęp ma również zastosowanie do dalszego przetwarzania danych osobowych na podstawie zgody.

6. Niniejszy artykuł stosuje się od dnia [Urząd Publikacji: proszę wstawić datę przypadającą 6 miesięcy po dacie wejścia w życie niniejszego rozporządzenia] r.

7. Administratorzy zapewniają, aby ich interfejsy internetowe umożliwiały osobom, których dane dotyczą:

a) wyrażenie zgody w sposób zautomatyzowany i nadający się do odczytu maszynowego, o ile spełnione są warunki zgody określone w niniejszym rozporządzeniu;

b) odrzucenie wniosku o wyrażenie zgody w sposób zautomatyzowany i nadający się do odczytu maszynowego.

8. Administratorzy szanują wybory dokonane przez osoby, których dane dotyczą, zgodnie z ust. 7.

9. W przypadku interfejsów internetowych administratorów zgodnych z normami zharmonizowanymi lub ich częściami, o których mowa w art. 88b ust. 4 rozporządzenia (UE) 2016/679, domniemywa się, że spełniają one wymogi objęte tymi normami lub ich częściami, o których mowa w ust. 7.

10. Ust. 7–9 stosuje się od dnia [Urząd Publikacji: proszę wstawić datę przypadającą 24 miesiące po dacie wejścia w życie niniejszego rozporządzenia] r.”;

8) w art. 39 wprowadza się następujące zmiany:

a) ust. 4 otrzymuje brzmienie:

„4. Przyjęte przez Komisję wykazy, wzór i metodyka, o których mowa w art. 35 ust. 6a rozporządzenia (UE) 2016/679, powinny mieć zastosowanie do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.”;

b) skreśla się ust. 5 i 6;

9) dodaje się artykuł w brzmieniu:

„Artykuł 45a

Przyjęte przez Komisję wspólne kryteria, o których mowa w art. 41a rozporządzenia (UE) 2016/679, powinny mieć zastosowanie do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.”.

Artykuł 5

Zmiany w dyrektywie 2002/58/WE (dyrektywa o e-prywatności)

W dyrektywie 2002/58/WE wprowadza się następujące zmiany:

1. uchyla się art. 4;

2. po art. 5 ust. 3 dodaje się akapit w brzmieniu:

„Niniejszy ustęp nie ma zastosowania, jeżeli abonent lub użytkownik jest osobą fizyczną, a przechowywane informacje lub informacje, do których uzyskuje się dostęp, stanowią przetwarzanie danych osobowych lub do niego prowadzą.”.

Artykuł 6

Zmiany w dyrektywie (UE) 2022/2555

W dyrektywie (UE) 2022/2555 wprowadza się następujące zmiany:

1. Dodaje się art. 23a w brzmieniu:

„Artykuł 23a

Pojedynczy punkt kontaktowy do zgłaszania incydentów

1) ENISA opracowuje i utrzymuje pojedynczy punkt kontaktowy w celu wsparcia obowiązku zgłaszania incydentów i powiązanych zdarzeń na podstawie aktów prawnych Unii, jeżeli tak przewidziano w tych aktach prawnych Unii (»pojedynczy punkt kontaktowy«). Bez uszczerbku dla art. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 ENISA może zapewnić, aby pojedynczy punkt kontaktowy opierał się na pojedynczej platformie sprawozdawczej ustanowionej na mocy tego rozporządzenia.

2) ENISA wprowadza odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa pojedynczego punktu kontaktowego oraz informacji przekazywanych lub rozpowszechnianych za pośrednictwem pojedynczego punktu kontaktowego. ENISA uwzględnia wrażliwość informacji przekazywanych lub rozpowszechnianych na podstawie aktów prawnych Unii, o których mowa w ust. 1, oraz zapewnia, aby właściwe organy na podstawie tych aktów prawnych Unii miały dostęp do informacji i przetwarzały je zgodnie z wymogami tych aktów prawnych Unii.

3) ENISA zapewnia i wdraża specyfikacje dotyczące środków technicznych, operacyjnych i organizacyjnych związanych z utworzeniem, utrzymaniem i bezpiecznym funkcjonowaniem pojedynczego punktu kontaktowego. ENISA opracowuje specyfikacje we współpracy z Komisją, siecią CSIRT i właściwymi organami na podstawie aktów prawnych Unii, o których mowa w ust. 1. Specyfikacje zapewniają, aby:

a) zagwarantowano niezbędną zdolność w zakresie interoperacyjności w odniesieniu do innych odpowiednich obowiązków zgłaszania, o których mowa w ust. 1;

b) wprowadzono rozwiązania techniczne umożliwiające odpowiednim podmiotom i organom na mocy aktów prawnych Unii, o których mowa w ust. 1, dostęp do informacji, ich przekazywanie, pobieranie, przesyłanie lub przetwarzanie w inny sposób z pojedynczego punktu kontaktowego oraz zapewniono protokoły i narzędzia techniczne umożliwiające podmiotom i organom dalsze przetwarzanie otrzymanych informacji w ich systemach;

c) należycie uwzględniono specyfikę wymogów dotyczących zgłaszania incydentów określonych w aktach prawnych Unii, o których mowa w ust. 1;

d) w stosownych przypadkach pojedynczy punkt kontaktowy był interoperacyjny i kompatybilny z europejskimi portfelami biznesowymi, o których mowa w *[wniosek dotyczący rozporządzenia: wstawić tytuł wniosku]*, oraz aby europejskie portfele biznesowe mogły być wykorzystywane co najmniej do identyfikacji i uwierzytelniania podmiotów za pomocą pojedynczego punktu kontaktowego;

e) podmioty korzystające z pojedynczego punktu kontaktowego mogły pobierać i uzupełniać informacje, które wcześniej przekazały za pośrednictwem pojedynczego punktu kontaktowego;

f) pojedyncze zgłoszenie informacji przekazanych przez podmiot za pośrednictwem pojedynczego punktu kontaktowego mogło być wykorzystane do wypełnienia obowiązków w zakresie zgłaszania określonych w dowolnym z pozostałych aktów prawnych Unii, które przewidują zgłaszanie incydentów do pojedynczego punktu kontaktowego.

4) O ile nie przewidziano tego w aktach prawnych Unii, o których mowa w ust. 1 niniejszego artykułu, ENISA nie może mieć dostępu do zgłoszeń przekazywanych za pośrednictwem pojedynczego punktu kontaktowego.

5) W okresie [18] miesięcy od wejścia w życie niniejszego rozporządzenia ENISA pilotuje funkcjonowanie pojedynczego punktu kontaktowego w odniesieniu do każdego dodanego aktu prawnego Unii, w tym testowanie, które uwzględnia specyfikę i wymogi dotyczące zgłoszeń określone w każdym odpowiednim akcie prawnym Unii, oraz po konsultacji z Komisją i odpowiednimi właściwymi organami na podstawie odpowiednich aktów prawnych Unii. ENISA umożliwia zgłaszanie incydentów na podstawie każdego aktu prawnego Unii, o którym mowa w ust. 1, dopiero po przeprowadzeniu pilotażu funkcjonowania i po opublikowaniu przez Komisję zawiadomienia na podstawie ust. 6.

6) Komisja, we współpracy z ENISA, ocenia właściwe funkcjonowanie, niezawodność, integralność i poufność pojedynczego punktu kontaktowego. Jeżeli Komisja, po konsultacji z siecią CSIRT i właściwymi organami na podstawie aktów prawnych Unii, o których mowa w ust. 1, stwierdzi, że pojedynczy punkt kontaktowy zapewnia właściwe funkcjonowanie, niezawodność, integralność i poufność, publikuje zawiadomienie w tej sprawie w *Dzienniku Urzędowym Unii Europejskiej*.

7) W przypadku gdy Komisja stwierdzi w swojej ocenie, że pojedynczy punkt kontaktowy nie zapewnia właściwego funkcjonowania, niezawodności, integralności lub poufności, ENISA niezwłocznie wprowadza, we współpracy z Komisją i bez zbędnej zwłoki, wszelkie niezbędne środki naprawcze w celu zapewnienia

właściwego funkcjonowania, niezawodności, integralności lub poufności oraz informuje Komisję o wynikach. Następnie Komisja ponownie ocenia właściwe funkcjonowanie, niezawodność, integralność lub poufność pojedynczego punktu kontaktowego i publikuje zawiadomienie zgodnie z ust. 6.”;

2. w art. 23 wprowadza się następujące zmiany:

a) ust. 1 zdanie pierwsze otrzymuje brzmienie:

„Każde państwo członkowskie zapewnia, aby podmioty kluczowe i ważne bez zbędnej zwłoki zgłaszały swojemu właściwemu CSIRT lub, jeżeli ma to zastosowanie, swojemu właściwemu organowi zgodnie z ust. 4 niniejszego artykułu każdy incydent mający istotny wpływ na świadczenie przez nie usług, o których mowa w ust. 3 niniejszego artykułu (znaczący incydent), za pośrednictwem pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a.”;

a) dodaje się ust. 12 w brzmieniu:

„W przypadku gdy producent zgłasza poważny incydent zgodnie z art. 14 ust. 3 rozporządzenia (UE) 2024/2847, a zgłoszenie incydentu na podstawie tego artykułu zawiera istotne informacje wymagane na podstawie ust. 4 niniejszego artykułu, zgłoszenie dokonywane przez producenta na podstawie art. 14 ust. 3 rozporządzenia (UE) 2024/2847 stanowi zgłoszenie informacji na podstawie ust. 4 niniejszego artykułu.”;

3. art. 30 ust. 1 otrzymuje brzmienie:

„1. Państwa członkowskie zapewniają, by w uzupełnieniu obowiązków zgłaszania, o których mowa w art. 23, następujące podmioty mogły dobrowolnie przekazywać zgłoszenia CSIRT lub, w stosownych przypadkach, właściwym organom, na zasadzie dobrowolności za pośrednictwem pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a:

a) podmioty kluczowe i ważne w przypadku incydentów, cyberzagrożeń i potencjalnych zdarzeń dla cyberbezpieczeństwa;

b) podmioty inne niż te, o których mowa w lit. a), niezależnie od tego, czy są objęte zakresem stosowania niniejszej dyrektywy, w odniesieniu do poważnych incydentów, cyberzagrożeń oraz potencjalnych zdarzeń dla cyberbezpieczeństwa.”;

Artykuł 7

Zmiana rozporządzenia (UE) nr 910/2014

W rozporządzeniu (UE) 910/2014 wprowadza się następujące zmiany:

1. w art. 19a dodaje się ust. 1a w brzmieniu:

„1a. Powiadomienia na podstawie ust. 1 lit. b) niniejszego artykułu przekazywane są organowi nadzorczemu oraz, w stosownych przypadkach, innym odpowiednim właściwym organom za pośrednictwem pojedynczego punktu kontaktowego zgodnie z art. 23a dyrektywy (UE) 2022/2555.”;

2. w art. 24 dodaje się ust. 2a w brzmieniu:

„2a. Powiadomienia na podstawie ust. 2 lit. fb) niniejszego artykułu przekazywane są organowi nadzorczemu oraz, w stosownych przypadkach, innym odpowiednim właściwym organom za pośrednictwem pojedynczego punktu kontaktowego zgodnie z art. 23a dyrektywy (UE) 2022/2555.”;

3. w art. 45a dodaje się ust. 3a w brzmieniu:

„3a. Powiadomienia na podstawie ust. 3 przekazywane są Komisji i właściwemu organowi nadzorczemu za pośrednictwem pojedynczego punktu kontaktowego zgodnie z art. 23a dyrektywy (UE) 2022/2555.”.

Artykuł 8

Zmiany w rozporządzeniu (UE) 2022/2554

W art. 19 rozporządzenia (UE) 2022/2554 wprowadza się następujące zmiany:

1. ust. 1 akapit pierwszy otrzymuje brzmienie:

„Podmioty finansowe zgłaszają poważne incydenty związane z ICT odpowiedniemu właściwemu organowi, o którym mowa w art. 46, za pośrednictwem pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555, zgodnie z ust. 4 niniejszego artykułu.”;

2. ust. 2 akapit pierwszy otrzymuje brzmienie:

„Podmioty finansowe mogą dobrowolnie powiadomić za pośrednictwem pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555 odpowiedni właściwy organ o znaczących cyberzagrożeniach, jeżeli uznają dane zagrożenie za istotne dla systemu finansowego, użytkowników usług lub klientów. Odpowiedni właściwy organ może przekazać takie informacje innym odpowiednim organom, o których mowa w ust. 6.”.

Artykuł 9

Zmiany w dyrektywie (UE) 2022/2557

W art. 15 dyrektywy (UE) 2022/2557 wprowadza się następujące zmiany:

1. w ust. 1 zdanie pierwsze otrzymuje brzmienie:

„Państwa członkowskie zapewniają, aby podmioty krytyczne bez zbędnej zwłoki zgłaszały właściwemu organowi, za pośrednictwem pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555, incydenty, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych.”;

2. w ust. 2 dodaje się akapit w brzmieniu:

„Komisja może przyjmować akty wykonawcze doprecyzowujące rodzaj i format informacji zgłaszanych na podstawie art. 15 ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 24 ust. 2.”.

Artykuł 10

Uchylenia i klauzule przejściowe

1. Rozporządzenie (UE) 2019/1150 traci moc z dniem [data = rozpoczęcie stosowania niniejszego rozporządzenia] r.

2. Na zasadzie odstępstwa od ust. 1 następujące przepisy pozostają w mocy do dnia 31 grudnia 2032 r.:

   (a) art. 2 pkt 1;

   (b) art. 2 pkt 2;

   (c) art. 2 pkt 5;

   (d) art. 4;

   (e) art. 11;

   (f) art. 15.

3. Następujące akty tracą moc ze skutkiem od dnia [data dostosowana do daty rozpoczęcia stosowania zmian] r.:

   a) rozporządzenie (UE) 2022/868;

   b) rozporządzenie (UE) 2018/1807;

   c) dyrektywa (UE) 2019/1024.

4. Odesłania do rozporządzenia (UE) 2022/868, rozporządzenia (UE) 2018/1807 i dyrektywy 2019/1024 odczytuje się zgodnie z tabelą korelacji zawartą w załączniku I do niniejszego rozporządzenia.

Artykuł 11

Przepisy końcowe

Niniejsze rozporządzenie wchodzi w życie trzeciego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

W drodze odstępstwa od ust. 3 art. 5 ust. 2 wchodzi w życie 6 miesięcy po publikacji w *Dzienniku Urzędowym Unii Europejskiej*.

Art. 3 ust. 8 lit. a)–c), art. 6 ust. 2 i 3 oraz art. 7–9 wchodzą w życie 18 miesięcy od wejścia w życie niniejszego rozporządzenia. W drodze odstępstwa od zdania pierwszego, w przypadku gdy Komisja stwierdzi w swojej ocenie na podstawie art. 23a ust. 7 dyrektywy (UE) 2022/2555, że pojedynczy punkt kontaktowy nie zapewnia właściwego funkcjonowania, niezawodności, integralności lub poufności, obowiązki w zakresie dokonywania zgłoszeń za pośrednictwem pojedynczego punktu kontaktowego określone w art. 23 ust. 4 dyrektywy (UE) 2022/2555, art. 19a ust. 1a, art. 24 ust. 2a i art. 45a ust. 3a rozporządzenia (UE) nr 910/2014, art. 33 ust. 1 rozporządzenia (UE) 2016/679, art. 19 ust. 1 i 2 rozporządzenia (UE)

2022/2554 oraz art. 15 ust. 1 dyrektywy (UE) 2022/2557 wchodzą w życie 24 miesiące od wejścia w życie niniejszego rozporządzenia.

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

Sporządzono w Brukseli dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH I CYFROWYCH REGULACJI

1.STRUKTURA WNIOSKU/INICJATYWY 3
1.1.Tytuł wniosku/inicjatywy 3
1.2.Obszary polityki, których dotyczy wniosek/inicjatywa 3
1.3.Cel(e) 3
1.3.1.Cel(e) ogólny(-e) 3
1.3.2.Cel(e) szczegółowy(-e) 3
1.3.3.Oczekiwane wyniki i wpływ 3
1.3.4.Wskaźniki dotyczące realizacji celów 3
1.4.Wniosek/inicjatywa dotyczy: 4
1.5.Uzasadnienie wniosku/inicjatywy 4
1.5.1. ... Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy 4
1.5.2. ..... Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tej sekcji „wartość dodaną z tytułu zaangażowania Unii Europejskiej" należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie. 4
1.5.3.Główne wnioski wyciągnięte z podobnych działań 4
1.5.4. ..... Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami 5
1.5.5. ..... Ocena różnych dostępnych możliwości finansowania, w tym możliwości przegrupowania środków 5
1.6.Czas trwania wniosku/inicjatywy i jego/jej wpływu finansowego 6
1.7.Planowane metody wykonania budżetu 6
2.ŚRODKI ZARZĄDZANIA 8
2.1.Zasady nadzoru i sprawozdawczości 8
2.2.System zarządzania i kontroli 8
2.2.1. ..... Uzasadnienie dla proponowanych metod wykonania budżetu, mechanizmów finansowania wykonania, sposobów dokonywania płatności i strategii kontroli 8
2.2.2. ..... Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia 8
2.2.3. ..... Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu) 8
2.3.Środki zapobiegania nadużyciom finansowym i nieprawidłowościom 9

3.SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY 10
3.1. ..... Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ 10
3.2.Szacunkowy wpływ finansowy wniosku na środki 12
3.2.1.Podsumowanie szacunkowego wpływu na środki operacyjne 12
3.2.1.1.Środki z uchwalonego budżetu 12
3.2.1.2.Środki z zewnętrznych dochodów przeznaczonych na określony cel 17
3.2.2.Przewidywany produkt finansowany ze środków operacyjnych 22
3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne 24
3.2.3.1. Środki z uchwalonego budżetu 24
3.2.3.2.Środki z zewnętrznych dochodów przeznaczonych na określony cel 24
3.2.3.3.Ogółem środki 24
3.2.4.Szacowane zapotrzebowanie na zasoby ludzkie 25
3.2.4.1. Finansowane z uchwalonego budżetu 25
3.2.4.2.Finansowane z zewnętrznych dochodów przeznaczonych na określony cel 26
3.2.4.3.Zapotrzebowanie na zasoby ludzkie ogółem 26
3.2.5.Przegląd szacowanego wpływu na inwestycje związane z technologiami cyfrowymi 28
3.2.6.Zgodność z obowiązującymi wieloletnimi ramami finansowymi 28
3.2.7.Udział osób trzecich w finansowaniu 28
3.3.Szacunkowy wpływ na dochody 29
4.WYMIAR CYFROWY 29
4.1.Wymogi cyfrowe 30
4.2.Dane 30
4.3.Rozwiązania cyfrowe 31
4.4.Ocena interoperacyjności 31
4.5.Środki wspierające cyfrowe wdrażanie 32

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie uproszczenia dorobku prawnego UE w dziedzinie cyfrowej, zmiany rozporządzenia (UE) 2023/2854, rozporządzenia (UE) 2016/679, rozporządzenia (UE) 2024/1689 oraz dyrektywy 2002/58/WE i dyrektywy (UE) 2022/2555 oraz uchylenia rozporządzenia (UE) 2022/868, rozporządzenia (UE) 2018/1807, rozporządzenia (UE) 2019/1150 i dyrektywy (UE) 2019/1024 (pakiet aktów zbiorczych dotyczących cyfrowego dorobku prawnego UE)

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

Sieci komunikacyjne, treści i technologie;

Rynek wewnętrzny, przemysł, przedsiębiorczość i MŚP

1.3. Cel(e)

1.3.1. Cel(e) ogólny(-e)

Uproszczenie stosowania cyfrowego dorobku prawnego UE i oszczędność kosztów dla przedsiębiorstw

1.3.2. Cel(e) szczegółowy(-e)

Cel szczegółowy nr 1

Poprawa zarządzania i skutecznego egzekwowania cyfrowego dorobku prawnego UE dzięki zmniejszeniu złożoności przepisów, kosztów administracyjnych dla przedsiębiorstw i administracji oraz uchyleniu aktów prawnych

Cel szczegółowy nr 2

Zapewnienie pojedynczego punktu kontaktowego do zgłaszania incydentów w kilku ramach prawnych

1.3.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Zmniejszenie kosztów ponoszonych przez przedsiębiorstwa w wyniku ograniczenia złożoności przepisów i usprawnienia zgłaszania

1.3.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

Wskaźnik 1

Obliczone obniżone koszty dla przedsiębiorstw

Wskaźnik 2

Oszczędności kosztów związane ze zgłaszaniem incydentów przez przedsiębiorstwa

Wskaźnik 3

1.4. Wniosek/inicjatywa dotyczy:

☐ nowego działania

☐ nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego[39]

☒ przedłużenia bieżącego działania

☐ połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Wejście w życie spodziewane jest w ciągu 3 dni od publikacji w Dzienniku Urzędowym Unii Europejskiej. *Rozpoczęcie stosowania powinno nastąpić natychmiast, z istotnymi wyjątkami w odniesieniu do przepisów, które wymagają okresu przejściowego. W przypadku rozdziału III dotyczącego zgłaszania incydentów i przepisów dotyczących platform wymagany jest wystarczający okres na wdrożenie, który jest dostosowany do potrzeb przedsiębiorstw, państw członkowskich i organów UE.*

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tej sekcji „wartość dodaną z tytułu zaangażowania Unii Europejskiej" należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Przyczyny działania na szczeblu UE wynikają z faktu, że zmiany dotyczą obowiązującego prawodawstwa UE i zmniejszają złożoność prawa UE (*ex ante*). Oczekiwana wygenerowana unijna wartość dodana (*ex post*) polega na usprawnieniu prawa UE oraz zmniejszeniu obciążeń administracyjnych i kosztów dla przedsiębiorstw. W przypadku ustanowienia pojedynczego punktu kontaktowego do zgłaszania incydentów szczególna wartość dodana wynika z zapewnienia rozwiązania na szczeblu Unii, które spełnia wymogi krajowe. Zapewnienie jednego punktu optymalizuje koszty dla przedsiębiorstw, niezależnie od tego, gdzie w Unii zlokalizowany jest podmiot dokonujący zgłoszenia i jakie organy są upoważnione do przyjmowania zgłoszeń.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Zmiany w odpowiednich rozporządzeniach opierają się na praktycznych doświadczeniach we wdrażaniu przepisów, jak wyszczególniono w towarzyszącym dokumencie roboczym służb Komisji. Opierają się one na szeroko zakrojonych konsultacjach z zainteresowanymi stronami, koncentrujących się przede wszystkim na codziennym stosowaniu przepisów.

[39] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Zmiany te są spójne z wieloletnimi ramami finansowymi, ponieważ nie przewiduje się dodatkowych wydatków.

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym możliwości przegrupowania środków

Nie dotyczy.

1.6. Czas trwania wniosku/inicjatywy i jego/jej wpływu finansowego

5. ☐ Ograniczony czas trwania

☐ Czas trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

☐ Czas trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

6. ☒ Nieograniczony czas trwania

Wprowadzenie w życie z okresem rozruchu od RRRR r. do RRRR r.,

po którym następuje faza operacyjna.

1.7. Planowane metody wykonania budżetu[40]

7. ☒ **Bezpośrednie zarządzanie** przez Komisję

☒ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii

☐ przez agencje wykonawcze

8. ☐ **Zarządzanie dzielone** z państwami członkowskimi

9. ☐ **Zarządzanie pośrednie** przez przekazanie zadań związanych z wykonaniem budżetu:

☐ państwom trzecim lub organom przez nie wyznaczonym

☐ organizacjom międzynarodowym i ich agencjom (wyszczególnić)

☐ Europejskiemu Bankowi Inwestycyjnemu i Europejskiemu Funduszowi Inwestycyjnemu

☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego

☐ organom prawa publicznego

☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, w zakresie, w jakim są im zapewnione odpowiednie gwarancje finansowe

☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego i zapewniono odpowiednie gwarancje finansowe

☐ podmiotom lub osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym

---

[40] Szczegóły dotyczące metod wykonania budżetu oraz odniesienia do rozporządzenia finansowego znajdują się na stronie BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

☐· podmiotom mającym siedzibę w państwie członkowskim, podlegającym prawu prywatnemu państwa członkowskiego lub prawu Unii i kwalifikującym się, zgodnie z przepisami sektorowymi, do powierzenia im wykonywania środków finansowych Unii lub gwarancji budżetowych, w zakresie, w jakim podmioty te są kontrolowane przez podmioty prawa publicznego lub podmioty podlegające prawu prywatnemu świadczące usługi użyteczności publicznej, a także posiadają odpowiednie gwarancje finansowe w formie odpowiedzialności solidarnej organów kontrolnych lub równoważne gwarancje finansowe, które mogą być ograniczone, w odniesieniu do każdego działania, do maksymalnej kwoty wsparcia Unii.

I

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

10. Zmiany będą monitorowane w ramach zmienionego prawodawstwa.

2.2. System(y) zarządzania i kontroli

2.2.1. Uzasadnienie dla proponowanych metod wykonania budżetu, mechanizmów finansowania wykonania, sposobów dokonywania płatności i strategii kontroli

11. Systemy zarządzania i kontroli, które mają zastosowanie do obowiązującego prawodawstwa, zapewniają skuteczną kontrolę również w odniesieniu do zmian

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

12. Nie zidentyfikowano żadnego dodatkowego ryzyka

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

13. Koszt kontroli nie będzie się różnił od poprzedniego kosztu

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

14. Te same środki zapobiegania nadal mają zastosowanie do zmian

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

Istniejące linie budżetowe

15. Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn.[41]	państw EFTA[42]	krajów kandydujących i potencjalnych kandydatów[43]	innych państw trzecich	pochodzący z pozostałych dochodów przeznaczonych na określony cel
	20 02 06 Wydatki administracyjne	Środki niezróżnicowane	NIE	NIE	NIE	NIE

Proponowane nowe linie budżetowe

16. Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn.	państw EFTA	krajów kandydujących i potencjalnych kandydatów	innych państw trzecich	pochodzący z pozostałych dochodów przeznaczonych na określony cel

[41] Środki zróżnicowane/środki niezróżnicowane.
[42] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.
[43] Kraje kandydujące oraz, w stosownych przypadkach, potencjalni kandydaci z Bałkanów Zachodnich.

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

☒Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej

3.2.1.1. Środki z uchwalonego budżetu

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	

Dyrekcja Generalna: <…….>			Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
Środki operacyjne							
Linia budżetowa	Środki na zobowiązania	(1a)					**0,000**
	Środki na płatności	(2a)					**0,000**
Linia budżetowa	Środki na zobowiązania	(1b)					**0,000**
	Środki na płatności	(2b)					**0,000**
Środki administracyjne finansowane ze środków przydzielonych na określone programy[44]							
Linia budżetowa		3)					**0,000**
OGÓŁEM środki	Środki na zobowiązania	=1 a+1b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[44] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

dla Dyrekcji Generalnej <…….>	Środki na płatności	=2a+2b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

==========

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznika 5[45] do decyzji Komisji w sprawie przepisów wewnętrznych dotyczących wykonania budżetu ogólnego Unii Europejskiej), przesyłanego do DECIDE w celu konsultacji między służbami.

Dyrekcja Generalna: <…….>		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
• Zasoby ludzkie		0,000	0,000	0,000	0,000	**0,000**
• Pozostałe wydatki administracyjne		0,000	0,000	0,000	0,000	**0,000**
OGÓŁEM Dyrekcja Generalna <….>	Środki	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Dyrekcja Generalna: <…….>		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
• Zasoby ludzkie		0,000	0,000	0,000	0,000	**0,000**
• Pozostałe wydatki administracyjne		0,000	0,000	0,000	0,000	**0,000**
OGÓŁEM Dyrekcja Generalna <….>	Środki	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[45] Jeżeli zgłaszane jest wykorzystanie środków na dział 7, wypełnienie załącznika 5 jest obowiązkowe.

w mln EUR (do trzech miejsc po przecinku)

		Rok 2024	Rok 2025	Rok 2026	Rok 2027	OGÓŁEM WRF 2021–2027
OGÓŁEM środki na DZIAŁY od 1 do 7	Środki na zobowiązania	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
wieloletnich ram finansowych	Środki na płatności	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.1.2. Środki z zewnętrznych dochodów przeznaczonych na określony cel

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	

Dyrekcja Generalna: <…….>			Rok 2024	Rok 2025	Rok 2026	Rok 2027	OGÓŁEM WRF 2021–2027
Środki operacyjne							
Linia budżetowa	Środki na zobowiązania	(1a)					**0,000**
	Środki na płatności	(2a)					**0,000**
Linia budżetowa	Środki na zobowiązania	(1b)					**0,000**
	Środki na płatności	(2b)					**0,000**
Środki administracyjne finansowane ze środków przydzielonych na określone programy[46]							

[46] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

Linia budżetowa		3)					**0,000**
OGÓŁEM środki dla Dyrekcji Generalnej <…….>	Środki na zobowiązania	=1a+1b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
	Środki na płatności	=2a+2b+3	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Dział wieloletnich ram finansowych	**7**	„Wydatki administracyjne”[47]

w mln EUR (do trzech miejsc po przecinku)

Dyrekcja Generalna: <…….>		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
• Zasoby ludzkie		0,000	0,000	0,000	0,000	**0,000**
• Pozostałe wydatki administracyjne		0,000	0,000	0,000	0,000	**0,000**
OGÓŁEM Dyrekcja Generalna <….>	Środki	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Dyrekcja Generalna: <…….>		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
• Zasoby ludzkie		0,000	0,000	0,000	0,000	**0,000**
• Pozostałe wydatki administracyjne		0,000	0,000	0,000	0,000	**0,000**
OGÓŁEM Dyrekcja Generalna <….>	Środki	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

[47] Niezbędne środki należy określić na podstawie danych dotyczących średnich rocznych kosztów, dostępnych na odpowiedniej stronie internetowej BUDGpedia.

w mln EUR (do trzech miejsc po przecinku)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
OGÓŁEM środki na DZIAŁY od 1 do 7	Środki na zobowiązania	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
wieloletnich ram finansowych	Środki na płatności	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.2. Szacowany produkt finansowany ze środków operacyjnych (nie wypełniać w przypadku agencji zdecentralizowanych)

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty ⇩			Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. sekcja 1.6)						**OGÓŁEM**	
	PRODUKT																	
	Rodzaj[48]	Średni koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[49]																		
- Produkt																		
- Produkt																		

[48] Produkty odnoszą się do produktów i usług, które mają zostać zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[49] Zgodnie z opisem w sekcji 1.3.2. „Cel(e) szczegółowy(-e)”.

- Produkt																		
Cel szczegółowy nr 1 – suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2																		
- Produkt																		
Cel szczegółowy nr 2 – suma cząstkowa																		
OGÓŁEM																		

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

☒Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej

3.2.3.1. Środki z uchwalonego budżetu

ZATWIERDZONE ŚRODKI	Rok 2024	Rok 2025	Rok 2026	Rok 2027	OGÓŁEM 2021–2027
DZIAŁ 7					
Zasoby ludzkie	0,000	0,000	0,000	0,000	**0,000**
Pozostałe wydatki administracyjne	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa DZIAŁ 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Poza DZIAŁEM 7					
Zasoby ludzkie	0,000	0,000	0,000	0,000	**0,000**
Pozostałe wydatki o charakterze administracyjnym	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa poza DZIAŁEM 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
OGÓŁEM	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte ze środków dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

3.2.4. Szacowane zapotrzebowanie na zasoby ludzkie

☒Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej

3.2.4.1. Finansowane z uchwalonego budżetu

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy (EPC)[50]

17.

ZATWIERDZONE ŚRODKI	Rok 2024	Rok 2025	Rok 2026	Rok 2027
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)				
20 01 02 01 (w centrali i w biurach	0	0	0	0

[50] Proszę określić w tabeli poniżej, ile EPC w ramach wskazanej liczby jest już przydzielonych na zarządzanie tym działaniem lub może zostać przesuniętych w ramach Państwa dyrekcji generalnej oraz jakie są Państwa potrzeby netto.

przedstawicielstw Komisji)					
20 01 02 03 (w delegaturach UE)		0	0	0	0
01 01 01 01 (pośrednie badania naukowe)		0	0	0	0
01 01 01 11 (bezpośrednie badania naukowe)		0	0	0	0
Inna linia budżetowa (określić)		0	0	0	0
• Personel zewnętrzny (w EPC)					
20 02 01 (CA, SNE z globalnej koperty finansowej)		0	0	0	0
20 02 03 (CA, LA, SNE i JPD w delegaturach UE)		0	0	0	0
Linia budżetowa na wsparcie adm. [XX.01.YY.YY]	- w centrali	0	0	0	0
	- w delegaturach UE	0	0	0	0
01 01 01 02 (CA, SNE – pośrednie badania naukowe)		0	0	0	0
01 01 01 12 (CA, SNE – bezpośrednie badania naukowe)		0	0	0	0
Inna linia budżetowa (określić) – dział 7		0	0	0	0
Inna linia budżetowa (określić) – poza działem 7		0	0	0	0
OGÓŁEM		**0**	**0**	**0**	**0**

3.2.5. Przegląd szacowanego wpływu na inwestycje związane z technologiami cyfrowymi

18. Obowiązkowo w tabeli poniżej: szacowany wpływ wniosku/inicjatywy na inwestycje związane z technologiami cyfrowymi.

19. W wyjątkowych przypadkach, jeżeli wymaga tego realizacja wniosku/inicjatywy, we wskazanym wierszu należy podać środki z działu 7.

20. Środki z działów 1–6 należy podać w wierszu „Wydatki na IT wynikające z realizacji polityki tytułem programów operacyjnych”. Wydatki te odnoszą się do budżetu operacyjnego na ponowne wykorzystanie / zakup / rozwój platform / narzędzi informatycznych bezpośrednio związanych z realizacją inicjatywy oraz powiązanych z nimi inwestycji (np. licencje, badania, przechowywanie danych). Informacje podane w tej tabeli powinny zgadzać się z informacjami przedstawionymi w sekcji 4 „Wymiar cyfrowy”.

OGÓŁEM środki na IT i technologie cyfrowe	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM WRF 2021–2027**
DZIAŁ 7					
Wydatki na IT (ponoszone przez organizację)	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa DZIAŁ 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Poza DZIAŁEM 7					
Wydatki na IT wynikające z realizacji polityki tytułem programów operacyjnych	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa poza DZIAŁEM 7	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
OGÓŁEM	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**

3.2.6. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

21. Wniosek/inicjatywa:

☒może zostać w pełni sfinansowany(-a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF)

☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF

☐ wymaga rewizji WRF

3.2.7. Udział osób trzecich w finansowaniu

22. Wniosek/inicjatywa:

☒nie przewiduje współfinansowania ze strony osób trzecich

☐ przewiduje współfinansowanie ze strony osób trzecich zgodnie z poniższymi szacunkami:

środki w mln EUR (do trzech miejsc po przecinku)

	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	Ogółem
Określić organ współfinansujący					
OGÓŁEM środki objęte współfinansowaniem					

3.3. Szacunkowy wpływ na dochody

☒Wniosek/inicjatywa nie ma wpływu finansowego na dochody

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

– ☐ wpływ na zasoby własne

– ☐ wpływ na dochody inne

– ☐ Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[51]			
		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
Artykuł …….					

23. W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

24. […]

[51] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.

25. Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

26. […]

27. 4. WYMIAR CYFROWY

4.1. Wymogi cyfrowe

Ogólny opis wymogów cyfrowych i powiązanych kategorii (dane, cyfryzacja i automatyzacja procesu, rozwiązania cyfrowe lub cyfrowe usługi publiczne)

Odniesienie do wymogu	**Opis wymogu**	**Podmioty, których dotyczy wymóg lub na które wymóg ten ma wpływ**	**Procesy ogólne**	**Kategorie**
Artykuł 1	Zmiana art. 1 ust. 1 aktu w sprawie danych, rozszerzająca jego zakres stosowania, ustanawiając: • ramy rejestracji usług pośrednictwa danych; • ramy dotyczące dobrowolnej rejestracji podmiotów, które gromadzą i przetwarzają dane udostępniane z pobudek altruistycznych. • ramy dotyczące ustanowienia Europejskiej Rady ds. Innowacji w zakresie Danych.	Komisja Europejska Usługi pośrednictwa danych Podmioty zajmujące się gromadzeniem i przetwarzaniem danych	Rozszerzenie zakresu stosowania aktu w sprawie danych	Cyfrowe usługi publiczne
Artykuł 1	Zmiana art. 4 ust. 8 i art. 5 ust. 11 aktu w sprawie danych. Posiadacze danych odmawiający dzielenia się danymi na podstawie wyjątku dotyczącego tajemnic przedsiębiorstwa odpowiednio	Posiadacze danych (posiadacze tajemnicy przedsiębiorstwa) Inicjatorzy wniosków o	Powiadomienie	Dane

	powiadamiają o takiej decyzji.	dostęp		
Artykuł 1	Dodanie art. 15a do aktu w sprawie danych. Obowiązek udostępnienia danych na podstawie niebezpieczeństwa publicznego.	Organ sektora publicznego Komisja Europejska Europejski Bank Centralny Organ Unii Posiadacze danych	Udostępnianie danych	Dane
Artykuł 1	Zmiana art. 21 ust. 5 aktu w sprawie danych. Wymogi dotyczące dzielenia się danymi pozyskanymi w kontekście niebezpieczeństwa publicznego z organizacjami badawczymi lub urzędami statystycznymi. Dodanie art. 22a do aktu w sprawie danych, umożliwiającego składanie skarg w odniesieniu do rozdziału V („*Udostępnianie danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom Unii na podstawie wyjątkowej potrzeby*").	Organ sektora publicznego Komisja Europejska Europejski Bank Centralny Organ Unii Posiadacz danych Właściwy organ krajowy	Udostępnianie danych Skargi	Dane

Artykuł 1	Zmiany w art. 32 ust. 1–5 aktu w sprawie danych dotyczące dostępu państw trzecich do danych nieosobowych.	Dostawcy usług przetwarzania danych Dostawcy usług pośrednictwa danych Organizacje altruizmu danych Organy lub instytucje krajowe	Międzynarodowy dostęp administracji rządowej do danych i przekazywanie danych	Dane Cyfrowe usługi publiczne
Artykuł 1	Zmiana art. 35 ust. 5 aktu w sprawie danych, umożliwiająca Komisji przyjęcie wspólnych specyfikacji w odniesieniu do interoperacyjności usług przetwarzania danych.	Dostawcy usług przetwarzania danych Komisja Europejska	Przyjęcie wspólnych specyfikacji	Cyfrowe usługi publiczne
Artykuł 1	Zmiany w art. 32a–32e aktu w sprawie danych w celu wprowadzenia rozdziału VIIa dotyczącego ram regulacyjnych dla europejskiego znaku jakości w odniesieniu do usług pośrednictwa danych, w tym zgłaszania, utworzenia rejestru publicznego, warunków świadczenia usług, wyznaczenia właściwych organów i monitorowania zgodności Zmiany w art. 32h aktu w sprawie danych w celu wprowadzenia rozdziału VIIb dotyczącego swobodnego przepływu danych w Unii, w tym zakazu stosowania	Dostawcy usług pośrednictwa danych Osoby, których dane dotyczą, posiadacze danych, użytkownicy danych Państwa członkowskie Właściwe organy Komisja Europejska	Ustanowienie europejskiego znaku jakości dla usług pośrednictwa danych Ustanowienie swobodnego przepływu danych w Unii Europejskiej	Dane Rozwiązanie cyfrowe Cyfryzacja procesu Cyfrowe usługi publiczne

	wymogów dotyczących lokalizacji danych, obowiązków zgłaszania Komisji oraz publikacji skonsolidowanego wykazu.			
Artykuł 1	Zmiany w art. 32h aktu w sprawie danych w celu wprowadzenia rozdziału VIIb dotyczącego swobodnego przepływu danych w Unii, w tym zakazu stosowania wymogów dotyczących lokalizacji danych, obowiązków zgłaszania Komisji oraz publikacji skonsolidowanego wykazu.	Państwa członkowskie Komisja Europejska	Ustanowienie swobodnego przepływu danych w Unii Europejskiej	Dane Cyfryzacja procesu Cyfrowe usługi publiczne
Artykuł 1	Dodanie art. 32i do aktu w sprawie danych, określającego zakres rozdziału VIIc. Ustanawia on zbiór minimalnych przepisów regulujących ponowne wykorzystywanie danych oraz praktyczne ustalenia ułatwiające ponowne wykorzystywanie danych. Dodanie art. 32j do aktu w sprawie danych; przepis dotyczący	Państwa członkowskie Posiadacze danych Użytkownicy danych	Określenie przedmiotu i zakresu stosowania Niedyskryminacja	Cyfrowe usługi publiczne

	niedyskryminacji w odniesieniu do ponownego wykorzystywania danych i dokumentów.			
Artykuł 1	Dodanie art. 32k do aktu w sprawie danych. Przepisy w sprawie uzgodnień dotyczących wyłączności w zakresie ponownego wykorzystywania danych. Obejmuje to obowiązek podawania ostatecznych warunków uzgodnień do wiadomości publicznej.	Potencjalni uczestnicy rynku Organy sektora publicznego Strony takich umów		Cyfrowe usługi publiczne Dane
Artykuł 1	Zmiany w akcie w sprawie danych: • 41): dodanie art. 32n dotyczącego ogólnej zasady ponownego wykorzystywania otwartych danych publicznych; • 42): dodanie art. 32o dotyczącego rozpatrywania wniosków o ponowne wykorzystywanie danych; • 43): dodanie art. 32p dotyczącego formatów ponownego wykorzystywania danych; • 46): dodanie art. 32s dotyczącego praktycznych ustaleń ułatwiających wyszukiwanie danych lub dokumentów dostępnych do ponownego wykorzystywania.	Posiadacze danych Użytkownicy danych Państwa członkowskie (organy sektora publicznego) Komisja Europejska	Zasady ponownego wykorzystywania danych	Cyfrowe usługi publiczne Dane Cyfryzacja procesu

Artykuł 1	Dodanie art. 32t do aktu w sprawie danych; wymóg wspierania dostępności danych badawczych.	Państwa członkowskie Organizacje badawcze Użytkownicy danych	Zasady ponownego wykorzystywania danych	Cyfrowe usługi publiczne Dane
Artykuł 1	Dodanie art. 32u do aktu w sprawie danych. Ustanowienie zasad publikacji i ponownego wykorzystywania określonych zbiorów danych o wysokiej wartości.	Komisja Europejska Organy sektora publicznego, przedsiębiorstwa publiczne	Zasady ponownego wykorzystywania danych	Cyfrowe usługi publiczne Dane
Artykuł 1	Dodanie art. 32w do aktu w sprawie danych. Określenie warunków ponownego wykorzystywania niektórych kategorii danych. Procedury wnioskowania o takie ponowne wykorzystywanie i warunki zezwolenia na takie ponowne wykorzystywanie podaje się do wiadomości publicznej za pośrednictwem pojedynczego punktu informacyjnego.	Organy sektora publicznego Użytkownicy danych	Zasady ponownego wykorzystywania danych	Cyfrowe usługi publiczne Dane
Artykuł 1	Dodanie art. 32x do aktu w sprawie danych; wymogi dotyczące przekazywania danych nieosobowych do państw trzecich przez ponownych użytkowników.	Ponowni użytkownicy danych Organy sektora publicznego Osoby fizyczne/prawne, na których prawa może mieć to wpływ	Przekazywanie danych do państw trzecich	Cyfrowe usługi publiczne Dane

Artykuł 1	Zmiany w akcie w sprawie danych: • 55): dodanie art. 32z; środki organizacyjne dotyczące właściwych organów. • 57): dodanie art. 32ab dotyczącego procedur składania wniosków o ponowne wykorzystywanie danych. • 58): zastąpienie art. 38 ust. 1–2 dotyczącego prawa do wniesienia skargi.	Właściwe organy Państwa członkowskie Organy sektora publicznego	Ustanowienie właściwych organów Procedury składania wniosków Skargi	Cyfrowe usługi publiczne Dane
Artykuł 1	Dodanie art. 32aa do aktu w sprawie danych. Wprowadzenie obowiązku korzystania z pojedynczego punktu informacyjnego w celu ułatwienia ponownego wykorzystywania danych.	Państwa członkowskie Posiadacze danych Użytkownicy danych Komisja Europejska	Ustanowienie pojedynczego punktu dostępu	Rozwiązania cyfrowe Cyfrowe usługi publiczne Cyfryzacja procesu Dane

Artykuł 1	Zmiany w art. 41a, 42, 45, 46, 48a, 49 i 49a aktu w sprawie danych w celu wprowadzenia rozdziału IXa ustanawiającego Europejską Radę ds. Innowacji w zakresie Danych (EDIB) jako grupę ekspertów koordynującą egzekwowanie przepisów i ułatwiającą rozwój europejskiej gospodarki opartej na danych, w tym wymogi dotyczące składu, roli, ułatwiania współpracy między właściwymi organami oraz wspierania spójnego stosowania wymogów prawnych.	Komisja Europejska, Europejska Rada ds. Innowacji w zakresie Danych (EDIB) Przedstawiciele państw członkowskich odpowiedzialni za politykę w zakresie gospodarki opartej na danych Właściwe organy odpowiedzialne za egzekwowanie przepisów rozdziałów II, III i V Właściwe organy ds. ponownego wykorzystywania informacji sektora publicznego (dyrektywa w sprawie otwartych danych) Organy właściwe do spraw usług pośrednictwa danych Organy właściwe do spraw rejestracji organizacji altruizmu danych	Ustanowienie Europejskiej Rady ds. Innowacji w zakresie Danych (EDIB)	Cyfrowe usługi publiczne Dane

		Europejska Rada Ochrony Danych (EROD), Europejski Inspektor Ochrony Danych (EIOD) ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) Pełnomocnik UE ds. MŚP lub przedstawiciel sieci pełnomocników ds. MŚP Inni przedstawiciele właściwych organów w określonych sektorach Organy posiadające szczególną wiedzę fachową Organizacje normalizacyjne Parlament Europejski, Rada Unii Europejskiej, Europejski Komitet Ekonomiczno-Społeczny Dostawcy usług pośrednictwa danych Uznane organizacje altruizmu danych		

Artykuł 3	Zmiana art. 33 rozporządzenia (UE) 2016/679 (RODO) w odniesieniu do zgłaszania naruszeń ochrony danych osobowych. Nakazuje między innymi korzystanie z pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555 i przewiduje stosowanie wzorów zgłoszeń.	Przedmioty danych Administratorzy danych Organy nadzorcze Europejska Rada Ochrony Danych Komisja Europejska	Powiadomienie	Dane
Artykuł 3	Zmiana art. 35 i art. 70 ust. 1 rozporządzenia (UE) 2016/679 (RODO). Wymóg, aby Europejska Rada Ochrony Danych przekazywała Komisji wnioski w celu dalszego wdrażania niektórych aspektów oceny skutków dla ochrony danych. Obejmują one wspólny wzór takich ocen.	Europejska Rada Ochrony Danych Komisja Europejska	Wnioski Rady przekazane Komisji	Dane
Artykuł 3	Dodanie art. 88b do rozporządzenia (UE) 2016/679 (RODO); osoby, których dane dotyczą, muszą mieć możliwość wyrażenia zgody/wykonania prawa sprzeciwu w sposób zautomatyzowany i nadający się do odczytu maszynowego. Przewiduje się, że normy opracuje co najmniej jedna europejska organizacja normalizacyjna.	Przedmioty danych Administratorzy danych Europejskie organizacje normalizacyjne Komisja Europejska	Zautomatyzowane i nadające się do odczytu maszynowego wskazania wyborów dokonanych przez osobę, której dane dotyczą	Rozwiązania cyfrowe Automatyzacja procesów

Artykuł 6	Zmiana dyrektywy (UE) 2022/2555 (NIS 2): • 1): dodanie art. 23a dotyczącego opracowania i utrzymania pojedynczego punktu kontaktowego do zgłaszania incydentów; • 3): zmiany art. 23 ust. 4 w celu wprowadzenia obowiązku korzystania z pojedynczego punktu kontaktowego do celów zgłaszania poważnych incydentów; • 4): dodanie art. 23 ust. 12, który zapewnia, aby poważne incydenty zgłaszano tylko raz (na podstawie dyrektywy NIS 2 albo aktu dotyczącego cyberodporności); • 5): zmiana art. 30 ust. 1 zapewniająca możliwość dobrowolnego korzystania z pojedynczego punktu kontaktowego do celów zgłaszania przez różne podmioty.	Zgłaszający (podmioty kluczowe i ważne) CSIRT/właściwe organy (w stosownych przypadkach) Komisja Europejska ENISA,	Powiadomienie	Dane Rozwiązania cyfrowe Cyfrowe usługi publiczne
Artykuł 7	Zmiana rozporządzenia (UE) nr 910/2014 (europejski portfel tożsamości cyfrowej) wymagająca korzystania z pojedynczego punktu kontaktowego, zgodnie z art. 23a dyrektywy (UE) 2022/2555, w	Zgłaszający (niekwalifikowani dostawcy usług zaufania; kwalifikowani dostawcy usług zaufania; dostawcy przeglądarki	Powiadomienie	Dane

	odniesieniu do: • Art. 19a ust. 1a: zgłoszeń, o których mowa w ust. 1 lit. b). • Art. 24 ust. 2a: zgłoszeń, o których mowa w ust. 2 lit. fb). Art. 45a ust. 3a: zgłoszeń, o których mowa w ust. 3.	internetowej) Organy nadzorcze Inne odpowiednie właściwe organy/instytucje Komisja Europejska		
Artykuł 8	Zmiana rozporządzenia (UE) 2022/2554 (DORA) wymagająca korzystania z pojedynczego punktu kontaktowego, zgodnie z art. 23a dyrektywy (UE) 2022/2555, w odniesieniu do: • Art. 19 ust. 1: poważnych incydentów związanych z ICT. • Art. 19 ust. 2: dobrowolnego zgłaszania poważnych cyberzagrożeń.	Zgłaszający (podmioty finansowe) Organy nadzorcze Inne odpowiednie właściwe organy/instytucje Komisja Europejska ENISA,	Powiadomienie	Dane
Artykuł 9	Zmiana dyrektywy (UE) 2022/2557 (CER) wymagająca korzystania z pojedynczego punktu kontaktowego, zgodnie z art. 23a dyrektywy (UE) 2022/2555, w odniesieniu do: • Art. 15 ust. 1: incydentów, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych.	Zgłaszający (podmioty krytyczne) Organy nadzorcze Inne odpowiednie właściwe organy/instytucje Komisja Europejska ENISA,	Powiadomienie	Dane

4.2. Dane

Ogólny opis danych objętych zakresem inicjatywy

Rodzaj danych	**Odniesienie do wymogu/wymogów**	**Normy lub specyfikacje (stosownie do przypadku)**
Odrzucenie wniosku o dostęp do danych na podstawie wyjątku dotyczącego tajemnicy przedsiębiorstwa (*i powiadomienie o tym właściwego organu*)	Artykuł 1	Należy odpowiednio uzasadnić na podstawie obiektywnych elementów.
Dane, które należy udostępniać w kontekście niebezpieczeństwa publicznego	Artykuł 1	Uwzględnienie metadanych niezbędnych do interpretacji i wykorzystania danych. W przypadku danych osobowych – w miarę możliwości w formie pseudonimizowanej.
Powiadomienie o zamiarze udostępnienia danych w kontekście niebezpieczeństwa publicznego	Artykuł 1	Podanie danych identyfikacyjnych i kontaktowych organizacji lub osoby fizycznej otrzymującej dane, celu przekazania lub udostępnienia danych, okresu, przez który dane będą wykorzystywane, oraz zastosowanych technicznych środków ochrony i środków organizacyjnych.
Skargi na podstawie rozdziału V („*Udostępnianie danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom Unii na podstawie wyjątkowej potrzeby*”)	Artykuł 1	//
Dane nieosobowe przechowywane w Unii Europejskiej	Artykuł 1	//

Dane, które należy dostarczyć w odpowiedzi na wniosek o ponowne wykorzystywanie danych	Artykuł 1	Przekazanie minimalnej dopuszczalnej ilości danych
Powiadomienie o zamiarze udzielenia zgody na ponowne wykorzystywanie danych	Artykuł 1	//
Dane, w odniesieniu do których świadczone są usługi pośrednictwa (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	Format otrzymany od osoby, której dane dotyczą/posiadacza danych, konwersja wyłącznie w celu zwiększenia interoperacyjności lub zapewnienia zgodności z międzynarodowymi/europejskimi normami dotyczącymi danych
Informacje na temat wykorzystania danych i warunków (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	Należy przekazywać w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny
Wnioski o rejestrację w publicznym rejestrze unijnym i zmiany zgłoszonych informacji (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	Właściwe organy ustanawiają niezbędne formularze wniosków.
Przyjęte wnioski o rejestrację, które należy dodać do publicznego rejestru unijnego (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//
Powiadomienie o późniejszych zmianach w informacjach przekazanych w trakcie procesu składania wniosku (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//

Otrzymanie powiadomienia o późniejszych zmianach (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//
Informacje przekazywane osobom, których dane dotyczą/posiadaczom danych przed przetwarzaniem (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//
Zgoda (lub wycofanie zgody) na przetwarzanie danych przez uznaną organizację altruizmu danych (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	Do uzyskania drogą elektroniczną
Informacje na temat jurysdykcji państwa trzeciego, w którym ma mieć miejsce wykorzystanie danych	Artykuł 1	//
Powiadamianie o nieuprawnionym przekazywaniu danych nieosobowych, dostępie do nich lub ich wykorzystywaniu (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//
Informacje na potrzeby monitorowania zgodności (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	Wnioski muszą być proporcjonalne i uzasadnione
Powiadomienie o niezgodności (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//

Decyzja o cofnięciu prawa do korzystania ze znaku (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1	//
Projekty aktów w sprawie wymogów dotyczących lokalizacji danych	Artykuł 1	//
Ostateczne warunki uzgodnień dotyczących wyłączności	Artykuł 1	//
Dane (lub powiadomienia) dotyczące wniosku o ponowne wykorzystywanie	Artykuł 1	W dowolnym istniejącym formacie lub języku oraz, w miarę możliwości i w stosownych przypadkach, drogą elektroniczną, w formatach, które są otwarte, nadają się do odczytu maszynowego, są dostępne, możliwe do znalezienia i możliwe do ponownego wykorzystywania, wraz z ich metadanymi.
Dane badawcze finansowane ze środków publicznych	Artykuł 1	Ogólnie dostępne, zgodnie z zasadą „otwartości domyślnej” i zgodne z zasadami FAIR.
Określone zbiory danych o wysokiej wartości	Artykuł 1	Dostępne bezpłatnie; jest w formacie nadającym się do odczytu maszynowego; dostarczane za pośrednictwem interfejsów API oraz do zbiorczego pobrania (w stosownych przypadkach). Akty wykonawcze, które mają zostać przyjęte; mogą obejmować formaty danych i metadanych.
Warunki zezwolenia na ponowne wykorzystywanie danych lub dokumentów, o których mowa w art. 2 pkt 54	Artykuł 1	Rejestr jest publicznie dostępny.

Powiadomienie o niedozwolonym ponownym wykorzystywaniu danych nieosobowych	Artykuł 1	//
Powiadomienie o zamiarze przekazania danych nieosobowych do państwa trzeciego i cel takiego przekazania (*organowi sektora publicznego*)	Artykuł 1	//
Powiadomienie o zamiarze przekazania danych nieosobowych do państwa trzeciego, cel tego przekazania oraz odpowiednie zabezpieczenia (*na rzecz osoby fizycznej lub prawnej, na której prawa i interesy może to mieć wpływ*)	Artykuł 1	//
Wszystkie istotne informacje dotyczące stosowania art. 32z [warunki ponownego wykorzystywania], 32aa [państwa trzecie] i 32ab [opłaty] aktu w sprawie danych.	Artykuł 1	Łatwo dostępne za pośrednictwem pojedynczego punktu informacyjnego.
Skarga wniesiona przez osoby fizyczne/prawne, jeżeli ich prawa wynikające z aktu w sprawie danych zostały naruszone lub w odniesieniu do innych istotnych kwestii	Artykuł 1	//
Informacje na temat przebiegu postępowania/środków ochrony prawnej przed sądem w związku ze skargą złożoną na podstawie aktu w sprawie danych	Artykuł 1	//
Dane dotyczące doświadczeń i dobrych praktyk (EDIB)	Artykuł 1	//

Ocena rozdziałów II, III, IV, V, VI, VII i VIII aktu w sprawie danych Ocena rozdziałów VIIa, VIIb i VIIc aktu w sprawie danych	Artykuł 1 Artykuł 1	Określono minimalne wymogi dotyczące treści sprawozdań.
Zgłaszanie naruszeń ochrony danych osobowych	Artykuł 3	Za pośrednictwem (a tym samym z poszanowaniem specyfikacji) pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555. Europejska Rada Ochrony Danych przygotowuje wniosek dotyczący wspólnego wzoru (*zob. następny wpis*).
Wniosek EROD dotyczący wspólnego wzoru powiadomienia o naruszeniu ochrony danych	Artykuł 3	//
Wnioski EROD dotyczące oceny skutków dla ochrony danych	Artykuł 3	//
Zgłoszenia poważnych incydentów zgodnie z dyrektywą NIS 2	Artykuł 6	Za pośrednictwem (a tym samym z poszanowaniem specyfikacji) pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555.
Zgłaszanie naruszeń ochrony danych osobowych	Artykuł 3	Za pośrednictwem (a tym samym z poszanowaniem specyfikacji) pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555
Zgłaszanie poważnych incydentów związanych z	Artykuł 8	Za pośrednictwem (a tym samym z poszanowaniem

ICT na podstawie DORA; dobrowolne zgłaszanie poważnych cyberzagrożeń na podstawie DORA		specyfikacji) pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555
Zgłaszanie incydentów, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych, zgodnie z dyrektywą CER	Artykuł 9	Za pośrednictwem (a tym samym z poszanowaniem specyfikacji) pojedynczego punktu kontaktowego ustanowionego na podstawie art. 23a dyrektywy (UE) 2022/2555

Powiązanie z europejską strategią w zakresie danych

Wyjaśnienie, w jaki sposób wymogi te są zgodne z europejską strategią w zakresie danych.

Te zmiany w akcie w sprawie danych wprowadzają Europejską Radę ds. Innowacji w zakresie Danych (rozdział IXa), która koordynuje stosowanie przepisów i opracowuje wytyczne dotyczące sektorowych wspólnych europejskich przestrzeni danych; europejskie znaki jakości usług pośrednictwa danych i organizacji altruizmu danych (rozdział VIIa), które tworzą godny zaufania ekosystem dzielenia się danymi i ochrony praw; w rozdziale VIIb wdrożono swobodny przepływ danych nieosobowych przez zakazanie nieuzasadnionych wymogów dotyczących lokalizacji danych; w rozdziale VIIc usprawniono przepisy dotyczące ponownego wykorzystywania danych sektora publicznego, łącząc przepisy dyrektywy w sprawie otwartych danych i aktu w sprawie zarządzania danymi; przepisy dotyczące międzynarodowego przekazywania danych wzmacniają europejską suwerenność cyfrową dzięki ochronie danych przed nieuprawnionym dostępem ze strony państw trzecich; wreszcie zwolnienia dla MŚP i obecność pełnomocnika UE ds. MŚP w Europejskiej Radzie ds. Innowacji w zakresie Danych zapewniają również małym przedsiębiorstwom lepszy dostęp do gospodarki opartej na danych.

Powiązanie z zasadą jednorazowości

Wyjaśnienie, w jaki sposób uwzględniono zasadę jednorazowości i w jaki sposób zbadano możliwość ponownego wykorzystania istniejących danych.

Zmiany te wspierają zasadę jednorazowości przez stworzenie infrastruktury skutecznego ponownego wykorzystywania danych: Europejska Rada ds. Innowacji w zakresie Danych opracowuje normy interoperacyjności we wspólnych europejskich przestrzeniach danych, aby ograniczyć powielanie dostarczania danych; usługi pośrednictwa danych działają jako zaufani pośrednicy umożliwiający bezpieczną wymianę istniejących danych, eliminując zbędne gromadzenie; organizacje altruizmu danych ułatwiają dobrowolne dzielenie się danymi w interesie publicznym, udostępniając dane nadające się do ponownego wykorzystania na potrzeby badań naukowych i usług publicznych; przepisy dotyczące swobodnego przepływu zapobiegają powstawaniu barier wymagających powielonego przechowywania w różnych lokalizacjach;

oraz zabezpieczenia dotyczące międzynarodowego przekazywania danych zapewniają transgraniczną dostępność danych z jednoczesnym utrzymaniem ochrony, umożliwiając osobom fizycznym i przedsiębiorstwom zbiorowe jednokrotne dostarczanie ich danych, przy zaspokojeniu dalszych potrzeb za pomocą bezpiecznych mechanizmów wymiany z poszanowaniem praw. Tymczasem przepisy w ramach pojedynczego punktu kontaktowego dodatkowo umożliwiają stosowanie zasady jednorazowości w odniesieniu do zgłaszania incydentów.

Wyjaśnienie, w jaki sposób nowo utworzone dane są możliwe do znalezienia, dostępne, interoperacyjne i nadające się do ponownego wykorzystania oraz spełniają normy wysokiej jakości.

Zmiany te zapewniają zgodność nowo utworzonych danych z zasadami FAIR i normami jakości dzięki skoordynowanym mechanizmom: Europejska Rada ds. Innowacji w zakresie Danych opracowuje wspólną specyfikację techniczną i dostępne protokoły interoperacyjności we wszystkich sektorowych przestrzeniach danych; przepisy dotyczące swobodnego przepływu zapobiegają fragmentacji, która obniża jakość danych; rola koordynacyjna Europejskiej Rady ds. Innowacji w zakresie Danych może umożliwić zharmonizowane wdrażanie standardów metadanych, wymogów technicznych i wskaźników jakości we wszystkich państwach członkowskich.

Przepływ danych

Ogólny opis przepływu danych

Uwaga: większość przepływów danych opisanych poniżej to istniejące wcześniej przepływy, które przenosi się z jednego rozporządzenia do drugiego. W szczególności przepisy aktu w sprawie zarządzania danymi przeniesiono do aktu w sprawie danych.

Rodzaj danych	**Odniesienia do wymogów**	**Podmioty dostarczające dane**	**Podmioty otrzymujące dane**	**Czynnik uruchamiający wymianę danych**	**Częstotliwość (jeżeli dotyczy)**
Odrzucenie wniosku o dostęp do danych na podstawie wyjątku dotyczącego tajemnicy przedsiębiorstwa (*i powiadomienie o tym właściwego organu*)	Artykuł 1 *Zmiana art. 4 ust. 8 i art. 5 ust. 11 aktu w sprawie danych*	Posiadacz danych	Użytkownik danych (występujący z wnioskiem); właściwy organ wskazany na	Odrzucenie wniosku o dostęp do danych na podstawie wyjątku dotyczącego tajemnicy przedsiębiorstwa	Pomoc ad hoc

			podstawie art. 37		
Dane, które należy udostępniać w kontekście niebezpieczeństwa publicznego	Artykuł 1 *Dodanie art. 15a do aktu w sprawie danych*	Posiadacz danych	Organ sektora publicznego; Komisja Europejska; Europejski Bank Centralny Organ Unii	Niebezpieczeństwo publiczne + wniosek o dostęp do danych spełniający niezbędne warunki	Pomoc ad hoc
Powiadomienie o zamiarze udostępnienia danych w kontekście niebezpieczeństwa publicznego	Artykuł 1 *Zmiana art. 21 ust. 5 aktu w sprawie danych*	Organ sektora publicznego; Komisja Europejska; Europejski Bank Centralny Organ Unii	Posiadacz danych, od którego otrzymano dane	Niebezpieczeństwo publiczne + zamiar przekazania lub udostępnienia danych	Pomoc ad hoc
Skargi na podstawie rozdziału V („Udostępnianie danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom Unii na podstawie wyjątkowej potrzeby”)	Artykuł 1 *Dodanie art. 22a do aktu w sprawie danych*	Posiadacz danych; organ sektora publicznego; Komisja Europejska; Europejski Bank Centralny Organ Unii	Właściwy organ państwa członkowskiego, w którym posiadacz danych ma siedzibę	W przypadku powstania sporu dotyczącego wniosku o dane na podstawie art. 15a aktu w sprawie danych	Pomoc ad hoc
Dane nieosobowe przechowywane w Unii Europejskiej	Artykuł 1 *Zmiana następujących*	Dostawcy usług przetwarzania danych, dostawcy usług	Sądy/trybunały państw trzecich Organy	Wniosek państwa trzeciego na podstawie umowy międzynarodowej,	Pomoc ad hoc

	artykułów aktu w sprawie danych: *art. 32 ust. 1, art. 32 ust. 3, art. 32 ust. 4*	pośrednictwa danych, organizacje altruizmu danych	administracyjne państw trzecich, klienci (posiadacze danych/osoby, których dane dotyczą)	wniosek państwa trzeciego spełniający warunki określone w art. 32 ust. 3, wniosek klienta o dostęp do jego własnych danych	
Dane, które należy dostarczyć w odpowiedzi na wniosek o ponowne wykorzystywanie danych	Artykuł 1 *Zmiana art. 32 ust. 4–5 aktu w sprawie danych*	Dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych	Inicjator wniosku o ponowne wykorzystywanie danych (organ państwa trzeciego)	Data udzielenia zgody na ponowne wykorzystywanie	Pomoc ad hoc
Powiadomienie o zamiarze udzielenia zgody na ponowne wykorzystywanie danych	Artykuł 1 *Zmiana art. 32 ust. 4–5 aktu w sprawie danych*	Dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych	Klient	Data udzielenia zgody na ponowne wykorzystywanie przez organ państwa trzeciego (*z wyjątkiem przypadków, gdy wniosek służy celom egzekwowania prawa*)	Pomoc ad hoc
Informacje, które należy publikować w rejestrach publicznych (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32a do aktu w sprawie danych*	Komisja Europejska	Publikacja danych	Informacje na temat uznanych usług pośrednictwa danych lub organizacji altruizmu danych stają	Na bieżąco (rejestr regularnie aktualizowany)

				się dostępne lub wymagają zmiany	
Dane, w odniesieniu do których świadczone są usługi pośrednictwa (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32c do aktu w sprawie danych*	Osoby, których dane dotyczą Posiadacze danych	Użytkownicy danych (za pośrednictwem dostawcy usług pośrednictwa danych)	Zgoda osoby, której dane dotyczą Pozwolenie posiadacza danych Wniosek użytkownika danych	Zgodnie z porozumieniem/umową między stronami
Informacje na temat wykorzystania danych i warunków (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32c do aktu w sprawie danych*	Dostawca usług pośrednictwa danych	Przedmioty danych	Zanim osoba, której dane dotyczą, wyrazi zgodę na wykorzystanie danych	Za każdym razem przed żądaniem o zgody
Wnioski o rejestrację w publicznym rejestrze unijnym i zmiany zgłoszonych informacji (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32e do aktu w sprawie danych*	Dostawcy usług pośrednictwa danych Organizacje altruizmu danych	Właściwy organ w państwie członkowskim, w którym znajduje się główna jednostka organizacyjna	Składanie zgłoszeń	Pomoc ad hoc
Przyjęte wnioski o rejestrację, które należy dodać do	Artykuł 1 *Dodanie art. 32e do*	Właściwy organ	Komisja	Zatwierdzony wniosek	Doraźnie (w ciągu 12 tygodni od otrzymania

publicznego rejestru unijnego (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	*aktu w sprawie danych*		Europejska		wniosku, pod warunkiem że decyzja jest pozytywna)
Powiadomienie o późniejszych zmianach w informacjach przekazanych w trakcie procesu składania wniosku (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32e do aktu w sprawie danych*	Zarejestrowane podmioty	Właściwy organ	Zmiany w przekazanych informacjach lub gdy podmioty zaprzestają działalności w Unii	Pomoc ad hoc
Otrzymanie powiadomienia o późniejszych zmianach (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32e do aktu w sprawie danych*	Właściwy organ	Komisja Europejska	Zarejestrowane podmioty powiadamiają o zmianie (zob. pozycja powyżej)	Doraźnie, niezwłocznie
Informacje przekazywane osobom, których dane dotyczą/posiadaczom danych przed przetwarzaniem (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32f do aktu w sprawie danych*	Uznana organizacja altruizmu danych	Osoby, których dane dotyczą Posiadacze danych	Przed jakimkolwiek przetwarzaniem ich danych	Przed każdą czynnością przetwarzania (należy zapewnić jasność i zrozumiałość)
Zgoda (lub wycofanie zgody) na przetwarzanie danych przez uznaną organizację altruizmu danych (europejski znak	Artykuł 1 *Dodanie art. 32f do aktu w sprawie*	Osoby, których dane dotyczą Posiadacze danych (w	Organizacja altruizmu danych	Zgoda osoby, której dane dotyczą/pozwolenie posiadacza danych	Zgodnie z udzieloną zgodą/pozwoleniem, z możliwością wycofania w dowolnym

jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	*danych*	przypadku danych nieosobowych)		niezbędne do czynności przetwarzania	momencie
Informacje na temat jurysdykcji państwa trzeciego, w którym ma mieć miejsce wykorzystanie danych	Artykuł 1 *Dodanie art. 32f do aktu w sprawie danych*	Organizacja altruizmu danych	Posiadacze danych	W przypadku gdy organizacja altruizmu danych ułatwia przetwarzanie danych przez osoby trzecie	Pomoc ad hoc
Powiadamianie o nieuprawnionym przekazywaniu danych nieosobowych, dostępie do nich lub ich wykorzystywaniu (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32f do aktu w sprawie danych*	Organizacja altruizmu danych	Posiadacze danych	Nieupoważnione działanie	Doraźnie, niezwłocznie
Informacje na potrzeby monitorowania zgodności (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32g do aktu w sprawie danych*	Dostawcy usług pośrednictwa danych Organizacje altruizmu danych	Właściwe organy	Wniosek właściwego organu Wniosek osoby fizycznej lub prawnej	Doraźnie (na wniosek, który musi być proporcjonalny i uzasadniony)
Powiadomienie o niezgodności (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32g do aktu w sprawie danych*	Właściwy organ	Podmiot uznany za niespełniający wymogów	Właściwy organ stwierdza, że uznany dostawca usług pośrednictwa danych lub uznana	Doraźnie (z możliwością przedstawienia następnie swojego stanowiska przez podmiot w terminie 30

				organizacja altruizmu danych nie spełniają wymogów	dni)
Decyzja o cofnięciu prawa do korzystania ze znaku (europejski znak jakości dla usług pośrednictwa danych i organizacji altruizmu danych)	Artykuł 1 *Dodanie art. 32g do aktu w sprawie danych*	Właściwy organ	Publikacja danych	W następstwie decyzji o uchyleniu znaku	Pomoc ad hoc
Projekty aktów w sprawie wymogów dotyczących lokalizacji danych	Artykuł 1	Państwa członkowskie	Komisja Europejska	Opracowanie projektu aktu wprowadzającego nowy wymóg dotyczący lokalizacji danych lub zmieniającego istniejący wymóg dotyczący lokalizacji danych	Doraźnie, niezwłocznie
Ostateczne warunki uzgodnień dotyczących wyłączności	Artykuł 1	Strony uzgodnień	Publikacja danych	Uzgodnienia dotyczące wyłączności zawarte w dniu 16 lipca 2019 r. lub po tej dacie	Doraźnie, co najmniej dwa miesiące przed wejściem w życie uzgodnienia
Dane (lub powiadomienia) dotyczące wniosku o ponowne wykorzystywanie	Artykuł 1 *Dodanie art. 32p do aktu w sprawie*	Organy sektora publicznego	Inicjatorzy wniosków o ponowne	W przypadku dokumentów należy dostarczyć	Pomoc ad hoc

	danych		wykorzystywanie danych	którekolwiek z poniższych: wymagane dane/dokumenty; oferta licencji; powiadomienia o opóźnieniach; powiadomienie o decyzji odmownej.	
Ostateczne warunki uzgodnień dotyczących wyłączności	Artykuł 1 *Dodanie art. 32k do aktu w sprawie danych*	Strony uzgodnień dotyczących wyłączności	Ogół społeczeństwa	Ostateczne warunki wypracowanego uzgodnienia dotyczącego wyłączności	Pomoc ad hoc
Warunki zezwolenia na ponowne wykorzystywanie danych lub dokumentów, o których mowa w art. 2 pkt 54	Artykuł 1 *Dodanie art. 32z do aktu w sprawie danych*	Organy sektora publicznego (właściwe do udzielania lub odrzucania wniosków o dostęp)	Ogół społeczeństwa	Gdy udzielają zgody na ponowne wykorzystywanie danych lub dokumentów	Pomoc ad hoc
Powiadomienie o niedozwolonym ponownym wykorzystywaniu danych nieosobowych	Artykuł 1 *Dodanie art. 32z do aktu w sprawie danych*	Ponowny użytkownik (ewentualnie z pomocą organu sektora	Osoby fizyczne lub prawne, na których prawa i interesy może mieć to wpływ	Ponowne wykorzystywanie bez zezwolenia	Pomoc ad hoc

		publicznego)			
Powiadomienie o zamiarze przekazania danych nieosobowych do państwa trzeciego i cel takiego przekazania (organowi sektora publicznego)	Artykuł 1 *Dodanie art. 32aa do aktu w sprawie danych*	Ponowny użytkownik	Organ sektora publicznego	Zamiar przekazania danych do państwa trzeciego	Pomoc ad hoc
Powiadomienie o zamiarze przekazania danych nieosobowych do państwa trzeciego, cel tego przekazania oraz odpowiednie zabezpieczenia (na rzecz osoby fizycznej lub prawnej, na której prawa i interesy może to mieć wpływ)	Artykuł 1 *Dodanie art. 32aa do aktu w sprawie danych*	Ponowny użytkownik (ewentualnie z pomocą organu sektora publicznego)	Osoba fizyczna lub prawna, na której prawa i interesy może mieć to wpływ	Zamiar przekazania danych do państwa trzeciego	Pomoc ad hoc
Wszystkie istotne informacje dotyczące stosowania art. 32z [warunki ponownego wykorzystywania], 32aa [państwa trzecie] i 32ab [opłaty] aktu w sprawie danych.	Artykuł 1 *Dodanie art. 32ad do aktu w sprawie danych*	Państwa członkowskie	Dostępne dla użytkowników pojedynczego punktu informacyjnego	Należy podać odpowiednie informacje	Pomoc ad hoc
Skarga wniesiona przez osoby fizyczne/prawne, jeżeli ich prawa wynikające z aktu w sprawie danych zostały naruszone lub w odniesieniu do	Artykuł 1 *Zmiana art. 38 ust. 1–2 aktu w sprawie danych*	Osoby fizyczne i prawne	Odpowiedni właściwy organ w danym państwie członkowskim	Skarga, która zostanie złożona	Pomoc ad hoc

innych istotnych kwestii					
Informacje na temat przebiegu postępowania/środków ochrony prawnej przed sądem w związku ze skargą złożoną na podstawie aktu w sprawie danych	Artykuł 1 *Zmiana art. 38 ust. 1–2 aktu w sprawie danych*	Odpowiedni właściwy organ	Osoby fizyczne lub prawne, które złożyły skargę	Złożona skarga	Pomoc ad hoc
Dane dotyczące doświadczeń i dobrych praktyk (EDIB)	Artykuł 1 *Dodanie rozdziału IXa do aktu w sprawie danych*	Europejska Rada ds. Innowacji w zakresie Danych	Komisja; Właściwe organy	Informacje, które należy przekazać	Pomoc ad hoc
Ocena rozdziałów II, III, IV, V, VI, VII i VIII aktu w sprawie danych Ocena rozdziałów VIIa, VIIb i VIIc aktu w sprawie danych	Artykuł 1 *Zmiana art. 49 ust. 1 aktu w sprawie danych* Artykuł 1 *Zmiana art. 49 ust. 2 aktu w sprawie danych*	Komisja Europejska	Parlament Europejski; Rada; Europejski Komitet Ekonomiczno-Społeczny	Przeprowadzona ocena aktu w sprawie danych	Do 12 września 2028 r. Do dnia [wejście w życie plus 5 lat] r.
Zgłaszanie naruszeń ochrony danych osobowych	Artykuł 3 *Zmiana art. 33 ust. 1 RODO*	Administrator danych	Organ nadzorczy	Wystąpienie naruszenia ochrony danych	Pomoc ad hoc
Wniosek EROD dotyczący wspólnego wzoru powiadomienia o naruszeniu	Artykuł 3 *Zmiana art. 33 ust. 1*	Europejska Rada Ochrony Danych	Komisja	Wniosek, który zostanie złożony	W ciągu [miesięcy] od daty rozpoczęcia stosowania niniejszego

ochrony danych	*RODO*				rozporządzenia Co trzy lata
Wnioski EROD dotyczące oceny skutków dla ochrony danych	Artykuł 3 *Zmiana art. 70 ust. 1 RODO*	Europejska Rada Ochrony Danych	Komisja	Wniosek, który zostanie złożony	Pomoc ad hoc
Zgłoszenia poważnych incydentów zgodnie z dyrektywą NIS 2	Artykuł 6 *Dodanie art. 23a i 23b, zmiana art. 23 i art. 30 ust. 1 dyrektywy NIS 2*	Podmioty kluczowe i ważne	CSIRT/właściwe organy (w stosownych przypadkach)	Okoliczności opisane w art. 23 ust. 3 dyrektywy NIS 2	Pomoc ad hoc
Zgłaszanie naruszeń ochrony danych osobowych	Artykuł 3 *Zmiana art. 33 RODO*	Administratorzy danych	Organ nadzorczy	Naruszenie ochrony danych osobowych	Pomoc ad hoc
Zgłaszanie poważnych incydentów związanych z ICT na podstawie DORA; dobrowolne zgłaszanie poważnych cyberzagrożeń na podstawie DORA	Artykuł 8 *Zmiana art. 19 DORA*	Podmioty finansowe	Odpowiedni właściwy organ	Poważne incydenty związane z ICT; poważne cyberzagrożenia	Pomoc ad hoc
Zgłaszanie incydentów, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych, zgodnie z dyrektywą CER	Artykuł 9 *Zmiana art. 15 dyrektywy CER*	Podmioty krytyczne	Właściwy organ	Incydenty, które istotnie zakłócają lub mogą istotnie zakłócać świadczenie usług kluczowych	Pomoc ad hoc

4.3. Rozwiązania cyfrowe

Ogólny opis rozwiązań cyfrowych

Uwaga: wszystkie rozwiązania cyfrowe wyszczególnione poniżej są wcześniej istniejącymi rozwiązaniami, których podstawę prawną przenosi się z jednego rozporządzenia do drugiego. W szczególności przepisy aktu w sprawie zarządzania danymi przeniesiono do aktu w sprawie danych.

Rozwiązanie cyfrowe	**Odniesienia do wymogów**	**Podstawowa wymagana funkcjonalność**	**Organ odpowiedzialny**	**W jaki sposób zapewniania jest dostępność?**	**W jaki sposób uwzględniono wymóg ponownego wykorzystania?**	**Wykorzystanie technologii sztucznej inteligencji (stosownie do przypadku)**
Publiczny rejestr unijny usług pośrednictwa danych i organizacji altruizmu danych	*Dodanie art. 32a do aktu w sprawie danych*	Przechowywanie i publikowanie obowiązkowych informacji	Komisja Europejska	//	//	Nie dotyczy
Pojedynczy punkt informacyjny (na mocy aktu w sprawie danych)	Artykuł 1 *Dodanie art. 32ad do aktu w sprawie danych*	Informacje, których dostępność należy zapewnić Podmiot właściwy do otrzymywania zapytań lub wniosków o ponowne wykorzystywanie kategorii danych chronionych	Komisja Europejska	Pojedynczy punkt dostępu oferujący elektroniczny przeszukiwalny rejestr danych dostępnych w krajowych pojedynczych punktach informacyjnych oraz dalsze	Dostępność drogą elektroniczną przeszukiwalnego wykazu zasobów zawierającego przegląd wszystkich dostępnych zasobów danych [...] oraz warunki ich ponownego	Nie dotyczy

		Przekazywanie wniosków, w miarę możliwości i w stosownych przypadkach w sposób zautomatyzowany, właściwym organom sektora publicznego Udostępnienie drogą elektroniczną przeszukiwalnego wykazu zasobów zawierającego przegląd wszystkich dostępnych zasobów dokumentów		informacje na temat sposobu wnioskowania o dane za pośrednictwem tych krajowych pojedynczych punktów informacyjnych	wykorzystywania.	
Pojedynczy punkt kontaktowy do zgłaszania incydentów	Artykuł 6 *Dodanie art. 23a do dyrektywy NIS 2*	Umożliwienie zgłaszania incydentów zgodnie z odpowiednimi aktami na szczeblu Unii Zapewnienie interoperacyjności i kompatybilności z europejskimi portfelami	Komisja Europejska; ENISA,	Interoperacyjność i kompatybilność z europejskimi portfelami biznesowymi i ich własnymi środkami dostępności	Możliwość uwzględnienia zgłaszania incydentów na podstawie różnych aktów prawnych; możliwość włączenia w przyszłości dalszych podstaw	Nie dotyczy

		biznesowymi			prawnych do rozwiązania opartego na pojedynczym punkcie kontaktowym	

W odniesieniu do każdego rozwiązania cyfrowego wyjaśnienie, w jaki sposób to rozwiązanie cyfrowe spełnia wymogi mających zastosowanie polityk cyfrowych i aktów ustawodawczych

Publiczny rejestr unijny usług pośrednictwa danych i organizacji altruizmu danych

Polityka cyfrowa lub sektorowa (jeżeli mają zastosowanie)	**Wyjaśnienie, w jaki sposób te polityki są zgodne**
Akt w sprawie sztucznej inteligencji	Nie dotyczy
Ramy UE dotyczące cyberbezpieczeństwa	Nie dotyczy
eIDAS	Nie dotyczy
Jednolity portal cyfrowy oraz IMI	Zmiana rozporządzenia (UE) 2018/1724 w celu dodania „rejestracji jako dostawcy usług pośrednictwa danych” i „rejestracji jako uznanej w Unii organizacji altruizmu danych” w załączniku II.
Inne	Nie dotyczy

Pojedynczy punkt informacyjny (na mocy aktu w sprawie danych)

Polityka cyfrowa lub sektorowa (jeżeli mają zastosowanie)	Wyjaśnienie, w jaki sposób te polityki są zgodne
Akt w sprawie sztucznej inteligencji	Nie dotyczy
Ramy UE dotyczące cyberbezpieczeństwa	Organy sektora publicznego mogą przewidzieć wymóg, aby dostęp do danych lub dokumentów i ich ponowne wykorzystywanie odbywało się w sposób zdalny w bezpiecznym środowisku przetwarzania zapewnianym lub kontrolowanym przez organ sektora publicznego. W takich przypadkach organy sektora publicznego wprowadzają warunki, które pozwalają zachować integralność funkcjonowania systemów technicznych wykorzystywanego bezpiecznego środowiska przetwarzania.
eIDAS	Nie dotyczy
Jednolity portal cyfrowy oraz IMI	Nie dotyczy
Inne	Pojedynczy punkt informacyjny musi być zgodny z rozporządzeniem (UE) 2016/679 (RODO). Organy sektora publicznego mogą ustanowić wymogi dotyczące udzielania dostępu do celów ponownego wykorzystywania danych lub dokumentów wyłącznie w przypadku, gdy zostały one zanonimizowane lub poddane innym formom odpowiedniego przygotowania. Ponadto w przypadku nieuprawnionego ponownego wykorzystywania danych nieosobowych ponowny użytkownik ma obowiązek poinformować o tym osoby fizyczne, na których prawa i interesy może mieć to wpływ.

Pojedynczy punkt kontaktowy do zgłaszania incydentów

Polityka cyfrowa lub sektorowa (jeżeli mają zastosowanie)	Wyjaśnienie, w jaki sposób te polityki są zgodne
Akt w sprawie sztucznej inteligencji	Nie dotyczy
Ramy UE dotyczące	Zmiany dyrektywy NIS 2 nieodłącznie koncentrują się na cyberbezpieczeństwie. W szerszym ujęciu

cyberbezpieczeństwa	pojedynczy punkt kontaktowy ma służyć jako punkt dostępu, za pośrednictwem którego wszystkie zgłoszenia incydentów związanych z cyberbezpieczeństwem kieruje się do odpowiednich właściwych organów na podstawie kilku aktów prawnych Unii.
eIDAS	Pojedynczy punkt kontaktowy jest również wymagany do zgłaszania incydentów na podstawie rozporządzenia (UE) nr 910/2014 (rozporządzenie eIDAS). ENISA zapewnia, aby pojedynczy punkt kontaktowy był interoperacyjny i kompatybilny z europejskimi portfelami biznesowymi oraz aby europejskie portfele biznesowe można było wykorzystywać co najmniej do identyfikacji i uwierzytelniania podmiotów korzystających z pojedynczego punktu kontaktowego. Inicjatywa polityczna dotycząca europejskiego portfela biznesowego będzie opierać się na ramach eIDAS.
Jednolity portal cyfrowy oraz IMI	Nie dotyczy
Inne	We wniosku uwzględniono cały cyfrowy dorobek prawny UE, w tym polityki dotyczące danych, cyberbezpieczeństwa i telekomunikacji.

4.4. Ocena interoperacyjności

Ogólny opis cyfrowych usług publicznych, na które te wymogi mają wpływ

Cyfrowa usługa publiczna lub kategoria cyfrowych usług publicznych	**Opis**	**Odniesienia do wymogów**	**Rozwiązania Interoperacyjnej Europy** **(NIE DOTYCZY)**	**Inne rozwiązania w zakresie interoperacyjności**
Europejska infrastruktura zarządzania danymi i przejrzystości	Cyfrowa usługa publiczna zapewniająca infrastrukturę zarządzania danymi i przejrzystości oraz wykorzystująca m.in. publiczny rejestr unijny usług pośrednictwa danych i organizacji altruizmu danych oraz pojedynczy punkt informacyjny pomagający ponownym użytkownikom w znalezieniu informacji na temat ponownego wykorzystywania niektórych kategorii danych chronionych. Kategoria cyfrowych usług publicznych zgodnie z COFOG 04.9.0 – Sprawy gospodarcze, gdzie indziej niesklasyfikowane (usługi zbiorowe)	Artykuł 1	//	//
Zgłaszanie zdarzeń	Cyfrowa usługa publiczna umożliwiająca zgłaszanie incydentów za pośrednictwem	Artykuł 6	//	Europejskie portfele biznesowe

	pojedynczego punktu kontaktowego. Kategoria cyfrowych usług publicznych zgodnie z COFOG 03.6.0 Porządek i bezpieczeństwo publiczne, gdzie indziej niesklasyfikowane			

Wpływ wymogów na interoperacyjność transgraniczną dla każdej cyfrowej usługi publicznej

Uwaga: w poniższej analizie numery artykułów podane w sekcji „Środki" odnoszą się do zmienianych aktów. Mapowanie zgodnie z wymogami aktu zbiorczego przeprowadza się raz, na górze każdej komórki.

Cyfrowa usługa publiczna nr 1 – europejska infrastruktura zarządzania danymi i przejrzystości

Ocena	**Środki**	**Potencjalne utrzymujące się bariery (jeśli dotyczy)**
Dostosowanie do istniejących polityk cyfrowych i sektorowych. **Proszę wymienić mające zastosowanie polityki cyfrowe i sektorowe.**	Artykuł 1 Dostosowanie do obowiązujących polityk cyfrowych i sektorowych znajduje odzwierciedlenie w motywach aktu w sprawie zarządzania danymi: Jednolity portal cyfrowy (rozporządzenie (UE) 2018/1724) (motyw 56): procedury zgłaszania na potrzeby usług pośrednictwa danych i procedury rejestracji organizacji altruizmu danych należy udostępniać za pomocą jednolitego portalu cyfrowego, aby zapewnić transgraniczny dostęp online. Europejskie ramy interoperacyjności (motyw 54): infrastruktura cyfrowa musi być zgodna z zasadami europejskich ram interoperacyjności, aby zapewnić transgraniczne i międzysektorowe wykorzystanie danych. Moduły instrumentu „Łącząc Europę" (instrument „Łącząc Europę" – infrastruktura usług cyfrowych) (motyw 54): Odniesienia do „słowników podstawowych i modułów	

	instrumentu »Łącząc Europę«”. Usługa cyfrowa powinna wykorzystywać moduły instrumentu „Łącząc Europę” (takie jak eDelivery, tożsamość elektroniczna, podpis elektroniczny) do wdrażania technicznego. Wymogi dostępności (dyrektywy (UE) 2016/2102 i (UE) 2019/882) (motyw 62). Dyrektywa (UE) 2016/2102 (dyrektywa w sprawie dostępności stron internetowych): rejestry publiczne i usługi cyfrowe muszą być dostępne dla osób z niepełnosprawnościami; dyrektywa (UE) 2019/882 (europejski akt prawny w sprawie dostępności): usługi cyfrowe muszą spełniać wymogi dostępności. RODO (rozporządzenie (UE) 2016/679) (motyw 4 i 35): wszystkie usługi cyfrowe przetwarzające dane osobowe muszą być zgodne z wymogami RODO w zakresie ochrony danych, prywatności i bezpieczeństwa. Rozporządzenie (UE) 2018/1725 (motyw 4): w przypadku gdy instytucje Unii przetwarzają dane za pośrednictwem tych rejestrów, muszą przestrzegać niniejszego rozporządzenia. Dyrektywa w sprawie otwartych danych (dyrektywa (UE) 2019/1024) (motywy 6 i 10): „Dyrektywa (UE) 2019/1024 oraz sektorowe prawo Unii zapewniają, aby podmioty sektora publicznego umożliwiały łatwy dostęp do większej ilości wytworzonych przez siebie danych na potrzeby ich wykorzystywania oraz ponownego wykorzystywania”; Usługa cyfrowa uzupełnia dyrektywę w sprawie otwartych danych przez uwzględnienie kategorii danych chronionych, które nie wchodzą w jej zakres, przy jednoczesnym zapewnieniu, aby w stosownych przypadkach organy sektora publicznego przestrzegały zasad „otwartości w fazie projektowania i otwartości domyślnej”. Polityki sektorowe dotyczące europejskich przestrzeni danych i danych sektorowych, w tym europejskiej przestrzeni danych dotyczących zdrowia, europejskiej przestrzeni danych dotyczących mobilności, danych dotyczących Europejskiego Zielonego Ładu/danych dotyczących klimatu i energii, danych produkcyjnych i przemysłowych, danych dotyczących usług finansowych, danych dotyczących rolnictwa, przestrzeni danych dla administracji publicznej i przestrzeni danych dotyczących umiejętności.	

Środki organizacyjne na rzecz sprawnego transgranicznego świadczenia cyfrowych usług publicznych. **Proszę wymienić przewidywane środki zarządzania.**	Artykuł 1 **Wyznaczenie i koordynowanie właściwego organu** - Artykuł 32b: każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za rejestrację dostawców usług pośrednictwa danych i organizacji altruizmu danych. Te właściwe organy zachowują niezależność od wszelkich uznanych dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych. Artykuł 32ac: każde państwo członkowskie wyznacza co najmniej jeden właściwy organ wspomagający organy sektora publicznego, które udzielają lub odmawiają dostępu do celów ponownego wykorzystywania kategorii danych chronionych. Artykuł 32g: właściwe organy monitorują i nadzorują przestrzeganie przepisów aktu w sprawie danych przez uznanych dostawców usług pośrednictwa danych i uznane organizacje altruizmu danych. **Mechanizm jurysdykcji transgranicznej** Artykuł 32e: usługi pośrednictwa danych wchodzą w zakres kompetencji właściwego organu w państwie członkowskim, w którym znajduje się główna jednostka organizacyjna. Ta sama zasada ma zastosowanie do organizacji altruizmu danych. **Wzajemne uznawanie i jedna rejestracja** Artykuł 32e: rejestracja jako usługa pośrednictwa danych/organizacja altruizmu danych jest ważna we wszystkich państwach członkowskich. Artykuł 32a: stosowanie wspólnego wzoru logo **Scentralizowane rejestry na szczeblu UE na potrzeby gromadzenia danych i przejrzystości** Artykuł 32a: publiczne rejestry unijne wszystkich uznanych dostawców usług pośrednictwa danych i organizacji altruizmu danych.	

	Artykuł 32e: właściwe organy niezwłocznie powiadamiają Komisję drogą elektroniczną o nowych rejestracjach, zmianach i usunięciach, a Komisja odpowiednio aktualizuje rejestry UE **Monitorowanie i koordynacja egzekwowania przepisów** Właściwe organy krajowe Europejska Rada ds. Innowacji w zakresie Danych **Zarządzanie przekazywaniem danych do państw trzecich** Artykuł 32aa: wymogi dotyczące przekazywania danych nieosobowych do państw trzecich przez ponownych użytkowników. **Uzgodnienia dotyczące wyłączności** Artykuł 32k: określenie dopuszczalności uzgodnień dotyczących wyłączności odnoszących się do ponownego wykorzystywania danych lub dokumentów będących w posiadaniu organów sektora publicznego. Domaganie się przejrzystości ostatecznych warunków.	
Środki podjęte w celu zapewnienia wspólnego zrozumienia danych **Proszę wymienić takie środki.**	Artykuł 1 **Wspólne normy i interoperacyjne ramy** - Europejska Rada ds. Innowacji w zakresie Danych doradza Komisji Europejskiej w sprawie działań normalizacyjnych, które należy podjąć w odniesieniu do międzysektorowych aspektów dzielenia się danymi, w tym w odniesieniu do powstawania wspólnych europejskich przestrzeni danych, z uwzględnieniem sektorowych działań normalizacyjnych. o Artykuł 42: Europejska Rada ds. Innowacji w zakresie Danych pomaga w przyjęciu „wytycznych ustanawiających specyfikacje w zakresie interoperacyjnych i wspólnych praktyk na potrzeby funkcjonowania wspólnych europejskich przestrzeni danych”.	

	- Wspólne logo na potrzeby identyfikacji usług pośrednictwa danych i organizacji altruizmu danych. - Artykuł 32q: organy sektora publicznego i przedsiębiorstwa publiczne udostępniają swoje dane lub dokumenty, w miarę możliwości i stosownie do przypadku, za pomocą środków elektronicznych – w formatach, które są otwarte, nadają się do odczytu maszynowego, są dostępne, możliwe do znalezienia i możliwe do ponownego wykorzystywania, wraz z ich metadanymi. W miarę możliwości zarówno format, jak i metadane muszą być zgodne z otwartymi standardami formalnymi. **Inne właściwe środki:** - Artykuł 32t: państwa członkowskie, we współpracy z Komisją, kontynuują starania na rzecz uproszczenia dostępu do zbiorów danych, udostępniając odpowiednie zbiory danych w formatach, które są dostępne, łatwe do znalezienia i możliwe do ponownego wykorzystywania za pomocą środków elektronicznych. - Artykuł 32u: państwa członkowskie wspierają dostępność danych badawczych w sposób zgodny z zasadami FAIR.	
Stosowanie wspólnie uzgodnionych otwartych specyfikacji i norm technicznych. **Proszę wymienić takie środki.**	Artykuł 1 **Środki w zakresie danych nadające się do odczytu maszynowego:** - Artykuł 32a: nadający się do odczytu maszynowego rejestr dostawców usług pośrednictwa danych Unii Europejskiej. - Artykuł 32a: nadający się do odczytu maszynowego rejestr organizacji altruizmu danych Unii Europejskiej. - Artykuł 32q: organy sektora publicznego będą udostępniać swoje dane/dokumenty, w miarę możliwości, w formatach, które są otwarte, nadają się do odczytu maszynowego, są dostępne, możliwe do znalezienia i możliwe do ponownego wykorzystywania, wraz z ich metadanymi. W miarę możliwości	

	zarówno format, jak i metadane muszą być zgodne z otwartymi standardami formalnymi. - Artykuł 32q: zbiory danych o wysokiej wartości są udostępniane do ponownego wykorzystywania w formacie nadającym się do odczytu maszynowego, za pośrednictwem odpowiednich interfejsów API oraz, w odpowiednich przypadkach, do zbiorczego pobrania. - Artykuł 32t: państwa członkowskie wprowadzają ustalenia praktyczne ułatwiające wyszukiwanie danych lub dokumentów dostępnych do ponownego wykorzystywania, takie jak wykazy najważniejszych zasobów danych lub dokumentów wraz z odpowiednimi metadanymi, dostępne – jeżeli jest to możliwe i w stosownych przypadkach – w internecie i w formatach nadających się do odczytu maszynowego, oraz portale połączone z wykazami zasobów. W miarę możliwości państwa członkowskie ułatwiają wielojęzyczne wyszukiwanie danych lub dokumentów. - Artykuł 32w określone zbiory danych o wysokiej wartości nadają się do odczytu maszynowego. Akty wykonawcze mogą określać ustalenia dotyczące formatów danych i metadanych oraz rozwiązania techniczne na potrzeby rozpowszechniania. **Środki interakcji maszyna-maszyna:** - Artykuł 32ad: wprowadzenie obowiązku korzystania z pojedynczego punktu informacyjnego. Pojedynczy punkt informacyjny jest właściwy do przyjmowania zapytań lub wniosków oraz przekazuje je, w miarę możliwości i w stosownych przypadkach w sposób zautomatyzowany, właściwym organom sektora publicznego lub właściwym organom. **Inne właściwe środki:** - Artykuł 48a: zmiana załącznika II do rozporządzenia (UE) 2018/1724 (jednolity portal cyfrowy). Analiza synergii. - Motyw 52 aktu zbiorczego: w miarę możliwości ENISA powinna uwzględniać	

	istniejące krajowe rozwiązania techniczne ułatwiające zgłaszanie incydentów, takie jak platformy krajowe, przy opracowywaniu specyfikacji dotyczących środków technicznych, operacyjnych i organizacyjnych związanych z utworzeniem, utrzymaniem i bezpiecznym funkcjonowaniem pojedynczego punktu kontaktowego. Ponadto ENISA powinna rozważyć protokoły i narzędzia techniczne, takie jak interfejsy programowania aplikacji i standardy nadające się do odczytu maszynowego, które umożliwiają podmiotom ułatwienie włączenia obowiązków sprawozdawczych do procesów biznesowych, a organom połączenie pojedynczego punktu kontaktowego z ich krajowymi systemami zgłaszania.	

Cyfrowa usługa publiczna nr 2 – zgłaszanie incydentów

Ocena	**Środki**	**Potencjalne utrzymujące się bariery (jeśli dotyczy)**
Dostosowanie do istniejących polityk cyfrowych i sektorowych. **Proszę wymienić mające zastosowanie polityki cyfrowe i sektorowe.**	Artykuł 6 Ogólne dostosowanie do istniejących polityk cyfrowych i sektorowych zapewnia dyrektywa (UE) 2022/2555 (NIS 2), którą zmienia obecnie akt zbiorczy prawa cyfrowego. Ponadto w akcie zbiorczym przewidziano synergie z europejskim portfelem biznesowym oraz rozporządzeniem (UE) 2024/2847 (akt dotyczący cyberodporności). W szczególności: • W art. 23 ust. 4 nakazano korzystanie z pojedynczego punktu kontaktowego do celów zgłaszania w ramach dyrektywy NIS 2. • Art. 23 ust. 1 stanowi, że zgłoszenie poważnego incydentu na podstawie art. 14 ust. 3 rozporządzenia (UE) 2024/2847 (akt dotyczący cyberodporności) stanowi również zgłoszenie informacji na podstawie dyrektywy (UE) 2022/2555 (NIS 2). Jest to zgodne z zasadą jednorazowości. • W art. 23a ust. 3 lit. d) przewidziano powiązanie z europejskimi portfelami biznesowymi.	

Środki organizacyjne na rzecz sprawnego transgranicznego świadczenia cyfrowych usług publicznych. **Proszę wymienić przewidywane środki zarządzania.**	Artykuł 6 W art. 23a określono role i obowiązki. Mianowicie ENISA: • Opracowuje i utrzymuje pojedynczy punkt kontaktowy w celu wsparcia obowiązku zgłaszania incydentów i powiązanych zdarzeń na podstawie aktów prawnych Unii. • Wprowadza środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa pojedynczego punktu kontaktowego oraz przekazywanych lub rozpowszechnianych informacji. W tym celu konsultuje się z Komisją, siecią CSIRT i odpowiednimi właściwymi organami.	
Środki podjęte w celu zapewnienia wspólnego zrozumienia danych **Proszę wymienić takie środki.**	Artykuł 6 W art. 23a zobowiązano ENISA do przygotowania specyfikacji, które zapewnią niezbędną zdolność na potrzeby interoperacyjności w odniesieniu do innych odpowiednich obowiązków w zakresie zgłaszania. *Uwaga: wymogi dotyczące treści na potrzeby zgłaszania incydentów określono bardziej szczegółowo w odpowiednich aktach prawnych Unii, w tym w dyrektywie (UE) 2022/2555 (NIS 2). W art. 23a ust. 3 lit. c) pakietu zbiorczego wyjaśniono, że ENISA zapewnia, aby zostały one należycie uwzględnione.*	
Stosowanie wspólnie uzgodnionych otwartych specyfikacji i norm technicznych. **Proszę wymienić takie środki.**	Artykuł 6 W art. 23a wzywa się do opracowania specyfikacji: • ENISA zapewnia i wdraża specyfikacje dotyczące środków technicznych związanych z utworzeniem, utrzymaniem i bezpiecznym funkcjonowaniem pojedynczego punktu kontaktowego. Specyfikacje te obejmują między innymi:	

	○ zdolności niezbędne do zapewnienia interoperacyjności w odniesieniu do innych istotnych obowiązków w zakresie zgłaszania; ○ rozwiązania techniczne umożliwiające odpowiednim podmiotom i organom dostęp do informacji, ich przekazywanie, pobieranie, przesyłanie lub przetwarzanie w inny sposób z pojedynczego punktu kontaktowego oraz protokoły i narzędzia techniczne umożliwiające podmiotom i organom dalsze przetwarzanie otrzymanych informacji w ich systemach. • Jeżeli są dostępne, pojedynczy punkt kontaktowy musi być interoperacyjny i kompatybilny z europejskimi portfelami biznesowymi.	

4.5. Środki wspierające cyfrowe wdrażanie

Ogólny opis środków wspierających cyfrowe wdrażanie

Opis środka	**Odniesienia do wymogów**	**Rola Komisji** (jeżeli dotyczy)	**Podmioty, które mają być zaangażowane** (jeżeli dotyczy)	**Przewidywany harmonogram** (jeżeli dotyczy)
Akt wykonawczy: wzór wspólnego logo dla dostawców usług pośrednictwa danych	Artykuł 1	Określa się cechy wspólnego logo, w tym jego wzór i zasady stosowania.	Komitet w zakresie procedury sprawdzającej	//
Akt wykonawczy: wzór wspólnego logo	Artykuł 1	Określa się cechy wspólnego logo, w tym	Komitet w zakresie	//

dla uznanego altruizmu danych		jego wzór i zasady stosowania.	procedury sprawdzającej	
Monitorowanie i przestrzeganie przepisów: właściwe organy mogą monitorować przestrzeganie przepisów z własnej inicjatywy albo na wniosek osób fizycznych lub prawnych.	Artykuł 1	//	Właściwe organy, usługi pośrednictwa danych, organizacje altruizmu danych	//
Akt wykonawczy: określone zbiory danych o wysokiej wartości	Artykuł 1	Ustanowienie wykazu określonych zbiorów danych o wysokiej wartości. Można określić warunki publikacji i ponownego wykorzystywania zbiorów danych o wysokiej wartości.	Komitet w zakresie procedury sprawdzającej	//
Wytyczne: • Europejska Rada ds. Innowacji w zakresie Danych doradza w sprawie wytycznych dotyczących wspólnych europejskich przestrzeni danych • Europejska Rada ds. Innowacji w zakresie Danych ma przyjąć wytyczne dotyczące interoperacyjnych ram	Artykuł 1	Wsparcie z Europejskiej Rady ds. Innowacji w zakresie Danych	Europejska Rada ds. Innowacji w zakresie Danych	//

Akt wykonawczy: wspólny wzór zawiadomienia o naruszeniu ochrony danych osobowych	Artykuł 3	Przyjęcie wspólnego wzoru w oparciu o wniosek EROD.	Komitet w zakresie procedury sprawdzającej	//
Akt delegowany: zautomatyzowane i nadające się do odczytu maszynowego wskazania wyborów dokonanych przez osobę, której dane dotyczą	Artykuł 3	Określenie obowiązku dla przeglądarek internetowych i dostawców końcowych urządzeń	Komitet w zakresie procedury sprawdzającej	//
Akt wykonawczy: zgłaszanie incydentów CER	Artykuł 9	Doprecyzowanie rodzaju i formatu informacji zgłaszanych na podstawie art. 15 ust. 1 dyrektywy (UE) 2022/2557 (CER).	//	//